

# L'intelligence Artificielle

Daniel Chow

## **Introduction**

L'intelligence artificielle (ci-après IA) est devenue une technologie omniprésente dans nos quotidiens. Touchant plusieurs domaines dont la médecine, afin d'améliorer nos capacités en matière d'imagerie médicale<sup>1</sup>, ou sinon le droit pour améliorer le rendement des avocats<sup>2</sup>, il s'agit d'un réel outil de productivité et d'efficacité polyvalent pour plusieurs professions. Toutefois, si son usage apporte plusieurs bienfaits, il n'en reste pas moins que plusieurs critiques existent à son égard. En effet, nous savons que l'objectif brut de l'IA est de reproduire la structure complexe et nuancée du raisonnement humain, issu de plusieurs milliers d'années d'évolution. Ainsi, est-ce qu'il ne serait pas prudent d'être sceptique face à une utilisation de plus en plus accrue d'une technologie comparativement jeune, lors de la prise de décisions *high-stakes* ? Comme l'explique la professeure Karen Eltis, il y a donc un jeu d'équilibre à atteindre en cette matière ; il faut d'une part « harness the great advantages that machine learning offers toward safety and efficiency », en même temps d'assurer que l'utilisation d'algorithmes ne

---

<sup>1</sup> Nicholson Price, « Black-Box Medicine », (2015) 28:2 Harv JL & Tech 420 à la p 439 ; Sébastien Langevin, « L'intelligence artificielle au service de l'imagerie médicale » (24 avril 2018), en ligne (blogue) : ÉTS < <https://cutt.ly/YF81IBC> >.

<sup>2</sup> *Cass c. 1410088 Ontario Inc.*, 2018 ONSC 6959 ; *Drummond c. Cadillac Fairview Corporation Limited*, 2019 ONCA 447.

soit pas un « crutch, insidiously replacing nuanced, all-too-human decision-making »<sup>3</sup>.

Ainsi, le but du présent essai sera d'explorer le thème de l'IA et les problématiques s'y rattachant, en prêtant une attention particulière à son utilisation par le gouvernement. Les problématiques du secteur privé causées par l'utilisation de l'IA étant déjà suffisamment explorées par la littérature, cet angle de recherche permettra de faire intervenir dans l'analyse, certaines considérations touchant la charte et les droits fondamentaux.

Afin de décortiquer ce thème fort complexe, il y a lieu de d'abord définir plusieurs termes d'importance. Ensuite, une deuxième section se consacrera à l'exploration des diverses problématiques entourant l'utilisation de l'IA, notamment la question de la discrimination et l'épineuse question de la protection des données. Finalement, une troisième et dernière partie sera consacrée au cadre réglementaire existant, et nous porterons parallèlement un regard critique sur l'efficacité des mesures en place.

## **Définitions importantes**

### **o Les définitions de termes de base**

Tout d'abord, commençons par définir plusieurs termes importants pour pouvoir mieux cerner l'étendue du présent sujet. À cette fin, nous examinerons successivement les définitions de l'IA, le système décisionnel automatisé, et finalement l'algorithme.

L'expression IA est devenue galvaudée et surutilisée par divers secteurs<sup>4</sup>, rendant sa définition par le citoyen moyen extrêmement difficile. Ce constat flagrant en est une de longue date, concrétisée pour une des premières fois dans une décision de 1989 de la Commission des oppositions des marques

---

<sup>3</sup> Karen Eltis, « Think easy, think hard: When to let AI make business decisions », *The Globe and Mail* (5 août 2019) en ligne: < <https://cutt.ly/4F80f28> >.

<sup>4</sup> Secrétariat du Conseil du Trésor du Canada, « Responsible Artificial Intelligence in the Government of Canada - Digital disruption white paper series » (2018) Gouvernement du Canada Document de travail No. 2018-2.0 à la p 8 ; Medium, « The "AI" Label is Bullsh\*t » (17 juin 2020), en ligne (blogue): *Medium* < <https://cutt.ly/yF89E55> >.

de commerce (*Knowledge Network c Leppik*)<sup>5</sup>. Il est donc possible de voir d'emblée, un réel besoin de limiter l'étendue du terme pour ne pas le confondre avec d'autres termes similaires.

