Montreal AI Ethics Institute

L'Institut d'éthique en intelligence artificielle de Montréal

https://montrealethics.ai

Rapport préparé par:

Mirka Snyder Caron, Associée Senior

Réponse à la Commission d'accès à l'information du Québec portant sur les amendements potentiels à la Loi sur la protection des renseignements personnels dans le secteur privé particuliers à l'intelligence artificielle.

Date: 22 mars 2020

Introduction:

En février 2020, l'Institut d'éthique en intelligence artificielle de Montréal **(MAIEI)** a été invité par le Commissariat à la vie privée du Canada **(CVPC)** afin de se joindre à une table ronde d'experts et de commenter sur leurs propositions portant sur certains amendements à la *Loi sur la protection des renseignements personnels et les documents électroniques* **(LPRPDE)** portant sur l'intelligence artificielle **(IA)**. En parallèle, MAIEI a aussi été invité par la Commission d'accès à l'information du Québec **(CAIQ)** à présenter leurs commentaires par écrit concernant le processus de consultations et les propositions particulière à la loi québécoise en matière de vie privée, soit la *Loi sur la protection des renseignements personnels dans le secteur privé* **(LPRPSP)**.

Le présent document inclut les réponses, les recommandations, et les commentaires de MAIEI par écrit. Pour chaque proposition et question de CAIQ, MAIEI donne une réponse courte, une liste sommaire des recommandations, et des commentaires pertinents. Nous vous laissons avec trois déclarations à garder en tête alors que vous passerez à travers les prochaines pages:

1) Les systèmes IA devraient être utilisés de manière à augmenter la capacité humaine à bâtir des connections et des associations significatives à des fins valorisantes, et non pas comme substitut à une relation de confiance.

2) Les humains ont collectivement accepté de respecter la règle de droit et la loi, mais pour les machines, le code est la règle. Là où les systèmes socio-techniques sont déployés afin de prendre des décisions importantes, et afin de créer profils ou des inférences concernant des individus, nous aurons de plus en plus à tenter l'exercice difficile de rédiger et de structurer nos lois de manière à pouvoir être interprétées par ces machines.

3) Travaillons ensemble afin de bâtir un monde ou l'IA Responsable devient la règle, et afin d'éviter que nos systèmes socio-techniques deviennent "trop connectés pour échouer"[1].

Bien vôtre,
MAIEI[2]

[1]ARNER, Douglas, OTHERS, *The Dark Side of Digital Financial Transformation: The New Risks of Fintech and the Rise of TechRisk*, University of Hong Kong Faculty of Law Research Paper No. 2019/112, 37 pages,p. 5.
[2]https://montrealethics.ai

Proposition CAIQ 1: L'inférence ou la création de renseignements personnels à partir d'un algorithme devraient être limitées, en application du critère de nécessité.

Commentaires généraux MAIEI:

Limiter l'inférence ou la création de renseignements personnels **("RP")** revient à exclure la majorité des systèmes et algorithmes IA complexes mais qui peuvent être extrêmement performants. De plus, il pourrait être techniquement difficile de programmer le système d'intelligence artificielle **("IA")** afin de respecter cette règle[3]. Des solutions plus efficaces serait une combinaison cumulative de:

a) programmation au moment du design ("*privacy by design*"[4] et "*human rights by design*"[5])

b) consentement libre et éclairé

c) droit de l'individu de négocier le résultat proposé par le système[6]

d) des mécanismes organisationnelles et techniques de vérification et de validation. (incluant l'opportunité d'un mécanisme de "remise à zéro" ("*reset*")[7]).

Proposition CAIQ 2: Les activités de profilage, d'analyse et de prédiction devraient être définies dans la loi. La loi devrait prévoir des conditions et des obligations les encadrant, comme :

2.1. Interdire l'utilisation de certains types de renseignements personnels afin d'effectuer du profilage (ex. : renseignements concernant l'origine raciale ou ethnique, les croyances et les opinions politiques, la santé, l'orientation sexuelle et les renseignements

[3]BOURTOULE, LUCAS, OTHERS,, Machine Unlearning, University of Toronto and Vector Institute, https://arxiv.org/pdf/1912.03817.pdf., 16 pages.
[4]CAVOUKIAN, "Privacy by Design: Foundational Principles", https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf; Search Encrypt, Medium, "7 Principles of Privacy by Design", https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce
[5]ALLISON-HOPE, Dunston, BSR, "Human Rights by Design", https://www.bsr.org/en/our-insights/blog-view/human-rights-by-design; PENNEY, Jonathon, OTHERS, "Human Rights by Design", Schneier on Security, https://www.schneier.com/blog/archives/2018/12/human_rights_by.html;
[6]Voir GUPTA, Abhishek, SNYDER CARON, Mirka, MAIEI Response to Office of the Privacy Commissioner of Canada Consultation Proposals pertaining to amendments to PIPEDA relative to Artificial Intelligence, 2020, 76 pages.
[7]RIBEIRO, Marco Tulio, OTHERS, "Why should I trust you?" Explaining the Predictions of any Classifier", https://arxiv.org/pdf/1602.04938v1.pdf; YAMPOLSKY, Roman, "Artificial Intelligence Safety and Security", CRC Press, 2018.

financiers ou biométriques), sauf si certaines conditions prévues dans la loi le permettent;

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

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

Commentaires généraux MAIEI:

Il y a problème inhérent dans l'exercice d'établir une définition, en particulier lorsque la définition revient à un exercice de limitations de concept. Il faudrait au moins s'assurer de rédiger la définition en préconisant une interprétation large et libérale, avec plutôt une liste d'exemples non exhaustifs fondés sur des cas concrets et existants, et non pas une interprétation limitative ou exclusive, afin de considérer les conséquences de "**l'effet mosaïque**"[8] de l'écosystème des données de cette ère.

Il nous semble préférable de concentrer les efforts de définition sur les activités et les fins de "systèmes" que de "l'IA", vu la difficulté et l'ambiguïté de définir des associations avec un potentiel illimité de création et de connections[9]. Afin d'éviter les tentatives d'exclure l'application de la loi créant des catégories entre des systèmes complètement automatisés, semi-automatisés, ou non, nous proposons que la définition, et les obligations relevant de "**systèmes socio-techniques**"[10], devraient comprendre à la fois les plateformes non augmentées[11], et ce, quelque soit le nombre et la qualification de l'humain liés ou intégrés au processus ou au système concerné[12].

Toutefois, nous considérons qu'il peut être intéressant, selon le degré de pessimisme et d'inquiétude liés à l'IA, qu'une allusion expresse dans la loi pourrait

[8]HUBER, Rose, "Mosaic Effect" Paints Vivid Pictures of Tech Users' Lives", https://wws.princeton.edu/news-and-events/news/item/mosaic-effect-paints-vivid-pictures-tech-users-lives-felten-tells-privacy

[9]Voir GUPTA, Abhishek, SNYDER CARON, Mirka, MAIEI Response to Office of the Privacy Commissioner of Canada Consultation Proposals pertaining to amendments to PIPEDA relative to Artificial Intelligence, 2020, 76 pages (Ci-après **"Rapport MAIEI au CVPC"**); SNYDER CARON, Mirka, "The Transformative Effect of AI on the Banking Industry", Banking & Finance Law Review, April 2019, 34 BFLR 79-345; NORVIG, Peter, "Artificial Intelligence: A Modern Approach", Pearson, 3rd edition, 2016, p. 18ss.

[10]Voir Rapport MAIEI au CVPC.

[11]Par **"augmenté**" nous désirons viser le traitement automatisé de bases de données ou de profils d'individus soumis à des algorithmes prédictifs, d'apprentissage, ou d'apprentissage profond, afin d'inclure les systèmes, techniques et algorithmes compris comme étant des systèmes d'intelligence artificielle, quelque soit le type, (eg. arbre décisionnel versus deep-learning ("DL")).

[12]Contrairement à les catégorisations de processus et systèmes "complètement automatisés" et "semi-automatisés" proposées par le RGPD en UE.

être bénéfique si l'objectif législatif d'une loi amendée inclut l'intention de rassurer les citoyens canadiens et autres individus passant par le Canada ou y résidant, -et dans le cadre de la présente consultation, plus particulièrement au Québec-, en incluant des références à l'IA et à certaines obligations de gouvernance spécifiques. Mais nous suggérons alors de s'assurer que la rédaction favorise une interprétation promouvant une protection plus large que simplement concentrée sur ces systèmes, et qui puisse prendre en compte le potentiel quasi-illimité d'associations technologiques et de bases de données à ces systèmes.

Proposition CAIQ 2.1:

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

Commentaires MAIEI:

Oui.

Proposition CAIQ 2.2:

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;

Commentaires MAIEI:

Telle que rédigée, la proposition prend pour acquis que les entreprises utilisent déjà des systèmes d'analytique, profilage et prédiction, et impose l'obligation de désactiver ces systèmes. Nous suggérons plutôt que l'obligation générale soit rédigée de manière à ce que les entreprises n'activent pas ces systèmes liés à ces activités tant qu'elles n'auront pas reçu un consentement libre et éclairé de la part de l'individu concerné, et que le cadre de gouvernance responsable de ces systèmes, comprenant des mesures et mécanismes techniques et organisationnelles soit adéquatement mis en place.

En d'autres mots, nous suggérons plutôt une obligation générale soumise à des conditions de **"ne pas activer ces systèmes tant que (…)"**, au lieu de **"désactiver"** ces systèmes, cette désactivation devenant par ailleurs implicite si le consentement et les mesures et mécanismes ne sont pas mises en place dans les entreprises utilisant déjà ces systèmes. Le mécanisme de "désactivation" ou de

"désabonnement" devrait toutefois demeurer disponible durant tout le cours de la relation entre l'individu et l'entreprise, que cette relation soit purement contractuelle ou non, si l'individu décide que ces systèmes ne devraient plus être utilisés par l'entreprise lorsque celle-ci prend une décision à son égard, une fois qu'il ait été avisé des conséquences de cette option.

Si ces systèmes sont déjà utilisés avant l'amendement à la présente loi, un scénario de mise en conformité transitionnel devrait être permis, à savoir une période raisonnable pour modifier les systèmes concernés, ainsi que l'obligation d'aller obtenir un nouveau consentement de la part des personnes concernées. Il serait souhaitable que le régulateur désigné ait les compétences techniques et réglementaires, ainsi que la capacité en budget et en ressources humaines et techniques, afin d'accompagner les entreprises qui procèdent à cette transition[13] et qui requièrent certaines directives ou guides, par exemple, par l'entremise d'un "bac à sable conformité"[14], et non pas seulement un "bac à sable pour innovation"[15]. Ceci mènera l'industrie à mieux gérer son risque de conformité et permettra aussi au régulateur de connaître les développements en cours qu'il doit surveiller selon son mandat et sa juridiction.

Nous notons que si l'option de ne pas activer ou de désactiver ces systèmes est disponible à l'individu concerné, il y a un risque opérationnel qu'une majorité d'individus refusent l'application de ces systèmes à leurs RP, si ce mécanisme est facilement mis à leur disposition (ce qui, selon nous, devrait malgré tout, être imposé comme obligation expresse), et si les bénéfices à leur intention ne sont pas clairement indiqués ou réalisés.

Plateformes en ligne et médias sociaux:

Nous lions ce commentaire à l'exemple des plateformes de médias sociaux, qui permettent à des individus à travers le monde de connecter entre eux s'ils le désirent et selon leurs intérêts communs, quelque soit la classe sociale ou la hiérarchie professionnelles ou managériales, ou leurs origines.

Un aspect positif de l'utilisation de ces plateformes revient à une forme de "démocratisation d'accès et de connections", en permettant à chacun de gratuitement créer un profil, de s'exprimer librement et de connecter avec des

[13]GUPTA, Abhishek, SNYDER CARON, Mirka, "Response to the AHRC and WEF regarding Responsible Innovation in AI", Montreal AI Ethics Institute, 25 pages.
[14]ARNER, Douglas, OTHERS, "Fintech and Regtech in a nutshell, and the Future in a Sandbox", CFA Institute Research Foundation, https://www.cfainstitute.org/-/media/documents/article/rf-brief/rfbr-v3-n4-1.ashx
[15]Id.

individus, des groupes et des événement qu'ils considèrent désirables selon leurs préférences personnelles, et ce, "gratuitement"[16].