Au Canada, une directive gouvernementale, la *Directive sur la prise de décisions automatisée*<sup>6</sup> (ci-après directive) permet de définir plusieurs termes pertinents à notre recherche. Cette directive avait comme but d'instaurer des balises au pouvoir de ministères fédéraux souhaitant faire usage de telles technologies, et définit l'IA comme étant « toute technologie de l'information qui exécute des tâches pour lesquelles il faut habituellement faire appel à l'intelligence biologique, comme comprendre le langage parlé, apprendre des comportements ou résoudre des problèmes ». Notons toutefois que de nos jours, quand nous parlons usuellement de l'IA, nous faisons souvent référence à l'aspect *machine learning*, à savoir la capacité pour la machine d'apprendre et adapter continuellement son comportement à la lumière des données fournies (*training data*)<sup>7</sup>.

D'autre part, la directive définit le système décisionnel automatisé comme comprenant :

toute technologie qui soit informe ou remplace le jugement des décideurs humains. Ces systèmes proviennent de domaines tels que les statistiques, la linguistique et les sciences informatiques, et utilisent des techniques telles que les systèmes basés sur des règles, la régression, l'analytique prédictive, l'apprentissage automatique, l'apprentissage en profondeur et les réseaux neuronaux

---

<sup>5</sup> *Knowledge Network c. Leppik*, 1989 TMOB 235.

<sup>6</sup> Gouvernement du Canada, « Directive sur la prise de décisions automatisée » (dernière modification : 1 avril 2021), en ligne (pdf) : *Gouvernement du Canada* < <https://cutt.ly/DF89vJP> > [Directive].

<sup>7</sup> Ethem Alpaydin, « Introduction to Machine Learning », 2e éd, Cambridge, MIT Press, 2010 à la p 31 ; The Medical Futurist, « Simple Algorithms vs. A.I. And What They Mean For Medicine » (29 décembre 2020), en ligne (blogue): *TMF* < <https://cutt.ly/uF880rX> >.

Finalement, l'algorithme, la pierre angulaire de ce sujet, peut être compris comme une liste de différentes « instructions bien définies »<sup>8</sup> que l'on donne à une machine, dans le but ultime de déboucher sur un résultat final ou résoudre un problème quelconque. En ce sens, pour reprendre la description simplifiée des auteurs Molnar et Gill, il s'agit en somme d'une recette composée d'ingrédients se trouvant sous la forme d'étapes programmées<sup>9</sup>.

En résumé, sur la foi de ces nombreuses définitions, il est possible de comprendre que l'automatisation d'un système décisionnel se fait grâce à l'usage d'un algorithme, une liste de séquences bien définies, rappelant l'analogie précitée d'une recette. La formule « recette » de l'algorithme étant la forme la plus basique de l'algorithme, certains algorithmes plus complexes, dont celles utilisées pour la prise de décisions, peuvent en tour être qualifiés d'IA. Nous parlons dans ce cas-ci, d'algorithmes utilisant notamment la technique *machine learning*, permettant à une machine d'atteindre un seuil d'intelligence et indépendance donnée comparable à « l'intelligence biologique »<sup>10</sup>, suite à un entraînement spécial employant des données présélectionnées, du *training data*.

- **Brève introduction et définition de la problématique des biais algorithmique**

Pour poursuivre, il y a lieu d'introduire brièvement dans cette même section une problématique tirant sa source des concepts prédéfinis, à savoir le problème des biais algorithmiques.

D'abord, les biais algorithmiques sont des préjugés proprement humains qui sont introduits lors de la conception d'un algorithme. Les algorithmes utilisant la technique *machine learning* sont calibrés par un humain, en

---

<sup>8</sup> Adriano Koshiyama et al, « Towards Algorithm Auditing » (2021), en ligne (pdf): SSRN < <https://cutt.ly/2F82OPw> > à la p 2.

<sup>9</sup> Petra Molnar et Lex Gill, « Bots at the gate - A human rights analysis of automated decision making in Canada's immigration and refugee system » (2018), en ligne (pdf): Citizenlab < <https://cutt.ly/1F82ZCU> > à la p 16. [Bots].

<sup>10</sup> Directive, *supra* note 6.

utilisant des données (*training data*), et la question est simplement de déterminer si les données proposées à la machine représentent une image fidèle de la réalité ou une image biaisée de celle-ci. Comme l'expliquent les auteures Molnar et Gill, l'algorithme mal calibré à l'issue de données biaisées, aura comme effet de perpétuer ce biais original et parfois même d'en amplifier ses conséquences :

Biases of the individual(s) designing an automated system or selecting the data that trains it, or shortcomings of the input data itself, can be compounded to create discriminatory outcomes that not only reproduce, but even sometimes magnify patterns of discrimination<sup>11</sup>

En somme, il est donc possible de concevoir qu'une calibration biaisée d'un algorithme peut avoir certaines conséquences sur le droit à l'égalité ; la machine qu'on croyait neutre ne l'est pas en réalité ! En effet, comme l'explique Dr David Leslie, directeur de l'Institut Alan Turing, les algorithmes de décisions automatisées discriminent le plus souvent les femmes et les personnes racisées, deux groupes rarement représentés dans le *training data* des algorithmes<sup>12</sup>. D'ailleurs, une étude récente menée par Joy Buolamwini de l'université MIT confirme les résultats précités. Buolamwini conclut de ses travaux qu'en moyenne, les logiciels d'analyse faciale révèlent un taux d'erreur de 34,7 % pour les femmes à la peau foncée, contrastant avec un taux minime de seulement 0,8 % pour les hommes blancs<sup>13</sup>. Les femmes et personnes racisées sont donc pénalisées indûment par l'utilisation de technologies de décisions automatisées biaisées.

Ainsi, d'après nous, il est donc possible de voir à travers l'exemple précité que l'IA, bien qu'elle soit normalement vendue comme étant le summum de

---

<sup>11</sup> Bots, *supra* note 9 à la p 38.

<sup>12</sup> David Leslie, « Understanding bias in facial recognition technologies » (2018), en ligne (pdf): SSRN < <https://cutt.ly/oF84ZYR> > à la p 6.

<sup>13</sup> Joy Buolamwini et Timnit Gebru, « Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification », (2018) 81:1 PMLR 15.

la « neutralité et l'objectivité »<sup>14</sup>, ne l'est pas en réalité, car les décisions qui en découlent peuvent être facilement influencées par l'humain et ses données biaisées. Ce constat flagrant, transposé dans le contexte du présent essai, peut donc nous faire songer à la nature dangereuse de l'IA, souvent employée dans le secteur public par l'état pour la prise de diverses décisions automatisées. Nous nous attarderons donc de manière critique sur cette problématique et ses conséquences dans la section qui suivra, en mettant une emphase particulière sur les droits et libertés pouvant être affectés par l'utilisation de l'IA.

## **Gouverner l'ère numérique**

### **o La problématique contemporaine**

Enfin, le penchant du gouvernement de privilégier l'usage de la technologie dans diverses facettes de ses activités affectant la sphère publique, s'inscrit dans une nouvelle tendance de gouvernance de l'état, créée pour s'adapter à l'ère numérique<sup>15</sup>. Effectivement, d'après Mike Bracken, l'ancien chef du service numérique du gouvernement britannique, la prolifération de la technologie ces dernières années, a donné lieu à la naissance d'une gouvernance de l'ère numérique ayant ses propres « set of characteristics, both physical and cultural »<sup>16</sup>. Le secteur privé s'appuyant de manière croissante sur les algorithmes pour prendre des décisions avec célérité et précision, les affaires économiques à l'ère technologie sont devenues encore davantage rapide et complexe, exigeant que le gouvernement s'adapte en conséquence<sup>17</sup>. Il y a donc eu un changement de paradigme au niveau des services publics offerts, poussant ainsi l'état à « rethink public services »<sup>18</sup>,

---

<sup>14</sup> Theo Araujo et al, « In AI we trust? Perceptions about automated decision-making by artificial intelligence », (2020) 35:6 AI & Society 611 à la p 613.

<sup>15</sup> Cary Coglianese, « Optimizing Government for an Optimizing Economy » (2016), en ligne (pdf): *Penn Law* < <https://cutt.ly/wF86rOm> > à la p 1 [Coglianese, « Optimizing »].

<sup>16</sup> Mike Bracken, « On policy and delivery » (21 octobre 2014), en ligne (blogue): *Mike Bracken* < <https://cutt.ly/LF4qiPS> >.