Certainement, il y a différents aspects négatifs qui ont été liés à ces plateformes sans frontières ("*cross-border technologies*"), par exemple, la propagation d'idées ou de mouvements allant à l'encontre des droits humains, ainsi que la circulation de fausses idées ou nouvelles trompeuses, ou d'informations manipulées à des fins d'interférence, de manipulation de masse ou d'exacerbation d'instabilité ("*fake news*" et "*disinformation*"), mais ceux-ci sont plutôt reliés aux types d'utilisation néfastes ou malicieuses de la plateforme plutôt que la plateforme elle-même.

Le modèle d'affaires général de plusieurs entreprises offrant l'accès à ce type de plateformes, revient à l'opportunité et la capacité de monétiser sur le volume de trafic d'individus et d'activités humaines roulant sur leurs plateformes et ce, généralement sur deux fronts: vendre des rapports marketing selon les intérêts et les préférences des individus utilisant leur plateforme à des entreprises, et poussant de la publicité de ces entreprises, ainsi que du contenu d'intérêt pour assurer une certaine loyauté, aux individus-utilisateurs.

Avec le temps, afin de mieux personnaliser à la fois leurs rapports marketing et la publicité poussée aux individus-utilisateurs, différents algorithmes ont été déployés sur ces plateformes pour augmenter les capacités intelligentes des systèmes afin de "lire", "d'apprendre", de "prédire", et de "personnaliser" les services offerts, sur la base des RP, des activités, et des comportements des individus-utilisateurs publiés sur ces plateformes. Dans certains cas, d'autres algorithmes ont aussi été déployés afin de prévenir, mitiger et éliminer les risques d'atteintes aux droits et libertés humains, les pratiques illégales, et les détections de langage ou d'activité extrémiste violente, entre autres.

En pratique, vu le volume de publicité que les entreprises veulent pousser, et le volume et la rapidité du trafic des individus-utilisateurs, il est humainement presqu'impossible de sélectionner un à un, par un employé, le type de publicité qui serait intéressant pour un individu-utilisateur donné et le rendre disponible sur la plateforme. Il serait aussi probablement insensé, inutile et ennuyant à l'individu-utilisateur de recevoir des publicités ou du contenu aléatoire ("*random selection*"), sans lien avec des intérêts ou préférences personnels. Le même commentaire s'applique aux algorithmes de détection, de prévention et d'élimination de pratiques illégales.

Lors de la rédaction d'une telle obligation de "non-activation" ou de "désactivation", il faudra considérer l'impact financier, économique et social que cela pourrait avoir sur

[16]Brian D. Loader & Dan Mercea (2011): "Networking Democracy?", Information, Communication & Society, 14:6, 757-769.;

ce type de modèles d'affaires. Il faudra aussi considérer l'impact sur l'individu-utilisateur.

Enfin, à tout événement, nous proposons un droit de négociation disponible à l'individu en tout temps lorsqu'un système socio-technique peut avoir un impact sur lui, et en particulier dans les cas où il y a une prise de décision automatisée ou augmentée à son endroit[17].

Utilisation des tableaux de bord:

À noter qu'il n'est pas clair en pratique si les plateformes style "tableau de bord ("*dashboard*") seront incluses ou non dans cette restriction, puisque ces outils permettent d'obtenir une vue d'ensemble des personnes concernées sans qu'il y ait autrement eu d'algorithmes prédictifs appliqués dessus, et peuvent permettre, par l'utilisation d'APIs, entre autres, la surveillance continue d'individus sur la base de données continuellement ou régulièrement mises à jour en temps réel ("*real-time*"). Nous suggérons qu'elles soient incluses, selon le type d'utilisation qui en est fait, vu leur impact potentiel sur les prises de décisions de l'utilisateur concernant des individus identifiables.

Autres intérêts:

À noter aussi qu'il faudra balancer les intérêts commerciaux, ainsi que l'intérêt du public, qui obligent par exemple certaines entreprises ou certains ordres professionnels de bien identifier, vérifier et connaître leurs clients, incluant les obligations "Know Your Client" **("KYC")**, pour le recyclage des produits de la criminalité et le financement des activités de terrorisme **("RPCFAT")**.

Par exemple, dans le contexte RPCFAT, il ne serait pas sensé de permettre à un individu de demander la non-activation ou la désactivation du système socio-technique, et, en pratique, proposer un haut niveau de transparence pourrait nuire aux enquêtes et à la prévention ou l'élimination de ce type d'activités ou de transactions.

Par contre, toujours en pratique, des erreurs humaines ou techniques de classification ou d'inférences, sont possibles[18]. Par exemple, un individu ou une entreprise peut être mis sur une liste d'indésirables, qui pourrait être partagée entre différentes institutions, et effectivement empêcher cet individu d'obtenir des produits ou services auprès d'une industrie spécifique, affectant ainsi son statut légal et financier.

[17]BOURTOULE, LUCAS, OTHERS,, Machine Unlearning, University of Toronto and Vector Institute, https://arxiv.org/pdf/1912.03817.pdf., 16 pages.; Voir "Rapport MAIEI au CPVP".
[18]RIBEIRO, Marco Tulio, OTHERS, "Why should I trust you?" Explaining the Predictions of any Classifier", https://arxiv.org/pdf/1602.04938v1.pdf

Dans ce cas, il serait aussi important que des mécanismes de notification, de révision, de vérification, de négociation et de correction soit imposés, et mis en place et disponibles en temps opportun, afin d'obtenir un équilibre entre la primauté de ces intérêts publics et commerciaux, et les droits civils, et les droits et libertés humains de l'individu concerné.

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

Commentaires MAIEI:

Oui, toutefois, ce principe va inévitablement rencontrer des difficultés techniques importantes dans son application.

En pratique, il sera difficile d'établir des critères de divulgation légaux, suffisamment compréhensibles, clairs, complets, ou protecteurs. Évidemment, cela dépend du type de système socio-technique utilisé. Mais un système socio-technique avec algorithme d'apprentissage ("*machine-learning" ou "ML*"), ou évoluant par apprentissage profond ("*deep-learning" ou "DL*") continuera d'inférer et de créer de nouveaux RP, et les poids associés à ces RP continueront de changer[19].

Toutefois, l'individu qui sera potentiellement affecté par un système socio-technique créant des inférences provenant des renseignements sur lui ou créant de nouveaux renseignements afin d'arriver à un résultat, devrait être minimalement informé de ce fait, pour qu'il puisse porter plus attention au résultat produit par ce système et vérifier si le résultat semble correct, raisonnable ou approprié[20]. S'il y a un indice à l'effet que ce résultat serait erroné ou illégalement discriminatoire, ou si le résultat ne lui convient pas, l'individu devrait avoir un droit de négociation, afin d'obtenir plus de détails sur les paramètres du système et les poids établis par le système sur différentes données le concernant, afin de s'assurer d'avoir été l'objet d'un résultat juste[21].

Pour demeurer efficace, il devra être combiné avec d'autres mesures organisationnelles, légales et techniques pour assurer une protection adéquate des personnes concernées. (éviter la discrimination illégale, par exemple).

---

[19]Deepmind, AlphaGo, https://deepmind.com/research/case-studies/alphago-the-story-so-far; RIBEIRO, Marco Tulio, OTHERS, "Why should I trust you?" Explaining the Predictions of any Classifier", https://arxiv.org/pdf/1602.04938v1.pdf
[20]KLEINBERG, OTHERS, "Inherent Trade-Offs in the Fair Determination of Risk Scores", https://arxiv.org/abs/1609.05807; AI Fairness 360 Toolkit, IBM, https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/
[21]BOURTOULE, LUCAS, OTHERS,, Machine Unlearning, University of Toronto and Vector Institute, https://arxiv.org/pdf/1912.03817.pdf., 16 pages.; voir "Rapport MAIEI au CPVP".

Question 1: L'article 4 du *Règlement européen de protection des données4 (RGPD) présente la définition suivante du profilage.* D'après vous, est-ce que *cette définition est adéquate? Quels éléments devraient être retenus, retirés ou ajoutés?*

> **« *[...] 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* ».**

Réponse Courte:

La définition de profilage dans le RGPD nous paraît insuffisante. Nous proposons plutôt augmenter la LPRPSP en ajoutant les concept suivants, basés sur la proposition de la Commission:

- Une définition de "profil"
- Une définition d'activités existantes liées au RP telle que les activités de profilage, d'analyse, de prédiction et de décision
- Les conditions selon lesquelles ces activités sont permises, et non permises, selon les commentaires et les expectatives des citoyens québécois après consultation publique (voir. Déclaration de Montréal sur l'IA Responsable).

Liste de Recommandations:

0a) Viser non pas spécifiquement les "systèmes IA", mais plus largement les "systèmes", et selon nous de manière optimale en visant "les systèmes socio-techniques", afin de couvrir le spectre de différents systèmes, processus, et modèles de gouvernance le plus largement possible.

0b) Combiner une loi conservant la neutralité technologique en établissant une protection plus large qu'uniquement concentrée sur les systèmes socio-techniques, tout en établissant un Code pratique prescrit par Règlement pour mieux outiller et guider les entreprises et corporations concernées.

1-Définir les activités existantes, par exemples, le profilage, l'analyse, la prédiction, et la décision.

2-Établir la portée permise de ces activités, et les conditions applicables.

3-Lorsque possible, établir certains exemples non exhaustifs de comportements ou portée d'activités considérées non permises.

4-Établir une interdiction générale pour toute activité tombant hors la portée de ce qui est expressément identifiée à la loi, avec mécanisme d'autorisation par interprétation ou décision judiciaire, et directive par le régulateur compétent telle que approuvée par gouvernement

5-Établir certaines présomptions légales réfutables dans l'intérêt de l'individu (voir notre rapport au CVPC)

6-Renverser le fardeau de la preuve devant le régulateur et les tribunaux compétents.

Commentaires:

En premier lieu, il s'agit de considérer que la pratique de créer des profils sur des clients ou prospects et de prendre des décisions d'affaires ou autres sur la base de profils n'est pas nouvelle. Ce qui est nouveau est le niveau d'automatisation augmentée, c'est-à-dire, le fait que certains paramètres sont intégrés dans un système qui "lit" les RP du profil afin d'accélérer la prise de décisions ou la remise des résultats.

Afin de définir ce qu'est un profil, nous proposons de le faire le plus largement et libéral possible, au sens de la loi concernée, afin de prendre en compte "**l'effet mosaïque"**[22] de l'écosystème de données actuel, facilité notamment par "l'Internet des objets". Selon nous, la définition de profilage telle que proposée dans le RGDP demeure trop centralisée sur la confidentialité de l'identité d'un individu donné, et ne prend pas en compte ni les données "proxy"[23], ni les capacités techniques et de partenariats existantes qui permettent de créer des profils extrêmement intuitifs et une traçabilité directe ou indirecte à un individu, nonobstant le concept d'identification traditionnel utilisé de nos jours.

Nous proposons de passer d'une définition centrée sur l'idée traditionnelle de l'identité d'un individu à une définition acceptant qu'un attribut humain peut être suffisant afin de créer un profil pouvant servir à identifier un individu ou une catégorie d'individus, et d'en tirer des inférences, prédictions et décisions importantes et systémiques, qu'elles soient considérées acceptables, correctes ou erronées[24]. Ceci vient décentraliser l'importance de l'identification d'un individu dans la loi en matière de protection de la vie privée, et vient plutôt créer des fondations

[22]HUBER, Rose, "Mosaic Effect" Paints Vivid Pictures of Tech Users' Lives", https://wws.princeton.edu/news-and-events/news/item/mosaic-effect-paints-vivid-pictures-tech-users-lives-felten-tells-privacy
[23]FEDERAL TRADE COMMISSION, "Data Brokers: a Call for Transparency and Accountabliity", 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf
[24]RIBEIRO, Marco Tulio, OTHERS, "Why should I trust you?" Explaining the Predictions of any Classifier", https://arxiv.org/pdf/1602.04938v1.pdf

multiples incluant la protection du droit à la vie privée, le droit à l'autodétermination et le droit à la protection contre la discrimination illégale. Nous considérons que le fait de mettre en place uniquement des mesures ou techniques visant la protection ou l'élimination de l'identité de l'individu ne suffira pas à mitiger les autres risques à ces droits et libertés humains.

En d'autres mots, selon notre proposition, un profil[25] n'est pas défini par le fait qu'un individu est identifiable ou non, mais il est défini par l'exercice d'une entreprise de décrire un individu ou une catégorie d'individus sur la base d'attributs humains, ou en leur omission. Un individu peut aussi se voir attribuer plus d'un profils, qui peuvent avoir une incidence ou non sur lui dans le cadre des activités normales de l'entreprise.

Ainsi, les mécanismes, mesures de sauvegarde, techniques de dé-identification, et autres tests légaux existants associés à l'identification d'un individu demeurent pertinents, mais un profil donné évolue sur un spectre d'identification, et demeure une description pouvant affecter un individu ou une catégorie d'individus selon l'activité spécifique de l'entreprise utilisant ce ou ces profils, qu'ils soient entrés ("*input*") dans un système socio-technique ou non, et lorsque associés, corrélés ou liés à un individu spécifique.

Nous proposons aussi d'ajouter une autre activité aux trois qui ont été déjà été identifiés par la Commission, ce qui donne l'étendue complète suivante: 1) une activité de profilage; 2) une activité d'analyse; 3) une activité de prédiction; 4) une activité de décision.

Nous proposons que ces concepts soient présentés comme des modules fondés sur une approche "blocs de construction" (**"building blocks"**), selon le méta-modèle suivant, qui augmente le degré de protection et du caractère sophistiqué des mesures à prendre:

Niveau 0- Identification interne des informations pouvant établir un ou plusieurs profils lié à un individu sur la base de la définition légale

Niveau 1-Intention[26] ou exercice d'une activité de profilage

Niveau 2-Intention ou exercice d'une activité d'analyse

Niveau 3-Intention ou exercice d'une activité de prédiction

Niveau 4-Intention ou exercice d'une activité de décision

[25]Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/profile; Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/profile

[26]L'intention est incluse afin de s'assurer que les analyses préliminaires en matière de privacy by design et human rights by design soient prises au moment où les idées de prototypes ou de projets sont mis en oeuvre, et avant même que les prototypes soient initiés.

Nous proposons ci-dessous une approche de définitions de style "*common law"* selon différents concepts légaux que nous avons explorés. Un travail plus en profondeur afin de proposer une meilleure concision de ces définitions à des fins d'interprétation civile est suggérée. Les définitions proposées ci-dessous sont des projets plutôt que des versions finales, qui devront être prises selon le régime légal en place, et les particularités sémantiques, linguistiques, contextuelles et culturelles appropriées.

Définitions:

"Profil: Description, courte ou détaillée, sur quelque format, forme, méthode ou support que ce soit, de faits, de données, de caractéristiques, d'attributs ou de comportement humains, qu'ils soient pris isolément, collectivement ou catégorisés, augmentés ou non, incluant sans s'y limiter toute association, connection, corrélation, inférence, présomption, biais, point de vue, opinion, motifs, et modèle (*"pattern"*) récurrent ou non, entre ces faits, données, caractéristiques, attributs ou comportements, lorsque associés, liés ou attribués à un individu.

Une liste non exhaustive d'exemples de faits, données, caractéristiques et comportements humains, inclut, sans s'y limiter:

- La vie, le travail, l'historique, le caractère ou la personnalité d'un individu
- Ses origines et autres informations et données génétiques, médicales, ethniques, culturelles, démographiques et géographiques d'un individu
- Ses connections professionnelles, personnelles et sociales
- Ses moyens et son statut financiers, professionnelles, académiques, légaux, sociaux, personnelles, et familiaux
- Toute idée, et tout projet envisagé et/ou décision personnelle, professionnelle, et sociale, incluant sans s'y limiter tous historiques de recherche, de sélection, de défilement ("*scrolling*"), de visite, d'opinion (eg. "like") et de contenu personnel et transactions en ligne ou autre, et toutes transactions et toutes décisions portant sur sa santé, sa diète, ses activités, ses loisirs, et ses préférences personnelles, incluant son style, sa manière et sa méthode d'expression, sa culture, ses croyances et autres rituels sociaux ou activités de groupe, son orientation sexuelle, ses opinions politiques, scientifiques et sociales (**"décision autodéterminante"**)
- niveau de visibilité/présence ou d'invisibilité/absence public ou sur les médias publics, ou niveau d'attention publique ainsi niveau de vie privée et d'intimité (par exemple, un individu ne devrait pas être défavorisé au niveau du risque d'accès au crédit car il a pris une décision de ne pas être actif sur des plateformes de médias sociaux)[27].

[27]KLEINBERG, OTHERS, "Inherent Trade-Offs in the Fair Determination of Risk Scores", https://arxiv.org/abs/1609.05807; AI Fairness 360 Toolkit, IBM, https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/

- niveau de capacité et/ou de facultés cognitives ou d'intelligences, psychologiques, émotionnelles, rationnelles ou autre, standardisé selon des tests d'intelligence spécifiques ou reconnus (EQ, IQ, etc.), ou non-standardisé."

Note sur la protection de la décision autodéterminante ci-dessus:

La définition de profil et la liste des données personnelles doivent être rédigées de manière à s'assurer de protéger l'opportunité flexible et libre de l'apprentissage et de la croissance personnelle, évolutive, itérative et changeante d'un individu. Ceci comprend la considération du législateur de s'assurer de protéger le droit à l'erreur et à l'oubli de l'individu, car l'écosystème de données existant aujourd'hui permet en principe que toute décision, opinion et acte soit enregistrés à vie pour et contre un individu[28].

Là où la mémoire humaine ou communautaire oublie certains faits ou sujets concernant un individu avec le temps, lui permettant de progresser dans sa croissance personnelle et de lui permettre l'accès à certaines opportunités, l'écosystème en question peut effectivement "geler" cet accès à des opportunités de changements et de vie si certaines opinions et des informations sensibles demeurent accessibles en toute temps, aux employeurs et autres agences marketing ou de statut civil, par exemple. Un individu sera incapable de contrôler tous ces actes, faits et gestes enregistrables en tout temps.

Être "éternellement" défini par ses erreurs revient à restreindre son droit l'autodétermination et à ses libertés, en plus de certainement exacerber certains problèmes en matière de santé mentale, si l'individu doit constamment se sentir surveillé et ne peut être garanti une certaine part de liberté d'expression et d'être individuel sans en subir les conséquences."

"Profilage, et Activité de Profilage: acte pris dans le cours normal des affaires, qu'il ait été automatisé, augmenté* ou non, par lequel une entreprise a l'intention de procéder ou procède à l'association, la création, le montage, le traitement ou l'utilisation d'un ou de plusieurs profils à des fins spécifiques d'analyse, de prédiction, d'affaires, ou afin de prendre une décision de monter une stratégie concernant, dirigé vers, ou pouvant affecter un individu, ou une catégorie d'individus."

[28]Information Commissioner's Office, "Right to erasure", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/; THOMSON REUTERS LEGAL, "Right to Be Forgotten: Erasing Your Private Information from Cyberspace", https://legal.thomsonreuters.com/en/insights/articles/erasing-your-private-information-from-cyberspace; RFI, "French lawmakers vote for "right to make mistakes"" http://www.rfi.fr/en/france/20180124-french-lawmakers-vote-right-make-mistakes

"Analyse, et Activité d'analyse: acte pris dans le cours normal des affaires, qu'il ait été automatisé, augmenté ou non, par lequel une entreprise a l'intention de procéder ou procède à l'association, la création, le montage, le traitement ou l'utilisation d'un ou de plusieurs profils à des fins d'étude, de compréhension, de recherche et développement, et de stratégies ou de décisions d'affaires."

"Prédiction, et Activité de prédiction: acte pris dans le cours normal des affaires, qu'il ait été automatisé, augmenté ou non, par lequel une entreprise a l'intention de procéder ou procède à une connection, association, inférence, opinion, hypothèse, projection, corrélation ou modèle récurrent ou non, entre un ou plusieurs profils passés ou existant s d'un individu et un ou plusieurs de ses profils futurs ou scénarios personnels possibles, à des fins de profilage, d'analyse, ou de prises de décisions ou de stratégies d'affaires."

"Décision ou activité de décision: acte ou une omission d'agir dans le cours normal des affaires, automatisé, augmenté ou non, par lequel une entreprise a l'intention de procéder ou procède à prendre une décision ou une stratégie d'affaires pouvant concerner ou avoir une incidence ou un impact sur un individu ou une catégorie d'individus sur la base d'un profil."

Propositions de présomptions:

Considérant la position d'expertise et de contrôle de l'entreprise en défaveur de l'individu concerné dans les cadre des activités identifiées ci-dessus, en particulier concernant les systèmes socio-techniques, nous proposons différentes présomptions afin de rétablir l'équilibre des forces entre les parties.

Par exemple, là où l'individu n'a pas ou presque peu de visibilité sur le fonctionnement du cadre de gouvernance et des systèmes mis en place, il nous semble qu'établir certaines présomptions favoriserait une meilleure transparence et un plus grand dialogue entre l'entreprise et le public considérant sa culture corporative interne, sa responsabilité sociale, et la manière dans laquelle les RP des individus concernés sont gérés, utilisés et augmentés par l'entreprise dans le cours normal de ses affaires.

Afin de mitiger les risques de ré-identification dû à l'effet mosaïque[29], nous proposons une présomption réfutable à l'effet qu'une information est présumée pouvoir identifier et décrire un individu et dès lors devenir un profil de cet individu, sauf sur preuve suffisante du contraire, selon le point de vue objectif d'une personne moyenne et raisonnable placée dans les mêmes circonstances. Le point de vue subjectif de l'individu concerné peut aussi servir à établir la sensibilité et le caractère identifiable du profil et de l'information concernée. Enfin, un expert technique ou

[29]HUBER, Rose, "Mosaic Effect" Paints Vivid Pictures of Tech Users' Lives", https://wws.princeton.edu/news-and-events/news/item/mosaic-effect-paints-vivid-pictures-tech-users-lives-felten-tells-privacy

autre peut aussi donner son opinion sur le risque d'identification et d'association, comme moyen de preuve.

Présomption de profil: Toute information pouvant être associée à un fait, une donnée, une caractéristique, un attribut ou un comportement humain, est présumée définie comme pouvant établir un profil, et devient un profil dès qu'une description liée à un individu en est faite, sur quelque format, forme, méthode ou support que ce soit.

Présomption d'activité de prédiction: Tout acte ou décision qui n'est pas purement fondée sur une sélection ou une option aléatoire ou sur la chance est présumée être une intention de procéder à, ou une activité de prédiction, quelque soit le degré ou la probabilité d'exactitude, de précision ou de confiance de cette prédiction.

Présomption d'activités portant sur un individu identifiable: Les activités sont présumées ne pas avoir dé-identifié l'individu ou la catégorie d'individus concernée, à moins de transparence et de divulgation publique et contractuelle expresse à l'effet contraire de la part de l'entreprise assurant que:

1. des mesures organisationnelles et techniques appropriés et sécuritaires ont été mises en place,
2. l'entreprise reconnaît publiquement sa responsabilité civile dans les cas de manquements à une vérification diligente de ces systèmes socio-techniques, à un bris de confidentialité ou une déficience technique ou organisationnelle dans son cadre de gouvernance, pouvant causer un préjudice à un individu ou une catégorie d'individus, et
3. qu'outre les recours civils disponibles, des mécanismes privés de révision, de négociation, de médiation, de résolution et de compensation déployés par l'entreprise sont facilement disponibles et accessibles à l'individu concerné.

Présomption d'incidence ou d'impact: Toute activité de profilage, d'analyse et de décision est présumée pouvoir avoir une incidence ou un impact sur un individu ou une catégorie d'individu, à moins qu'il puisse être raisonnablement démontrée que ce n'est pas le cas.

Présomption d'illégalité: Toute autre fin ou activité qui ne semble pas explicitement et expressément identifiée ou permise par la présente loi est présumée interdite, sauf sur interprétation ou décision judiciaire par les tribunaux, ou sur directive du régulateur telle que 'approuvée par le gouvernement à l'effet contraire (afin de repousser expressément l'adage que ce que le législateur n'a pas expressément interdit est permis).