<sup>17</sup> Coglianese, « Optimizing », *supra* note 15 à la p 3.

<sup>18</sup> Bracken, *supra* note 16.

dans le but d'y intégrer les progrès technologiques contemporains (« productive capabilities of information technologies »<sup>19</sup> ). De telles applications de technologie aux services publics font surface notamment en matière de surveillance policière ou sinon, la prise de décisions administratives assistées par IA. Toutefois, l'utilisation de plus en plus accrue de l'IA par l'état dans la prestation de services au public suscite plusieurs questions éthiques, dont notamment l'importance de reconnaître et comprendre le rôle du décideur humain dans ces processus décisionnels<sup>20</sup>, ainsi que la question de la responsabilité si une décision administrative prise à la recommandation de l'IA va mal (est biaisée par exemple). D'autant plus, compte tenu du fait qu'il existe déjà un grand déséquilibre de pouvoir entre l'état et le citoyen moyen, l'utilisation de l'IA pour la prise de décisions gouvernementales peut d'après nous, avoir comme effet d'amplifier encore davantage cette dichotomie préexistante. Ainsi, à nos yeux, l'intégration de la technologie doit par conséquent se faire de manière prudente parallèlement à de « nouvelles interventions règlementaires »<sup>21</sup>. En outre, nous sommes d'avis qu'une prudence particulière doit être observée quant à la question de l'intégration étatique des systèmes décisionnels automatisés pour la prestation de services, car celles-ci peuvent avoir des effets discriminatoires sur le droit à l'égalité, et la vie privée.

- **Les systèmes décisionnels automatisés ayant des effets discriminatoires - le droit à l'égalité**

Pour poursuivre, la popularisation de l'utilisation de l'IA par le gouvernement, révèle une reconnaissance croissante de ses capacités à desservir divers contextes. Malgré tout, pour le moment, il est à noter que l'utilisation de l'IA par le gouvernement reste en grande partie partiellement

---

<sup>19</sup> Lucia Nalbandian, « Increasing the accountability of automated decision-making systems: An assessment of the automated decision-making system introduced in Canada's temporary resident visa immigration stream », (2022) 10:1 J Resp Tech 56\_à la p 57.

<sup>20</sup> *Ibid.*

<sup>21</sup> Evert Lindquist et Irene Huse, « Accountability and monitoring government in the digital era: Promise, realism and research for digital-era governance », (2017) 60:4 Canadian Public Administration 627\_à la p 631.

automatisée, la machine intelligente ne recommandant qu'une solution à un décideur humain qui en a le contrôle ultime<sup>22</sup>. Toutefois, d'après plusieurs auteurs, ce *statu quo* risque de changer dans un futur proche<sup>23</sup>, donnant davantage de pouvoir d'adjudication et régulation à la machine intelligente<sup>24</sup> au détriment d'un contrôle humain plus nuancé. Cette situation a d'ailleurs déjà été lentement observée à deux niveaux dans le contexte canadien, notamment en matière d'immigration, et police.

Par la suite, depuis au moins 2014, le service frontalier du Canada expérimente avec l'utilisation de l'IA (prédictions par algorithmes) pour faciliter le processus de filtrage des demandes d'immigration. En effet, un projet pilote a été lancé en 2017, visant à cibler et faire le triage de personnes immigrantes provenant de divers pays asiatiques<sup>25</sup>. Les demandes d'immigration étaient triées par paliers en fonction du risque du dossier; celles dont le risque était le plus faible étaient envoyées pour auto-approbation, et celles se trouvant aux paliers supérieurs étaient ensuite révisées par un agent du service frontalier. L'algorithme qui desservait les fins du service frontalier prenait en compte plusieurs facteurs dans sa décision, dont, « the merits of an immigration application (l'âge, le sexe, la nationalité et les itinéraires de voyage), spot potential red flags for fraud and weigh all these factors to recommend whether an applicant should be accepted or refused »<sup>26</sup>. Ainsi, suivant ce modèle, il est possible de voir que l'algorithme du service frontalier est utilisé à des fins évidentes de profilage,

---

<sup>22</sup> William Eggers et al, « AI-augmented government » (2016), en ligne (pdf): *Deloitte Center for Government Insights* < <https://cutt.ly/2F4rScl> > à la p 7.