Positionnement sur les activités et fins permises et interdites:

Enfin, pour déterminer les activités et les fins pour lesquelles les systèmes socio-techniques devraient être permis et interdits, nous suggérons le législateur de formellement procéder à des consultations auprès du grand public, et non seulement des experts et des représentants de l'industrie, afin que les appréhensions, les réticences, les approbations et les propositions de celui-ci soient effectivement représentés, ou du moins pris en compte, lors de la rédaction de la loi amendée, afin de guider les entreprises développant et mettant en place ces systèmes, afin de rassurer le grand public du type de design et de déploiement de système autorisé dans leur écosystème civil et urbain, et de s'assurer d'une protection appropriée des individus concernés[30].

À cet effet, un des meilleurs exemples que nous pouvons proposer est le processus suivi afin de créer la Déclaration de Montréal sur l'IA Responsable. Le fédéral semble aussi avoir tenu des consultations, informelles toutefois, similaires dans le cadre de sa stratégie d'innovation auprès des Canadiens[31].

Bien qu'une loi spécifique peut servir de méta-cadre pour un ensemble d'individu, et ainsi proposer des exemples extrêmes et des règles claires aux cas et scénarios socio-techniques qui seraient expressément interdits à travers une province ou un pays, certaines nuances démographiques, culturelles et même spécifique à certaines industries, par exemple celui de la santé, devraient être pris en compte, et une certain degré de flexibilité devrait être alloué pour la diversification éthique et sociale de l'acceptabilité sociale de ces positions et scénarios technologiques, afin que ces positionnements puissent évoluer et transitionner efficacement selon le degré de confort, d'éducation et d'optimisme ou pessimisme d'un écosystème humain donné[32].

Conclusion:

Nous sommes d'accord avec la Commission de concentrer les amendements sur les systèmes plutôt que seulement l'IA, quoique nous proposons de viser les "systèmes socio-techniques" comme définition ou fondement à ces amendements, pour que tout le spectre de profilage, d'analyse, de prédiction et de décision soit compris, quelque soit le degré d'humanisation, d'automatisation et d'augmentation pris ou envisagé, selon une approche évolutive, et itérative.

---

[30]CONGER, Katie, *San Francisco Bans Facial Recognition Technology*, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html
[31]GOUVERNEMENT DU CANADA, "Rapport Ce que nous avons entendu", https://ouvert.canada.ca/fr/contenu/ce-que-nous-avons-entendu-rapport-sommaire
[32]COLIN, Harris, *Montreal grapples with privacy concerns as more Canadian police forces use facial recognition*, CBC News, https://www.cbc.ca/news/canada/montreal/facial-recognition-artificial-intelligence-montreal-privacy-police-law-enforcement-1.5239892

De cette manière, la loi générale peut conserver sa neutralité technologique, tout en proposant des prescriptions de certaines mesures et méthodes en établissant un Code Pratique prescrit par Règlement afin de mieux guider et outiller les entreprises et corporations concernées et visées par la loi.

Question 2: D'après vous, quelles pourraient être les conditions et obligations permettant et/ou encadrant les activités de profilage, d'analyse et de prédiction? Le consentement exprès d'une personne fait-il partie des conditions auxquelles ces renseignements pourraient être recueillis ou utilisés? Est-il une voie réaliste ou souhaitable?

Réponse Courte:

Oui, le consentement exprès devrait demeurer une des conditions préalables permettant ces activités, toutefois, il doit être supporté par d'autres mécanismes et mesures, notamment un cadre de gouvernance et certaines divulgations légales obligatoires.

Liste de recommandations:

1-Exiger une preuve démontrable que les protocoles, mécanismes et mesures imposées par la loi ont été prises, tout le long du cycle de vie des systèmes et tels que régulièrement et continuellement révisés durant le cours normal des affaires.

Note: Des certifications par des organismes de normalisation ("*standard-setting bodies"*) reconnus ou crédibles, ainsi que des systèmes d'audit externe par tierces parties expertes, neutres et indépendantes, pourraient servir comme début de preuve.

2-Proposer les impacts, fins et méthodes permises et non permises pour chaque activité le plus clairement possible.

Note: Donner des cas et des exemples non-exhaustifs concrets, et les mesures organisationnelles et techniques à mettre en place et à démontrer afin de mitiger le risque légal et réglementaire, ainsi qu'assurer une protection adéquate des individus concernées. (ie. *Analogie au Go/No Go Zones*).

3-Laisser une certaine latitude expressément dans la loi pour que les municipalités et communautés puissent décider eux-mêmes de certains positionnements pour et contre certaines activités ou technologies.

Note: Ces positions pourront être prises selon leurs propres attentes, expectatives, et degré de confiance envers les systèmes socio-techniques. En d'autres mots, la loi

spécifique pan-industrie devient un "méta-cadre" légal, permettant toutefois certains règlements, lois, ou décrets spécifiques à certaines cultures ou industries[33] (ie. *Analogie à la structure du régime légal portant sur le cannabis*).

4-Imposer l'adoption de mesure plus strictes quant aux garanties et contrôles à mettre en place pour assurer la continuité des affaires, en particulier dans les cas d'industries symbiotiques, et de partenariats d'affaires déterminés comme étant critiques, afin d'éviter un scénario "Trop connecté pour échouer" ("*Too connected to fail*") (Analogie au régime bancaire)[34]

5-**De manière générale, afin de régir les activités mentionnées ci-dessus, nous proposons de procéder à une évaluation pondérée en fonction des risques en fonction des mesures et contrôles suivants** ("*risk-weighted assessment*")(Analogie aux standards de Bâle pour l'analyse du capital réglementaire des banques systémiques)[35]:

- Implanter et contrôler la confidentialité au moment de la conception **("Privacy by design"[36])** avec l'approche de confidentialité par cas utilisés **("Used Case Privacy Approach")**
- Implanter et contrôler les droits et libertés humains au moment de la conception **("Human Rights by design"[37])**
- Implanter et contrôler l'approche de la pensée systémique **("Systems Thinking Approach"[38])**
- Identifier clairement les fins spécifiques prévues aux activités entreprises (en donnant des cas et scénarios récents de systèmes socio-techniques)

---

[33]COLIN, Harris, *Montreal grapples with privacy concerns as more Canadian police forces use facial recognition*, CBC News, https://www.cbc.ca/news/canada/montreal/facial-recognition-artificial-intelligence-montreal-privacy-police-law-enforcement-1.5239892; CONGER, Katie, *San Francisco Bans Facial Recognition Technology*, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

[34]ARNER, Douglas, OTHERS, *The Dark Side of Digital Financial Transformation: The New Risks of Fintech and the Rise of TechRisk*, University of Hong Kong Faculty of Law Research Paper No. 2019/112, 37 pages,p. 5.; FINANCIAL STABILITY BOARD, "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications", https://www.fsb.org/wp-content/uploads/P011117.pdf; SNYDER CARON, Mirka, "The Transformative Effect of AI on the Banking Industry", Banking & Finance Law Review, April 2019, 34 BFLR 79-345.

[35]FINANCIAL STABILITY BOARD, "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications", https://www.fsb.org/wp-content/uploads/P011117.pdf; SNYDER CARON, Mirka, "The Transformative Effect of AI on the Banking Industry", Banking & Finance Law Review, April 2019, 34 BFLR 79-345.

[36]Search Encrypt, Medium, "7 Principles of Privacy by Design", https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce

[37]ALLISON-HOPE, Dunston, BSR, "Human Rights by Design", https://www.bsr.org/en/our-insights/blog-view/human-rights-by-design; PENNEY, Jonathon, OTHERS, "Human Rights by Design", Schneier on Security, https://www.schneier.com/blog/archives/2018/12/human_rights_by.html;

[38]MEADOWS, Donella, "Thinking in Systems", https://books.google.co.in/books/about/Thinking_in_Systems.html?id=CpbLAgAAQBAJ&redir_esc=y

- Obtention du consentement au préalable de l'individu concerné pour:
    - la création et l'utilisation du ou des profils, sur la base d'une description sommaire de son contenu et du type de données liées
    - les activités prévues et leurs fins responsables spécifiques pour lesquelles ces RP sont collectés, utilisés, communiqués, inférés, traités ("*processed*"), et les options de consentements disponibles à l'individu
- Mécanismes de consentement et de refus subséquents facilement disponibles en tout temps pour toute nouvelle activité et fin spécifique, ainsi que pour toute nouvelle base de données ou sources de données ajoutées ou liées aux profils concernant l'individu
- Mécanismes de révision, de négociation, de correction, de médiation, de résolution, et de compensation privés disponibles à l'individu en tout temps
- Le caractère a) non abusif[39]; b) raisonnable[40] c) correct d) à jour; e) négociable[41] des résultats proposés ou soumis par ces activités, aux fins déterminées.

Note: **Les Recours civils demeurent disponibles:** Identifier expressément ceci dans la loi, sur le site web du régulateur, et comme divulgation obligatoire des entreprises, afin d'assister les individus dans l'identification de leurs recours en vertu de la loi spécifique, mais aussi en parallèle avec d'autres recours civils (eg. LPC, Code criminel). Ceci permettra aussi de contrer la défense pour "code complet" ("*complete code defence*")[42].

---

[39]**non abusif:** nous référons ici à une analogie au recours disponible notamment sous la loi québécoise portant sur la protection du consommateur, et proposons qu'un recours analogue soit proposé dans le cadre de l'utilisation de systèmes socio-techniques, *Loi sur la protection du consommateur, P-40.1, art. 8, 103.5.*

[40]KLEINBERG, OTHERS, "Inherent Trade-Offs in the Fair Determination of Risk Scores", https://arxiv.org/abs/1609.05807; AI Fairness 360 Toolkit, IBM, https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/

[41]**négociable**: Voir le droit à la négociation dans le Rapport MAIEI au CPVP. Ceci ne modifie pas la nature non-négociable d'un contrat en droit civil, mais vise uniquement le processus décisionnel, automatisé, augmenté ou non, qui a été pris pour ou à l'encontre d'un individu ou d'une catégorie d'individus concernés. Ceci devrait être expressément mentionné dans la loi.

[42]Dixon, Brad, Maniago, Michelle, "*BCCA Restricts Ability of Non-Injured Plaintiffs to Claim Under the Business Practices and Consumer Protection Act*", http://blg.com/en/News-And-Publications/Publication_3634?sd=; *Low* v. *Pfizer Canada Inc.*, 2015 BCCA 506, p. 2;; *TELUS Communications Co. v. Rogers Communications Inc.*, 2009 BCCA 581 (CanLII);; *Koubi v. Mazda Canada*, 2012 BCCA 310.; *Tucci* v *Peoples Trust Company*, 2017 BCSC 1525 (CanLII);; *Wakelam* v. *Wyeth Consumer Healthcare/Wyeth Soins de Sante Inc*. 2014 BCCA 36, par. 82, 90 Supreme Court denied leave Sept 4. 2014, https://www.lexology.com/library/detail.aspx?g=0fe90893-c537-4355-8631-49652d6eabc3 (visited May 2, 2018); *Watson* v. *Bank of America*, 2015 BCCA 362, par. 172; Osborne, W., "Is the Competition Act a "Complete Code"?Courts Debate Whether Breaches of the Competition Act Can Support Common Law Claims", http://canliiconnects.org/en/commentaries/39082; Therien, Shawn, ""Complete Code" Argument Continues to be a Powerful Defence in Consumer Class Actions", https://www.lexology.com/library/detail.aspx?g=4d6a95a6-5f10-4e0d-a816-ea92155c6bd5.

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

Réponse courte:

Oui, mais il faut s'assurer de rendre le tout efficace en pratique en combinant avec certaines positions ou exemples clairs ainsi que des "outils" en preuve ou en procédure concrets, à défaut de quoi cette mention dans la loi demeurera théorique, voir Commentaires, et nos propos sous la Question 3 ci-dessous.

Commentaires:

Telle que rédigée, la proposition est selon nous peu utile. Il est implicite, dans l'écosystème légal et réglementaire québécois, qu'une fin illégitime ou avec une intention malveillante serait du moins *prima facie* illégale et donc pourrait donner accès aux recours civils et criminels déjà existants.

Il est déjà présumé connu que la tromperie au niveau des pratiques en marketing, de la description d'un produit ou service, ou d'une relation contractuelle, ou la discrimination illégale, ou le fait de causer un préjudice sur la base contractuelle ou extracontractuelle, est susceptible de donner accès à un recours civils, administratifs ou criminels **(nul ne peut ignorer la loi)**. Confirmer ceci peut venir rassurer l'individu concerné, et effectivement, des lignes directrices ou des exemples clairs de responsabilité potentielle sous les différentes lois spécifiques pourraient mieux assister les entreprises à s'assurer de demeurer responsables et à éviter la non conformité ou l'illégalité.