<sup>23</sup> Cary Coglianese et David Lehr, « Regulating by Robot: Administrative Decision Making in the Machine-Learning Era » (2017), en ligne (pdf): *Penn Law* < <https://cutt.ly/kF4trAQ> > à la p 6 [Coglianese, « Regulating »]; Vikas Chawla et al, « Decoding the Digital Jungle », 1e éd, Chennai, Notion Press, 2021 au chap 18.

<sup>24</sup> Coglianese, « Regulating », *supra* note 23 à la p 25.

<sup>25</sup> Immigration, Réfugiés et Citoyenneté Canada, « Overview of the Analytics-Based Triage of Temporary Resident Visa Applications » (2020), en ligne (pdf) : *Gouvernement du Canada* < <https://cutt.ly/SF4yNPQ> >.

<sup>26</sup> Nicholas Keung, « Canadian immigration applications could soon be assessed by computers », *Toronto Star* (5 janvier 2017) en ligne: < <https://cutt.ly/SF4urkH> >.

car celui-ci définit des profils, suite à un traitement automatisé des données, dans le but de prendre des décisions concernant un groupe de personnes<sup>27</sup>. Ajoutons que ce constat est d'autant plus préoccupant, car il est possible de concevoir que la catégorisation des personnes suite au profilage, peut facilement donner lieu à de la discrimination<sup>28</sup> (article 15 (1) de la charte canadienne) basée sur ces mêmes prédictions, si les groupes de personnes visées, reçoivent une différence de traitement basé sur leur pays d'origine par exemple.

Similairement, l'utilisation de l'IA en matière de cautions judiciaires dans certains états américains suscite ces mêmes préoccupations de discrimination aux mains de l'état. Effectivement, au sein de ce modèle nommé « Pretrial Risk Assessment », avant de prendre une décision de libération sous caution, le juge doit prendre en compte le résultat d'un algorithme<sup>29</sup> ; il s'agit notamment de la problématique illustrée dans la décision *Loomis c. Wisconsin*<sup>30</sup>. L'algorithme de libération sous caution prend généralement en compte plusieurs facteurs, notamment l'âge, l'historique judiciaire, la fréquence de défauts de comparution, etc, pour finalement produire sur la foi de ces facteurs, une recommandation en faveur, ou contre la libération provisoire de l'accusé. De manière empirique l'auteure Megan Stevenson est allée comparer l'effet et l'efficacité de telles politiques au Kentucky, débouchant finalement sur le constat que l'utilisation de tels outils avantageait en grande partie les accusés blancs, au détriment de personnes racisées<sup>31</sup>. Ainsi, il est possible de voir que l'utilisation de tels

---

<sup>27</sup> Valeria Ferraris et al, « Defining Profiling » (2020) Profiling Project Document de travail No. 2020-3.0 à la p 6.

<sup>28</sup> Maddalena Favaretto et al, « Big Data and discrimination: perils, promises and solutions. A systematic review », (2019) 6:1 J Big Data 1\_à la p 11.

<sup>29</sup> Sean Hill, « Bail Reform and the (False) Racial Promise of Algorithmic Risk Assessment », (2021) 68:4 UCLA L Rev 1\_à la p 44.

<sup>30</sup> *Loomis c. Wisconsin*, 881 NW (2d) 749 (Wis. 2016).

<sup>31</sup> Avec la mise en œuvre de cet outil, la proportion d'accusés noirs bénéficiant d'une libération sans caution n'a que légèrement augmenté, pour atteindre un peu plus de 25 %, alors que ce même taux pour les personnes blanches avait monté de plus de 35 % (Megan Stevenson, « Assessing Risk Assessment in Action », (2018) 103:58 Minn L Rev 304 aux pp

outils par l'état peut avoir un effet discriminatoire sur le droit à l'égalité de certaines populations, en amplifiant les inégalités sociales qu'ils vivent de jour en jour. De surcroît, étant un système basé sur l'IA, entrainé avec des données compilées de « criminal history information »<sup>32</sup> (les pratiques et tendances historiques en matière carcérale), le criminaliste John Raphling fait remarquer que les recommandations formulées par l'outil d'IA sont fortement biaisées (biais algorithmique), puisque la partialité raciale dans les pratiques policières est un problème historique et actuel aux États-Unis<sup>33</sup>. Nous assistons ainsi, pour reprendre les mots des auteures Molnar et Gill, à une magnification de « patterns of discrimination »<sup>34</sup> à travers l'utilisation d'un tel outil.

### **L'importance de la transparence et la nuance humaine**

Enfin, d'après nous, il y a lieu de reconnaître que les issues des deux exemples précités peuvent être dévastatrices sur la vie des justiciables. En effet, dans le cas de l'immigration, une décision de visa peut-être la différence entre la vie et la mort pour une victime de guerre civile par exemple<sup>35</sup>. Pareillement, une libération sous caution a plusieurs effets sur les droits et libertés de l'accusé. Ainsi, d'emblée, dans de pareilles situations « high-stakes » (et aussi de manière générale), il y a lieu de reconnaître la

---

362-63 ; Sarah Picard et al, « Beyond the Algorithm - Pretrial Reform, Risk Assessment, and Racial Fairness » (2018), en ligne (pdf): *Courtinnovation* < <https://cutt.ly/ZF4aYii> > à la p 9.)

<sup>32</sup> Alexis Briggs et Alec Karakatsanis, « Human Rights Watch advises against using profile-based risk assessment in bail reform » (17 juillet 2017), en ligne (blogue): *Human Rights Watch* < <https://cutt.ly/rF4s0mt> >.

<sup>33</sup> John Raphling, « Efficient Injustice: Too Much Pretrial Incarceration Damages the Integrity of Our Courts », (2018) 57:3 *Judges J 14 aux pp 14-15*.

<sup>34</sup> *Bots*, *supra* note 9 à la p 38.

<sup>35</sup> Adèle Garnier et al, « Is Canada's welcome to fleeing Ukrainians a new era of refugee policy? » (9 mars 2022), en ligne (blogue): *The Conversation* < <https://cutt.ly/uF4fQLq> >; *Bots*, *supra* note 9 à la p 8.

plus-value de la nuance que peut apporter l'humain, à l'équation décisionnelle de l'IA (« humans-in-the-loop »<sup>36</sup>).

Par la suite, toujours dans le cadre de situations « high-stakes », nous sommes d'avis que les conséquences possibles d'une décision prise par l'IA sont amplifiées en raison d'un manque de transparence. Effectivement, l'auteure Petra Molnar qualifie le raisonnement de l'IA comme « highly discretionary, and (...) often opaque »<sup>37</sup>, confirmant ce manque de transparence au sein des décisions de l'IA. En outre, cette même critique est reprise par la littérature scientifique à travers l'emploi de l'expression « black box », faisant référence à un algorithme qui « discerns patterns and make predictions in a way that cannot be intuitively understood or explained in the same way as conventional analysis can be »<sup>38</sup>. En langage simple, les utilisateurs d'algorithmes sont difficilement capables de comprendre le raisonnement interne de l'IA, car cette dernière s'appuie sur des « machine-learning algorithms that internalize data in ways that are not easily audited or understood by humans »<sup>39</sup>. Ainsi, d'après nous, il est facilement concevable que le « black box » de l'IA puisse amplifier le risque d'un justiciable dont le visa a été refusé, car ce dernier n'aura jamais accès aux motifs expliquant son refus, et par conséquent, ne sera jamais outillé pour pouvoir agir face à son malheur<sup>40</sup>. En outre, ajoutons que cette situation semble d'autant plus être une violation manifeste du principe fondamental du droit administratif

---

<sup>36</sup> Lucia Nalbandian, « Using Machine-Learning to Triage Canada's Temporary Resident Visa Applications » (2021) Ryerson Centre for Immigration and Settlement Document de travail No. 2021-9.0 à la p 14.

<sup>37</sup> Petra Molnar, « Governments' use of AI in immigration and refugee system needs oversight », *Options Politiques* (16 octobre 2018) en ligne: < <https://cutt.ly/9F7MRnt> >.

<sup>38</sup> Cary Coglianese et David Lehr, « Transparency and algorithmic governance » (2019) 71:1 Admin L Rev 1 à la p 14 [Coglianese, « Transparency »].

<sup>39</sup> Yavar Bathaee, « The artificial intelligence black box and the failure of intent and causation » (2018) 31:2 Harv JL & Tech 890 à la p 901.