Ce qu'il faudra pour appuyer ces concepts seront des exemples clairs et concrets, ou des positions dans la loi, de ce qui est considéré illégitime ou malveillant, avec un cas ou scénario passé ou présent, selon les développements technologiques en cours, à réviser périodiquement sur la base de futurs développements dans les différentes industries, pour bien encadrer les risques.

Question 3: Les concepts de « fins illégitimes » et d'« intentions malveillantes » sont subjectifs. Avez-vous d'autres propositions permettant d'atteindre l'objectif de ce principe ou ces concepts permettraient d'assurer une limitation acceptable de l'utilisation des SIA?

Réponse Courte:

Ces concepts peuvent devenir utiles en les combinant avec certaines positions ou exemples clairs ainsi que des "outils" en preuve ou en procédure concrets, à défaut de quoi cette mention dans la loi demeurera théorique.

Liste de recommandations:

1. Augmenter les concepts de "fins illégitimes" et "d'intentions malveillantes" avec des exemples clairs de ce qui est permis et non permis (Go/No Go Zones), alignés avec les cas et scénarios d'aujourd'hui, ou expressément déléguer ce positionnement aux autorités municipales ou communautaires compétences.

2. Proposer une approche par "liste de contrôle" ("checklist") pour les entreprises fin d'encadrer le "design" du système socio-technique socialement responsable, et afin de s'assurer que le développement et déploiement demeurent alignés avec ceux-ci, ces critères en 4 blocs modulables étant les suivants:

A. **Une fin perçue comme étant socialement acceptable, par l'entremise…**
B. **D'une méthode sécuritaire et responsable, avec…**
C. **Une conscience sociale quant au niveau de risque projeté ou existant, pour…**
D. **Un résultat socialement bénéfique[43].**

3. Augmenter la protection associée au concept "d'intentions malveillantes" en ajoutant expressément les cas de "négligence grossière" et de "mépris manifeste".

4. Établir une présomption réfutable à l'effet que si le cas, scénario, ou système socio-technique ne cadre pas avec la liste de contrôle ci-dessus et les exemples clairs qui ont été donnés, il s'agit d'un début de preuve à l'effet

[43]Voir GUPTA, Abhishek, SNYDER CARON, Mirka, "The social contract for AI", IJCAI AI for Social Good Workshop 2019, Abstract, 7 pages.

que le système a été déployé à des "fins illégitimes", ou "avec négligence grossière" ou avec "mépris manifeste".

5. En parallèle à 4, implanter un système d'approbation préalable au moment du "design" avec la Commission pour les cas où les entreprises sont incertaines.

7. Identifier "les fins illégitimes", la "négligence grossière" et le "mépris manifeste" comme des facteurs aggravants au moment de déterminer le montant des dommages punitifs ou la gravité des sanctions administratives à imposer.

8. Les propositions ci-dessus ne devraient pas être limités aux systèmes socio-techniques, mais aussi à toute violation des obligations liées à la collecte, l'utilisation, la communication et la conservation des RP.

Commentaires:

Les concepts de "fins illégitimes" et "d'intentions malveillantes" nous paraissent soient inutiles, car l'interdiction des fins illégales ou criminelles sont implicites, soient nébuleux. La seule manière par laquelle ces concepts pourront assurer une efficace pratique est d'identifier des zones claires de ce qui est permis et non permis ("*Go/No Go Zones*") en se basant sur des cas ou scénarios alignés aux développements récents, puis de réviser et amender ceux-ci régulièrement lorsque nécessaire. Ceci pourrait requérir un positionnement du législateur sur certains types, méthodes ou fins de systèmes socio-techniques, ou une délégation expresse aux autorités locales, municipales ou communautaires désignées compétentes, afin qu'un écosystème urbain et civil reflète les attentes et les valeurs des individus spécifiques à celui-ci[44].

Note 1: Pour le test proposé au #2 ci-dessus, nous proposons que les critères A et C demeurent non négociables, et que les critères B et D suivent une échelle ou une approche par évaluation pondérée en fonction des risques ("*risk-weighted assessment*").

Pour B, l'idéal serait d'identifier les standards minimums ou des lignes directrices pratiques à rencontrer afin qu'un modèle organisationnelle et technique soient considéré conforme, sécuritaire et responsable[45]. Garder en tête à la fois les micro-entreprises locales et les multinationales sophistiquées afin de considérer le

[44]Voir les commentaires de nos Montréalais durant les sessions MAIEI, tels que soumis dans l'Annexe 1 du Rapport MAIEI au CPVP.
[45]GUPTA, Abhishek, SNYDER CARON, Mirka, "Response to the AHRC and WEF regarding Responsible Innovation in AI", Montreal AI Ethics Institute, 25 pages.

fardeau financier. Cette évaluation devrait être tenue au moment du design et de la manufacture du système socio-technique, avant l'entrée sur le marché.

Pour D, nous proposons que le standard minimum est un résultat "neutre", c'est-à-dire que ce système n'a pas d'impact socialement bénéfique, mais du moins n'a pas d'impact social négatif. (eg. automatisation de certains processus internes non-décisionnels à des fins de réduction en temps)

Note 2: Toujours pour le test proposé au #2 ci-dessus, pour A, à la fois l'apparence ou la perception d'être socialement acceptable est considérée aussi importante que l'application concrète, nous tirons l'analogie de l'apparence de conflits d'intérêts comme norme pour les avocats ou les directeurs de corporation. Si l'entreprise n'a pas réussi à donner à son système l'apparence que c'est socialement accepté, alors elle ne rencontre pas le critère. Ceci s'associe aux principes de transparence, de divulgation publique, et d'éducation du public, et promeut l'importance de s'assurer de mettre les efforts nécessaires afin d'assurer la confiance du public et d'éviter de le tromper.

<u>Propositions CAIQ 4 à 10</u>:

> 4. Les entreprises et les organismes publics devraient obligatoirement divulguer l'utilisation d'un SIA, dès lors qu'une personne entre en interaction directe 114 avec celui-ci, au moment d'une collecte de renseignements personnels ou dans le cadre d'une prestation de services;
>
> 5. Une personne devrait être informée, au moment d'une collecte de renseignements personnels, que d'autres renseignements seront inférés de manière automatique à son sujet, que les données serviront à des activités de profilage, d'analyse ou de prédiction ou qu'une décision sera prise automatiquement à partir des informations qu'elle fournit;
>
> 6. Une personne doit pouvoir exiger obtenir une explication des facteurs et des paramètres les plus importants ayant mené à la prise d'une décision et de la logique du mécanisme de traitement automatisé utilisé pour la prendre, ainsi que de la liste des renseignements personnels utilisés;
>
> 7. Le cadre de gouvernance d'une entreprise ou d'une organisation qui utilise un SIA (voir principe 11) devrait être accessible pour qui en fait la demande, ou devrait être diffusé de façon proactive.
>
> 8. Prévoir le droit d'exiger une révision par une personne physique d'une décision prise initialement par un SIA.

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

10. Le droit à la rectification d'un renseignement inféré ne devrait pas inclure une obligation pour la personne concernée de démontrer son caractère inexact, incomplet ou équivoque; ou un recours plus spécifique à la nature de ce type de renseignement devrait être prévu, soit le droit de modifier l'inférence, l'opinion, le jugement ou la 161 qualification réalisés par un système automatisé.

Réponses courtes MAIEI:

Oui à toutes.

<u>Proposition CAIQ 11:</u>

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

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

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

Réponse Courte MAIEI:

Oui.

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

Réponse courte:

Oui, une évaluation devrait être imposée, mais la portée du EFVP nous semble trop étroite, si elle se concentre principalement et uniquement sur le droit à la vie privée.

Il faudrait aussi imposer l'implantation d'une vérification diligente des risques sur les droits et libertés de l'humain, incluant le droit à la vie privée ("*Human Rights Due Diligence*")[46], ainsi que incorporer une vérification du caractère responsable des activités et des fins spécifiques prévue[47]**.**

Liste de recommandations:

1. **Proposer plutôt une *évaluation des risques individuels et sociaux* (ERIS) pour tous les systèmes socio-techniques, automatisé, augmenté, ou non.**
2. **S'assurer que tous les droits et les libertés fondamentales sont pris et pesés en compte dans la balance, sans nécessairement isoler le droit à la vie privée. (*Nous comprenons toutefois qu'il pourrait y avoir des limites de portée de la loi spécifique, et de juridiction du régulateur concerné)[48].**
3. **Nous proposons qu'ERIS devrait au moins inclure:**
    1. **Une évaluation des processus et risques établis selon le Privacy by Design[49]**

[46]Office of the High Commissioner for Human Rights, United Nations, UN Guiding Principles for Businesses and Human Rights, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[47]*The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems,*https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf; Voir GUPTA, Abhishek, SNYDER CARON, Mirka, "The social contract for AI", IJCAI AI for Social Good Workshop 2019, Abstract, 7 pages.

[48]GUPTA, Abhishek, SNYDER CARON, Mirka, "Response to the AHRC and WEF regarding Responsible Innovation in AI", Montreal AI Ethics Institute, 25 pages.

[49]CAVOUKIAN, "Privacy by Design: Foundational Principles", https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf; Search Encrypt, Medium, "7 Principles of Privacy by Design", https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce

2. **Une évaluation des processus et risques établis selon le Human Rights by Design[50]**
3. **Une obligation de procéder à un Human Rights Due Diligence[51] pour chaque nouveau projet (une même catégorie de projets avec des paramètres, algorithmes, et données identiques pourrait suffire), à toutes les étapes du cycle de vie: Design, Développement, Déploiement, Destruction (Modèle 4D)**
4. **Analogue à 3, une obligation de procéder à une vérification diligente de la confidentialité des données et du respect à la vie privée ("Privacy Due Diligence.)**

Question 4: L'EFVP contient généralement : une description de la mise en oeuvre d'un système ou d'un processus, une analyse du cycle de vie du renseignement personnel, une vérification de la conformité aux lois de protection de renseignements personnels et une évaluation et une gestion des risques à la vie privée que cette mise en oeuvre suscite. D'après vous, est-ce que des tests particuliers (ex. processus de certification) ou des processus d'évaluation supplémentaire (ex. comité d'éthique) devraient faire également partie de l'EFVP, plus généralement, d'un cadre de gouvernance des SIA?

Réponse courte MAIEI:

Oui. Ces solutions techniques et organisationnelles incluant les certifications par des organisations normatives reconnues ou crédibles[52], des audits internes et externes indépendantes ou des comités d'évaluation, devraient être encouragés et peuvent servir de début de preuve à l'effet que le cadre de gouvernance semble appropriée et responsable, mais ne devrait pas être imposés dans un format spécifique car, prises isolément, ces solutions ont différentes limitations et certains défis structurels.

La flexibilité et une certaine autonomie dans les options de structurer ce type de solutions devraient être expressément permise dans la loi, pour ne pas restreindre

[50]ALLISON-HOPE, Dunston, BSR, "Human Rights by Design", https://www.bsr.org/en/our-insights/blog-view/human-rights-by-design; PENNEY, Jonathon, OTHERS, "Human Rights by Design", Schneier on Security, https://www.schneier.com/blog/archives/2018/12/human_rights_by.html;

[51]Office of the High Commissioner for Human Rights, United Nations, UN Guiding Principles for Businesses and Human Rights, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf; *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems,*https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf

[52]OECD Legal Instruments, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

certains modèles d'affaires ou indûment créer des fardeaux sur les entreprises, que celles-ci soient des microentreprises ou des multinationales systémiques.

Liste de recommandations:

1. **Désigner le Data Privacy Officer (DPO) en augmentant son mandat, ou, de manière optimale, appuyer celui-ci en désignant une seconde personne, soit un Responsible Systems Officer (RSO), afin qu'un humain demeure désigné responsable devant le public pour une entreprise donnée.**
2. **Le DPO et RSO devraient être pourvus de l'autorité, des outils, du budget et des ressources nécessaires afin de pouvoir concrètement guider et déployer le cadre de gouvernance, en collaboration avec les lignes d'affaires concernées par un projet ou une catégorie de projets.**

Note: Ni le DPO ni le RSO Il ne doit pas être un "jeton humain" ("*token human*")[53]. Ils doivent pouvoir être tenus personnellement responsables dans les cas clairs d'avoir approuvé un projet à des fins illégitimes, ou avec des intentions malveillantes, ou démontrant un comportement de négligence grossière ou de mépris manifeste aux conséquences et impacts causés par ces systèmes. Les mécanismes de sauvegarde, d'assurance professionnelle, et de défense standards à ce type de responsabilité devraient être expressément indiqués dans la loi.

3. **Le Conseil d'administration devrait être tenu régulièrement au courant des développements des systèmes socio-techniques et des impacts en cours, et devrait pouvoir être tenus personnellement responsables dans les cas clairs d'avoir approuvé un projet à des fins illégitimes, ou avec des intentions malveillantes, ou démontrant un comportement de négligence grossière ou de mépris manifeste aux conséquences et impacts causés par ces systèmes. Les mécanismes de sauvegarde, d'assurance professionnelle, et de défense standards à ce type de responsabilité devraient être expressément indiqués dans la loi.**
4. **Les certifications et autres groupes de vérification, ou d'audits de contrôle devraient être encouragés, mais non imposés, vu les limites pratiques associées à ces certifications et à ces audits, ainsi que la prise en considération de l'évolution des développements techniques et technologiques, ainsi que respecter la diversité des différents modèles d'affaires existants.**

[53]Voir RGPD.

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

Réponse courte: Oui.

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

Réponse courte: Oui.

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

Réponse courte:

L'utilité de la déclaration des incidents de sécurité sous le régime de la Directive ayant précédé le RGPD dans l'Union Européenne (UE) a été considérée négligeable. Cette mesure n'a pas autrement augmenté le degré de protection de la vie privée des individus concernés. Sur ce, le RGPD a restreint la déclaration obligatoire aux bris ayant un impact "significatif".

S'il doit y avoir une obligation de déclarer des incidents, pour des raisons d'adéquation avec le régime UE, nous proposons que cette obligation soit restreinte de manière analogue.

Commentaires:

Dans le cas d'une déclaration obligatoire imposée aux entreprises, nous proposons que cette obligation de déclaration soit restreinte aux "**incidents de nature systémique ou significative, qui pourraient affecter ou qui ont affecté de manière grave ou sévère les droits et les libertés d'un individu, incluant le droit à la vie privée.**"

Incident de nature systémique: Nous proposons que cet incident soit interprété de manière à inclure les cas affectant plus d'un individu, soit par exemple une catégorie d'individus dans un cas de biais menant à une discrimination illégale, ou à un bris de cybersécurité affectant un grand volume de profils d'individus avec des informations hautement sensibles.

Incident de nature significative: Nous proposons que cet incident soit interprété différemment d'un incident systémique, et peut inclure un cas individual où l'impact pourrait être ou a été particulièrement grave ou sévère envers cet individu.

Nous pensons par exemple à un cas de refus d'accès illégale à l'entrée d'un pays sur la base d'une décision automatisée, ou un cas d'une demande d'un pays étranger pour l'envoi d'un individu dans le cadre de procédures criminelles pouvant mener à une peine de mort ou à une peine criminelle considérée grave.

Nous pensons aussi aux prises de décisions judiciaires prises concernant la remise en liberté, ou l'inférence automatisation de la propension d'un individu à la récidive, telles que fondées ou supportées par des systèmes socio-techniques utilisant des bases de données à haut potentiel de biais illégalement discriminatoires[54].

Nous pensons aussi par exemple à un cas où un individu est incorrectement identifié comme étant un fraudeur sur une liste ou une base de données de "personnes indésirables" ou considérées "à haut risque" partagée à travers une ou plusieurs industries, bloquant alors effectivement toute opportunité civil ou légal sur la base de ce statut civil.

Manière grave ou sévère: Un positionnement clair par le législateurs de certains cas serait optimal, toutefois, nous proposons que ceci soit interprété selon le degré de sensibilité des RP en cause, ainsi que du degré d'impact sur un individu ou sur une collectivité. Ce dernier point peut se baser sur les interprétations soumises dans les décisions judiciaires et administratives antécédentes en matières de droit à la vie privée et des droits et libertés de l'humain, avec les adaptations nécessaires, sur la base du principe de la neutralité technologique.

Exigences d'implantation de mécanismes privés:

Nous proposons aussi en parallèle ou indépendamment de cette déclaration obligatoire une exigence à l'effet que pour les cas individuels, les entreprises devront mettre en place un cadre de gouvernance, de résolution et de compensation privés, que ce soit par la mise en place d'une division distincte ou dans le cadre générale du protocole de gestion de plaintes de la clientèle (nous considérons que le renvoi à un ombudsman reconnu est inclus et suffisant). Ces mécanismes devront inclure les suivants:

1. Mécanisme de prévention dans le cadre de gouvernance des systèmes socio-techniques
2. Mécanisme de réduction et d'élimination ("*mitigation*") des risques
3. Mécanisme de médiation et de résolution des cas individuels affectés

[54]RIBEIRO, Marco Tulio, OTHERS, "Why should I trust you?" Explaining the Predictions of any Classifier", https://arxiv.org/pdf/1602.04938v1.pdf

4. Mécanismes de compensation aux individus affectés

Note: Certaines considérations liés aux assurances et aux **protocoles de continuité des affaires** devraient être explorées plus en profondeurs[55].

Nuances liées à la déclaration obligatoire des incidents de sécurité au régulateur:

Bien que le mécanisme de déclaration obligatoire auprès du régulateur soit devenu de plus en plus populaire dans différents régimes de droit et plusieurs juridictions, nous avons certaines réserves à partager à cet effet. Nous percevons ce type de mécanisme comme étant un pansement ("*band-aid solution*") au problème inhérent qui est le manque de pouvoirs et de capacités budgétaire, technique ou organisationnelle de certains régulateurs[56].

Sous la Directive de l'UE ayant précédé le RGPD, l'obligation de déclaration incluait tous les incidents de sécurité, quelque soit le degré de sensibilité des RP ou de la gravité de l'impact.

Les statistiques semblent avoir démontré peu de plus-value ou une amélioration négligeable du degré de protection aux individus sur la base de cette déclaration systématique. Ce fut une des raisons ayant mené à la restriction de la déclaration obligatoire aux seuls incidents significatifs sous le RGPD, tels que définis par la loi[57].

Par contre, il est à noter qu'en pratique, si les entreprises ont l'option d'identifier, sur la base de la définition légale, les incidents qui sont interprétés comme étant significatifs ou non, il est à envisager que plusieurs efforts internes pourraient être déployés afin d'exclure un cas de la catégorie "significative", afin d'éviter de soumettre une telle déclaration, surtout si cette déclaration mène automatiquement au déclenchement d'un recours quasi-judiciaire ou à une sanction administrative pécuniaire ou autre importante.

De plus, il est supposé avoir des distinctions légales importantes entre les sanctions administratives, et les sanctions pénales et criminelles, notamment au niveau 1) du fardeau de la preuve passant de la "prépondérance des probabilités", à une preuve "hors de tout doute raisonnable"; 2) la nature administrative versus la nature pénale ou criminelle des sanctions disponibles; et 3) le type d'objectifs visés par ces sanctions, passant d'une sanction liée à une non-conformité à la loi, à une punition et à faire d'un individu ou d'une entreprise un exemple à ne pas faire ("deterrence"), entre autres.

---

[55]SNYDER CARON, Mirka, "The Transformative Effect of AI on the Banking Industry", Banking & Finance Law Review, April 2019, 34 BFLR 79-345.
[56]GUPTA, Abhishek, SNYDER CARON, Mirka, "Response to the AHRC and WEF regarding Responsible Innovation in AI", Montreal AI Ethics Institute, 25 pages.
[57]Voir préambule RGPD.

Au Canada, il nous semble qu'en pratique la distinction a peu à peu perdu de ses distinctions, ce qui nous semble un risque potentiellement important en termes du degré de protection procédurale à mettre en place dans une société démocratique prônant une indépendance et neutralité judiciaire, particulièrement dans un contexte ou une grande déférence judiciaire est démontrée de la part des cours supérieures envers les tribunaux administratifs et certains régulateurs, lorsque comparée à la flexibilité procédurale, semi-indépendante et dans certains cas quasi-judiciaires des instances de certains régulateurs chapeautant à la fois une division d'enquête, et une division analogue à un tribunal administratif[58].

Par contre, la Cour de Justice de l'Union Européenne s'est déjà prononcée à l'effet que sous certaines lois, la sévérité des sanctions disponibles, même si définies dans la loi comme étant de nature administrative, les a rendues analogues ou équivalentes à des sanctions de nature pénale et criminelle, requérant un haut degré de protection procédurale, incluant certaines mesures de sauvegarde à garantir afin de protéger le principe "*Ne bis in idem*"[59].

Un renversement du droit canadien dans ce domaine de droit n'est pas improbable, si les amendements des lois continuent de renforcer le mandat, les pouvoirs et les compétences quasi-judiciaires des régulateurs. Sous ce scénario, exiger une déclaration obligatoire pourrait un jour aller à l'encontre du principe de la présomption d'innocence, et le droit au silence dans un contexte criminel. Du moins, certains arguments constitutionnels visant ces protections procédurales ou la compétence du régulateur pourraient être soulevés.

Nous suggérons que le régulateur concerné explore certaines protections qui seraient mises à la disposition des entreprises lorsque celles-ci prennent l'initiative de collaborer et de coopérer avec le régulateur en faisant volontairement une telle déclaration, soit peut-être par exemple:

1) une période d'immunité et un anonymat temporaires afin de résoudre le risque ou l'Impact systémique le plus rapidement possible avec le régulateur comme

---

[58] *Banque Internationale de Commerce Mega (Canada)* c. *Procureur général du Canada* (2012 FC 407); *Banque MBNA Canada* c. *Canada (Commissaire, Agence de la consommation en matière financière)* (2004 CF 1665); *Martineau c Canada (Ministre du Revenu national)*, 2004 CSC 81, par. 24, [2004] 3 RCS 737.

[59] European Court of Human Rights, "Factsheet – Non Bis In Idem", April 2018, https://www.echr.coe.int/Documents/FS_Non_bis_in_idem_ENG.pdf; Cases C-596/16 and C-597/16, *Enzo Di Puma* v *Commissione Nazionale per le Società e la Borsa*, (2018), EU:C:2018:192, par. 88-89 ("Puma"); Case C-537/16; Garlsson Real Estate SA v Commissione Nazionale per le Società e la Borsa, EU:C:2018:193, par. 88, *Engel and Other*s v *The Netherlands*, ECHR 8 June 1976, (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72), http://www.worldlii.org/eu/cases/ECHR/1976/3.html; Case C-128/04 Raemdock, (2005), 2005 I-02445; Case C-489/10, Bonda (2012), EU:C:2012:319 Case C-617/10 Åkerberg Fransson (2013), EU:C:2013:105.

intermédiaire interventionniste et actif, notamment dans les cas sans frontières, afin de notifier et d'obtenir la coopération des régulateurs à l'étranger (Note: l'anonymat demeurant disponible à la discrétion du régulateur uniquement dans les cas ou la notification au public n'est pas considérée une mesure optimale afin de résoudre le problème);

2) une fois la période expirée, selon la gravité du cas, la diligence de l'entreprise concernée et les mesures qui ont été prises en temps opportun, incluant les mécanismes de médiation, résolution et de compensations privés en place, déterminer selon des critères équitables, publics et transparents s'il serait de l'intérêt du public que le processus de sanctions administratives, pénales ou criminelles soit amorcé; et

3) si oui, considérer donner un poids important dans la déclaration volontaire faite par l'entreprise et son niveau de diligence, de bonne foi, et de coopération, dans l'évaluation du montant ou de la nature de la peine ou de la sanction administrative, comme facteur de réduction.

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

Réponse courte:

Oui, elles devraient pouvoir obtenir l'accès au code des algorithmes et aux systèmes socio-techniques sur demande, que ce soit dans le cadre de leur inspection proactive ou de leur enquête, et aussi durant le recours administratif s'il y a lieu, sujet à certaines mesures de sauvegarde.

Mais le régulateur concerné devrait aussi s'assurer d'avoir la compétence et l'expertise technique nécessaires, ainsi que les outils technologiques, augmentés ou non, appropriés, afin de s'assurer d'un audit et d'un contrôle efficace[60].