<sup>40</sup> Cary Coglianese et Lavi Ben Dor, « AI in Adjudication and Administration » (2021) 86:3 Brook L Rev 791 à la p 806.

(équité procédurale) consistant à fournir des motifs de refus décisionnels « clairs, précis et intelligibles »<sup>41</sup>.

Finalement, malgré tout, il faut noter que pour le gouvernement, il ne s'agit pas uniquement d'une question de transparence, mais bien d'une question de redevabilité (accountability) envers le justiciable moyen. Effectivement, d'après l'auteure Nalbandian, « public sector organizations are largely operating in 'webs of accountability' in which they must explain their actions to various 'accountability forums' »<sup>42</sup>. Ainsi, il faut comprendre que dans nos sociétés démocratiques, la situation est similaire à un *quid pro quo* dans lequel la population élit le gouvernement, et ce dernier doit en tour, gouverner et offrir des services aux citoyens, tout en étant « bound by principles of transparency »<sup>43</sup>. Cette balance de responsabilité est à notre sens, pas retrouvée dans les deux cas de figure susmentionnés.

#### ○ **L'algorithme et le droit à la vie privée**

Par la suite, nous sommes aussi d'avis que l'utilisation de l'IA par l'état pose dans certains cas, un problème de droit à la vie privée. C'est notamment l'exemple de l'utilisation de l'application *Clearview AI* par la GRC pour des motifs légitimes à première vue. En effet, la technologie *Clearview AI* faisant usage du phénomène « Big Data »<sup>44</sup>, permet de collecter un grand volume d'images provenant de diverses sources sur le net, qui peuvent en tour aider les forces de l'ordre, les institutions financières et d'autres clients à identifier des personnes d'intérêt. L'utilisation d'une telle application peut donc soutenir certains objectifs de la GRC, notamment la sécurité nationale, la résolution de crimes ou l'identification de personnes disparues. Toutefois, plusieurs critiques, dont le Commissaire à la protection de la vie privée du

---

<sup>41</sup> Gouvernement du Canada, « Citoyenneté : Justice naturelle et équité procédurale » (dernière modification : 3 juillet 2015), en ligne (pdf) : *Gouvernement du Canada* < <https://cutt.ly/AF75o1B> >.

<sup>42</sup> Nalbandian, *supra* note 36 à la p 1.

<sup>43</sup> Coglianesi, « Transparency », *supra* note 38 à la p 5.

<sup>44</sup> Andrea De Mauro et al, « A formal definition of Big Data based on its essential features » (2016) 65:3 *Library Rev* 122 à la p 129.

Canada, Daniel Therrien, ont rapidement formulé des craintes à ce sujet, car l'utilisation de la banque de données de *Clearview*, contenait des milliards d'images extraites de sites internet sans le consentement des utilisateurs (contrevient à la *Loi fédérale sur la protection des renseignements personnels*, ci-après LPRPDE)<sup>45</sup>. Ces images sont en outre, en grande partie de personnes innocentes, sans quelconque suspicion de crimes, ce qui présente une violation claire de la vie privée. De surcroît, cette problématique s'aggrave si nous songeons au fait que l'internet n'a pas de frontières (contrairement aux pays, et les tribunaux). Les photos compilées par la compagnie américaine sont donc susceptibles de venir des quatre coins du monde, causant ainsi un problème de vie privée à portée extraterritoriale pour le plaignant, voyant sa photo utilisée par les forces de paix de l'autre bout du monde<sup>46</sup>. Quels seront alors les recours d'une victime similaire contre une telle violation de vie privée ?

Similairement, comme nous l'avons explicité précédemment, la transparence entre le gouvernement élu et le public est à notre sens cruciale, car c'est ce même public qui met au pouvoir le gouvernement. Ce dernier se doit donc d'être transparent quant aux objectifs pour lesquels les données personnelles du public seront traitées<sup>47</sup>. Toutefois, non seulement la GRC a longtemps nié l'utilisation de *Clearview*, mais aussi, comme nous l'explique Daniel Therrien, seuls 6 % des recherches effectuées par la GRC dans la banque de *Clearview* concernaient un incident lié à l'exploitation d'enfants

---

<sup>45</sup> *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5 ; Commissariat à la protection de la vie privée du Canada, « Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology » (dernière modification : 10 juin 2021), en ligne (pdf) : *Gouvernement du Canada* < <https://cutt.ly/NF5w9hQ> > [Vie privée].

<sup>46</sup> Plus de 600 agences policières à travers le monde font usage de la technologie *Clearview AI* : (Kashmir Hill, « The Secretive Company That Might End Privacy as We Know It », *The New York Times* (18 janvier 2020) en ligne: < <https://cutt.ly/sF5w5AF> >).

<sup>47</sup> Colin Bennett et Robin Bayley, « Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments » dans Bart van der Sloot et al, dir, *Exploring the Boundaries of Big Data*, 1e éd, Amsterdam, Amsterdam University Press, 2016, 205 à la p 209.

ou à des affaires sexuelles impliquant des mineurs. Près de 85 % des recherches restantes étaient à leur tour, de motifs inconnus, la GRC n'étant pas en mesure d'en rendre compte lors de l'enquête du Commissaire. Ainsi, face à des statistiques si hétérogènes et un manque flagrant de transparence, il est donc facile de concevoir que l'utilisation de l'IA dans de tels cas, peut facilement alimenter la méfiance historique de certaines communautés vulnérables, vis-à-vis les forces de l'ordre étatiques<sup>48</sup>. Cette conclusion est en outre miroitée par les commentaires des auteurs Bennett et Bayley, qui expliquent que la transparence est une pierre angulaire permettant de renforcer « powerful social norms »<sup>49</sup>, ici, la confiance du public dans les institutions étatiques.

En somme, nous pouvons donc voir que l'utilisation d'algorithmes par le gouvernement peut avoir une incidence profonde sur la vie privée du public. Ainsi, il est légitime d'explorer le cadre juridique encadrant cette matière, et les balises prévues par le gouvernement pour éviter de possibles abus de données privées.

### **La réponse du droit et certaines pistes de solutions**

Enfin, examinons dans cette dernière partie l'état de la législation canadienne face aux problématiques précitées, dans le but ultime d'essayer de déboucher sur des solutions. Traitons successivement des décisions automatisées, et ensuite le problème des données privées.

- **Favoriser la transparence et l'équité procédurale pour combattre la discrimination**

D'abord, la transparence et l'équité procédurale sont d'importance capitale en matière de décisions automatisées. Les conséquences de telles décisions pouvant avoir des effets graves sur la vie des justiciables, je suis donc d'avis qu'il est de la responsabilité de l'état d'assurer un encadrement réglementaire adéquat en cette matière. En ce sens, d'après moi, la LRPDE canadienne bénéficierait grandement de dispositions similaires aux

---

<sup>48</sup> *Vie privée, supra* note 45.

<sup>49</sup> *Bennett, supra* note 47.

articles 15 et 22 du RGPD. Effectivement, prendre inspiration de l'article 15(1)h) RGPD<sup>50</sup> permettra de rendre le processus décisionnel automatisé plus transparent pour le justiciable, car ce dernier pourra dès lors avoir accès aux « informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences » qui sous-tendent sa décision<sup>51</sup>. Cet article permettra ainsi de contourner le dilemme du « black box », car le justiciable pourra alors formuler de manière structurée et ordonnée une contestation de la décision prise à son égard. Parallèlement, l'adoption d'une disposition semblable à l'article 22 RGPD<sup>52</sup>, aura comme effet de remettre l'humain dans l'équation, en octroyant un pouvoir de contestation au justiciable, si ce dernier est soumis à une décision découlant d'un système automatisé. D'autant plus, le justiciable aura la possibilité « d'exprimer son point de vue et de contester la décision », constituant donc un prolongement du droit à l'explication précité. Dans ce cadre, l'homme, certes moins efficace que la machine, aura comme rôle d'apporter des nuances aux décisions automatisées de la machine, et en d'autres termes, de l'assister. Ainsi, à notre avis, l'ajout de dispositions inspirées du RGPD dans le contexte canadien permettra dès lors de rebalancer le terrain, en offrant au justiciable un processus décisionnel transparent et respectueux des règles d'équité procédurale, favorisant donc une plus grande équité.

En outre, pour combattre le problème des biais algorithmiques, à mes yeux, il est important de « continually position (...) development and use decisions in the wider context of historical and structural injustices and systemic