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

Réponse courte:

Oui.

[60]GUPTA, Abhishek, SNYDER CARON, Mirka, "Response to the AHRC and WEF regarding Responsible Innovation in AI", Montreal AI Ethics Institute, 25 pages.

Question 5: Comment traduire le principe de limitation de la collecte dans le contexte de l'utilisation d'un SIA?

Réponse Courte:

La portée du principe de limitation de la collecte ne prend suffisamment en considération les inférences qui sont faites ou créées suite à l'entrée des données collectées dans un système socio-technique, en particulier lorsqu'il s'agit de la collecte de tendances ("trends") ou de l'effet mosaïque[61]. Ceci pourrait affecter l'efficacité de ce principe.

Il devrait être supporté par des approches fondées sur la confidentialité selon des cas d'utilisation ("*use-based privacy*")[62], et de la pensée systémique ("s*ystems thinking*)[63].

Commentaires[64]:

En pratique, pour les systèmes socio-techniques, le principe de limitation de la collecte est difficile, mais pas impossible. les systèmes avec algorithmes d'apprentissage ("*Machine Learning* **(ML)**") requièrent des quantités importantes de nouvelles données pour continuer à être améliorés. Ces systèmes n'apprennent pas de la même manière que des humains.

Toutefois, il existe des méthodes et des techniques par laquelle les données peuvent relativement être dé-sensibilisées ou converties en données neutres, qui pourraient ensuite être entrées dans le système IA. Certains diront que nettoyer les données d'une manière à les anonymiser pourrait négativement impacter l'authenticité et l'exactitude de la donnée d'origine, mais il devrait être possible de minimiser la quantité et la sensibilité des RP à ce qui est strictement nécessaire pour fins spécifiques d'affaires identifiées pour proposer des produits ou services, et ensuite donner l'option à l'individu concerné d'augmenter le niveau de personnalisation du résultat sur la base de son consentement.

Ce ne sont pas tous les systèmes IA qui génèrent nécessairement une plus-value à une entreprise ou à la société, et il en va de même quant au niveau ou degré de personnalisation du résultat produit par le système socio-technique, car il peut être

[61]HUBER, Rose, "Mosaic Effect" Paints Vivid Pictures of Tech Users' Lives", https://wws.princeton.edu/news-and-events/news/item/mosaic-effect-paints-vivid-pictures-tech-users-lives-felten-tells-privacy
[62]BAGDASARYAN, OTHERS, "Ancile: Enhancing Privacy for Ubiquitous Computing with Used-Based Privacy", Cornell University, 2019, http://www.cs.cornell.edu/~jnfoster/papers/ancile.pdf
[63]MEADOWS, Donella, "Thinking in Systems", https://books.google.co.in/books/about/Thinking_in_Systems.html?id=CpbLAgAAQBAJ&redir_esc=y
[64]Voir Rapport MAIEI au CPVP, p. 34-36.

difficile de quantifier la valeur qualitative et quantitative exacte à la mise en place de ce processus ou mécanisme automatisé ou augmenté.

Un aspect qui n'est pas expressément couvert par le principe de minimisation de la collecte des donnée est le rôle des "*data proxies*" qui peuvent se retrouver l'extérieur de la portée du principe d'identification des fins et pourraient causer certains problèmes[65].

De plus, des données qui ne sont pas collectées auprès de l'individu comme source de ces données, et qui pourraient dès lors se retrouver à l'extérieur de la portée légale de ces deux principes, par exemple, les cas d'utilisation de bases de données colligées par des "courtiers en données"[66] qui opèrent en pratique à l'extérieur du régime de la loi concernée, ne semblent pas suffisamment pris en considération de manière expresse dans la loi, malgré l'interprétation large et libérale attribuée à un renseignement personnel et aux lignes directrices et autres commentaires indiquées par la CAIQ.

Un commentaire similaire concerne les "nouvelles" données créées ou inférées par un système socio-technique basées sur des RP sur un individu concerné. Certains arguments ont été soumis à l'effet que des techniques de dé-identification des RP pourraient exclure l'application du principe de minimisation des données.

Par contre, il y a tellement d'exemples récents démontrant que la dé-identification, prise isolément et sans autres combinaisons techniques ou organisationnelles, paraît grossièrement inadéquate comme mesures de protection de la vie privée.

Afin de contrer l'argument à l'effet que limiter la collecte de RP réduirait la qualité des inférences et des résultats obtenus de systèmes socio-techniques, nous soumettons que ce n'est pas nécessairement le cas. En particulier, la méthode du "*transfer learning*" peut permettre l'apprentissage sur des données non sensibles ou publiques[67].

Par exemple, il est possible d'entraîner et de tester un modèle sur des données concernant des individus qui sont décédés et qui raisonnablement ne subiront pas de préjudice causé par ou lié à l'utilisation de ces données. Ceci requiert des périodes d'expiration légalement imposées, qui sont déjà présentes, par lesquelles les données sont assumées avoir rejoint le domain public, sujet aux types de données spécifiques, comme les données génétiques, ou des données liés à la santé d'un individu potentiellement héréditaires, qui pourraient conserver une

[65]FEDERAL TRADE COMMISSION, "Data Brokers: a Call for Transparency and Accountabliity", 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; voir Rapport MAIEI au CPVP.
[66]Id.
[67]Voir Rapport MAIEI au CPVP, p. 34-36.

certaine pertinence et un potentiel de préjudice aux individus descendants ou autres que ceux qui sont décédés.

Un exemple de bases de données acceptables est par exemple l'apprentissage d'un modèle utilisant ImageNet afin d'identifier les caractéristiques de base de larges catégories d'objets. Ensuite, ce modèle pré-entraîné peut être utilisé sur des tâches spécifiques en améliorant le modèle.

Un autre exemple est "*large scale language models*" comme GPT2[68], qui peut capturer les bases des sémantiques du langage et la grammaire, et qui peut ensuite être amélioré pour tâches liées à des domaines spécifiques.

Finalement, les deux principes peuvent être augmentés en intégrant une approche de la pensée systémique ("*systems thinking approach*"[69]), par laquelle les différents acteurs et personnes concernées (stakeholders), ainsi que les répercussions potentielles ("*externalities*") peuvent être identifiés, et ceci peut enrichir l'analyse et le degré d'efficacité.

Question 6: 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?

Réponse Courte:

Les exceptions telles que déjà listées dans PIPEDA et la LPRPSP nous semblent complètes, sujet à ajouter certains critères relativement aux cas d'enquête et de collaboration pour violations de la loi entre entreprises, et les données collectées sur les employés lors de leur travail, qui, selon, exigent plus de protection dans un context de systèmes socio-techniques.

Liste de recommandations:

1. **Maintenir les exceptions existantes.**
2. **Ajouter certaines mesures de sauvegarde, en particulier concernant les listes d'indésirables, dans un contexte d'enquêtes et de collaborations entre entreprises concernant des violations de la loi telle la fraude, afin de mieux protéger les droits des individus et des entreprises concernées.**

[68]GPT-2, https://openai.com/blog/gpt-2-1-5b-release/
[69]MEADOWS, Donella, "Thinking in Systems",
https://books.google.co.in/books/about/Thinking_in_Systems.html?id=CpbLAgAAQBAJ&redir_esc=y

3. **Ajouter certaines mesures de sauvegarde concernant la collecte et l'utilisation des données des employés dans le cadre de leur travail, notamment en lien avec les prises de décision reliés à leur performance et leur productivité[70].**

Commentaires:

Les exceptions telle que déjà listées dans PIPEDA et la LPRPSP nous semblent couvrir la majorité, si non pas la totalité, des exceptions qui devraient être permises, et les critères déjà proposés nous semblent raisonnables.

Nous proposons toutefois que des critères plus stricts encadrent les protocoles d'enquêtes et de collaboration entre entreprises pour des cas de fraudes, RPCFAT et autres allégations de violations de la loi, afin d'éviter de causer du préjudice à des individus ou autres entreprises incluent sur des "listes d'indésirables" par des systèmes socio-techniques, sans suffisamment de mesures organisationnelles et techniques afin de protéger leur réputation, et la présomption d'innocence.

Nous proposons aussi que des critères plus stricts viennent encadrer l'utilisation de systèmes socio-techniques quant à l'analyse de la performance d'employés. Certaines préoccupations ont été soulevées à l'effet que des systèmes socio-techniques pourraient exacerber la position de pouvoir et de contrôle de l'employeur sur l'employé, en imposant des indicateurs de performance incomplets ou erronés ainsi que des taux ou objectifs de productivité abusifs, qui seraient paramétrés dans le système[71].

Ceci pourrait avoir comme conséquence d'augmenter les cas d'anxiété, de dépression et d'épuisement ("*burnout*"), en plus de potentiellement soulever de l'instabilité et des conflits liés à des associations d'employés[72]. Il pourrait être à prévoir que le taux de syndicalisation pourrait augmenter sur la base de l'implantation de systèmes socio-techniques dans ce contexte, quand ceux-ci sont utilisés afin d'augmenter la profondeur et la continuité de la surveillance des gestionnaires, et qui pourraient devenir intrusives et proprement intolérables aux employés[73].

[70]CHA, Sangmi, "*South Korean jobseekers and students are beating the AI interview bots - here's how*", World Economic Forum, 2020, https://www.weforum.org/agenda/2020/02/south-koreas-ai-hiring-bots/; DZIEZA, Josh, "How Hard will the robots make us work?", The Verge, 2020, https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon
[71]Id.
[72]CRAWFORD, Kate, others, *AI NOW 2019 Report*, December 2019, 100 pages.
[73]Id.

Les utilisations de ces systèmes concernant des prises de décision au niveau de l'embauche et du congédiement pourraient aussi déclencher certaines injustices. Finalement, considérant le risque associé au biais qui pourrait résulter de ce système, un risque demeure dans la prise de décision potentielle résultant dans une discrimination illégale. Nous suggérons à la Commission d'explorer plus en profondeur la permission présente associée à ce type de données, afin que ces systèmes ne soient pas utilisés afin de remplacer le degré de confiance dans une relation humaine, mais plutôt d'augmenter le rôle, les tâches et l'efficacité de l'employé.

Question 7: Est-ce que l'utilisation de données anonymisées ou de jeux de données synthétiques pour l'entraînement des SIA devrait être favorisée?

Réponse Courte:

Oui. Considérer aussi les "*Generative Adversarial networks*" (GANs)[74].

Commentaires:

Concernant les jeux de données synthétiques, ils pourraient devenir des sources alternatives de données afin d'entraîner l'apprentissage d'une machine, par contre, il serait suggéré d'explorer plus en profondeur le caractère suffisamment adéquat et représentatif de ces données, afin que les inférences et les résultats produits par les systèmes socio-techniques demeurent cohérents, raisonnables et corrects[75].

Une seconde approche potentielle, GANs, pourrait générer des distributions de données synthétiques utiles mais selon nous plus de recherches sont requise afin de vérifier l'efficacité de cette approche.

Question 8: Est-ce que la réidentification de données préalablement dépersonnalisées ou dé-identifiées, ou la réidentification délibérée, mais sans nécessité autorisée ou apparente devraient être interdites et sanctionnées?

Réponse Courte:

Oui, sujet à consentement de l'individu pour une fin spécifique, utile, et responsable, et sujet à certains cas listés dans la loi lorsque la vie ou la santé d'un individu, ou l'intérêt du public, le permet.

[74]GOODFELLOW, Ian, "*NIPS 2016 Tutorial: Generative Adversarial Network*s", https://arxiv.org/pdf/1701.00160.pdf
[75]KLEINBERG, OTHERS, "Inherent Trade-Offs in the Fair Determination of Risk Scores", https://arxiv.org/abs/1609.05807; AI Fairness 360 Toolkit, IBM, https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/

Commentaires:

Une obligation imposant la dépersonnalisation et la dé-identification devrait devenir une règle de base, avec pour corollaire une interdiction générale de ré-identifier des données dépersonnalisées ou dé-identifiées, sujet au consentement donné par l'individu pour une fin utile, spécifique et responsable.

Toutefois, certains cas pouvant affecter la vie ou la santé d'un individu, ou s'il est de l'intérêt du public de retracer l'identité de l'individu, devraient être listés comme étant des cas de ré-identification possible selon des critères stricts. Tout abus de ces permissions, et toute ré-identification illégale, sans consentement, avec une intention malicieuse ou dû à une négligence grossière ou un mépris manifeste, devraient être gravement sanctionnés.

Question CAIQ 9: 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?

Réponse courte:

Une approche systémique, incluant l'éducation de la population et la prise en compte d'une rétroaction du public lors de consultations entre le législateur et les citoyens, une responsabilisation légale et sociale des chercheurs et développeurs de systèmes socio-techniques, et une collaboration et une coopération de l'industrie avec les régulateurs désignés suffisamment capables, représente selon la meilleure approche.

Liste de recommandations:

1. **Mettre en place un bac à sable "innovation" et un bac à sable "conformité", permettant des échanges efficaces entre le régulateur et les entreprises en transition dans l'industrie[76].**
2. **Mettre en place une "boîte à outils" ("*Toolkit*") techniques et organisationnelles pour les entreprises offerte par le régulateur dans le cadre du bac à sable "conformité".**
3. **Permettre expressément dans la loi l'inspection proactive et l'audit des systèmes socio-techniques des entreprises par le régulateur, sujet à certaines protections réglementaires et légales.**

[76]ARNER, Douglas, OTHERS, "Fintech and Regtech in a nutshell, and the Future in a Sandbox", CFA Institute Research Foundation, https://www.cfainstitute.org/-/media/documents/article/rf-brief/rfbr-v3-n4-1.ashx

4. **Identifier les tierces parties et organisations normatives reconnues ou crédibles pour la certification et la standardisation des systèmes socio-techniques**[77]
5. **Éduquer le public par certification ou formations données par le régulateur et les entreprises (Analogie à l'obligation des institutions financières de développer la littératie financière du public)**
6. **Obliger expressément dans la loi la consultation régulière du public par le régulateur et le législateur dans le cadre d'amendements de la loi ou des règlements, ainsi que de la rédaction de lignes directrices ou positions d'interprétation du régulateur**
7. **Fortement encourager les entreprises à consulter régulièrement leurs clients, partenaires d'affaires critiques et autre grand public dans le cadre de gouvernance de leurs systèmes socio-techniques, incluant au moment du "design" et de l'identification des "fins" auxquelles ces systèmes sont prévus.**

Commentaires:

Nous recommandons de prendre en considération le changement d'objectif lors de la transition de la "mission" liée à la recherche et développement du système socio-technique en milieu de "laboratoire", que ce soit dans un département de R&D d'une entreprise ou au sein d'une institution académique, ce que nous appelons l'objectif scientifique "pur", à un déploiement en milieu d'affaires, ce que nous appelons l'objectif lucratif.

En résumé, nous identifions donc a priori deux milieux différents avec des fins générales, soit:

1. Le milieu de laboratoire, avec un objectif scientifique pur **(Fais le marcher/"Make it work")**
2. Le milieu d'affaires, avec un objectif lucratif **(Fais le marché/"Make it worth")**

Il y a évidemment un large spectre d'autres milieux et d'autres objectifs, mais dans le cadre de cette proposition, nous nous concentrons plutôt sur ceux-ci, en lien avec la portée traditionnelle de la loi en matière de vie privée dans le secteur privé.

En lien avec l'abondance d'investissements stratégiques dans le design et le déploiement de systèmes socio-techniques, nous voyons de plus en plus différents types de partenariats entre des institutions académiques et des entreprises dans un contexte de recherche, développement et déploiement de systèmes socio-techniques, que ce soit par des coentreprises ("*joint ventures*"), véhicules fiscaux ou juridiques à usage spécifique ("*special purpose vehicles*" or "SPVs"), des

[77]OECD Legal Instruments, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

fonds de capital-risques ("*venture funds*"), des subventions ("*grants*") privés ou publics, ou partenariats plus traditionnels.

Nous conservons une certaine inquiétude à l'effet que si la recherche scientifique est directement liée à un objectif lucratif, et que l'investissement en affaires impose des conditions pressantes en temps et en ressources au niveau du développement de différents modèles et algorithmes à des fins lucratives spécifiques, que certaines étapes d'analyse, de vérification diligente **("*due diligence*")**[78] et de considérations sociétales dans le déploiement de ces systèmes soient accélérées ou exclues, afin de rencontrer les expectatives des sponsors ou investisseurs.

La même inquiétude est exacerbée pour les laboratoires R&D internes et propres aux entreprises, qui connaissent un degré de symbiose et de pression de l'employeur encore plus élevés, par leur proximité et leur dépendance financière.

De manière générale, les lois en matière de vie privée que nous connaissons démontrent une plus grande souplesse, tolérance et un plus haut degré de permission au niveau de l'utilisation des RP, lorsque les fins sont celles de la recherche académique ou scientifique, journalistique, artistique, etc., afin de ne pas causer de détriment l'innovation et à la créativité humaine.

Nonobstant cette souplesse permissive, il devrait être possible d'imposer les mesures organisationnelles et techniques de dépersonnalisation et de dé-identification à tous les milieux, ainsi que favoriser l'utilisation de bases de données synthétiques, ou sans ou peu d'impacts (eg. individus décédés depuis plus de 30 ans[79], données du domaine public, etc.).

Si ce changement d'objectif n'est pas pris en compte ou n'est pas reconnu, il se peut que certaines entités tenteront d'éviter l'application de la loi et d'accéder à des bases de données plus permissives par l'entremise de leurs laboratoires ou de leurs partenariats avec des institutions académiques.

FIN.

CONTACT MAIEI:

Pour contacter Mirka Snyder Caron afin de soumettre des questions ou commentaires:

mirka@montrealethics.ai

[78] *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems,* https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf

[79] LPRPSP, art. 18.2

SOURCES:

ALLISON-HOPE, Dunston, BSR, "Human Rights by Design", https://www.bsr.org/en/our-insights/blog-view/human-rights-by-design;

ARNER, Douglas, OTHERS, "Fintech and Regtech in a nutshell, and the Future in a Sandbox", CFA Institute Research Foundation, https://www.cfainstitute.org/-/media/documents/article/rf-brief/rfbr-v3-n4-1.ashx

ARNER, Douglas, OTHERS, *The Dark Side of Digital Financial Transformation: The New Risks of Fintech and the Rise of TechRisk*, University of Hong Kong Faculty of Law Research Paper No. 2019/112, 37 pages.

BAGDASARYAN, OTHERS, "Ancile: Enhancing Privacy for Ubiquitous Computing with Used-Based Privacy", Cornell University, 2019, http://www.cs.cornell.edu/~jnfoster/papers/ancile.pdf

BOURTOULE, LUCAS, OTHERS,, Machine Unlearning, University of Toronto and Vector Institute, https://arxiv.org/pdf/1912.03817.pdf., 16 pages.

CAVOUKIAN, "Privacy by Design: Foundational Principles", https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf;

CHA, Sangmi, "*South Korean jobseekers and students are beating the AI interview bots - here's how*", World Economic Forum, 2020, https://www.weforum.org/agenda/2020/02/south-koreas-ai-hiring-bots/

COLIN, Harris, *Montreal grapples with privacy concerns as more Canadian police forces use facial recognition*, CBC News, https://www.cbc.ca/news/canada/montreal/facial-recognition-artificial-intelligence-montreal-privacy-police-law-enforcement-1.5239892

CONGER, Katie, *San Francisco Bans Facial Recognition Technology*, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

CRAWFORD, Kate, others, *AI NOW 2019 Report*, December 2019, 100 pages.

Deepmind, AlphaGo, https://deepmind.com/research/case-studies/alphago-the-story-so-far

DZIEZA, Josh, "How Hard will the robots make us work?", The Verge, 2020, https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon

FEDERAL TRADE COMMISSION, "Data Brokers: a Call for Transparency and Accountabliity", 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

FINANCIAL STABILITY BOARD, "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications", https://www.fsb.org/wp-content/uploads/P011117.pdf

GUPTA, Abhishek, SNYDER CARON, Mirka, "Response to the AHRC and WEF regarding Responsible Innovation in AI", Montreal AI Ethics Institute, 25 pages.

Voir GUPTA, Abhishek, SNYDER CARON, Mirka, "The social contract for AI", IJCAI AI for Social Good Workshop 2019, Abstract, 7 pages.

GUPTA, Abhishek, "The Evolution of Fraud: Ethical Implications in the Age of Large-scale Data Breaches and Widespread Artificial Intelligence Solutions Deployment", https://www.itu.int/en/journal/001/Documents/itu2018-12.pdf

GPT-2, https://openai.com/blog/gpt-2-1-5b-release/

HERN, Alex, "*I read all the small print on the internet*", The Guardian, 2015, https://www.theguardian.com/technology/2015/jun/15/i-read-all-the-small-print-on-the-internet

HUBER, Rose, "Mosaic Effect" Paints Vivid Pictures of Tech Users' Lives", https://wws.princeton.edu/news-and-events/news/item/mosaic-effect-paints-vivid-pictures-tech-users-lives-felten-tells-privacy

IMAGENET, http://www.image-net.org/

Information Commissioner's Office, "Right to erasure", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/;

KLEINBERG, OTHERS, "Inherent Trade-Offs in the Fair Determination of Risk Scores", https://arxiv.org/abs/1609.05807; AI Fairness 360 Toolkit, IBM, https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/

NIST Cybersecurity, https://www.nist.gov/topics/cybersecurity

NORVIG, Peter, "Artificial Intelligence: A Modern Approach", Pearson, 3rd edition, 2016, p. 18ss.

MEADOWS, Donella, "Thinking in Systems", https://books.google.co.in/books/about/Thinking_in_Systems.html?id=CpbLAgAAQBAJ&redir_esc=y

METZ, Cade, "Forget doomsday AI Google worried housekeeping bots gone bad", https://www.wired.com/2016/06/forget-doomsday-ai-google-worried-housekeeping-bots-gone-bad/

OECD Legal Instruments, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Office of the High Commissioner for Human Rights, United Nations, UN Guiding Principles for Businesses and Human Rights, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

PENNEY, Jonathon, OTHERS, "Human Rights by Design", Schneier on Security, https://www.schneier.com/blog/archives/2018/12/human_rights_by.html;

RIBEIRO, Marco Tulio, OTHERS, "Why should I trust you?" Explaining the Predictions of any Classifier", https://arxiv.org/pdf/1602.04938v1.pdf

Search Encrypt, Medium, "7 Principles of Privacy by Design", https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce

SHULL, Aaron, "The Charter and Human Rights in the Digital Age", Center for International Governance Innovation, 2018, 6 pages.

SNYDER CARON, Mirka, "The Transformative Effect of AI on the Banking Industry", Banking & Finance Law Review, April 2019, 34 BFLR 79-345.

SRINISAVAN, Hansa, ML-fairness-gym: A Tool for Exploring Long-Term Impacts of Machine Learning Systems, Google AI Blog, , http://ai.googleblog.com/2020/02/ml-fairness-gylem-tool-for-exploring-long.html

THOMSON REUTERS LEGAL, "Right to Be Forgotten: Erasing Your Private Information from Cyberspace", https://legal.thomsonreuters.com/en/insights/articles/erasing-your-private-information-from-cyberspace

VINCENT, James, "This is when experts think we'll build a truly intelligent AI", https://www.theverge.com/2018/11/27/18114362/ai-artificial-general-intelligence-when-achieved-martin-ford-book

WACHTER, Sandra, MITTELSTADT, Brent, "Re-Thinking Data Protection Law in the Age of Big Data and AI",Columbia Business Law Review, Vol. 2019, No. 2:494], p.495-620; 127pages.

LEGAL

Canadian Digital Charter for Human Rights, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html; https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

Canadian Charter of Rights and Freedoms, Constitution Act 1982.

Civil Code of Quebec, chapter CCQ-1991, ss. 35-40.

Déclaration de Montréal sur l'IA Responsable

General Data Protection Regulation, (EU) 2016/679.

EU Guidelines for Trustworthy AI, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Personal Information Protection and Electronic Documents Act, S.C. 2000, c.-5

Act Respecting the Protection of Personal Information in the Private Sector, c. P-39.1

Office of the High Commissioner for Human Rights, UN Guiding Principles on Business and Human Rights, United Nations, 42 pages.

Reference re Same-Sex Marriage, [2004] 3 S.C.R. 698, 2004 SCC 79, "living tree"

*The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems,*https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf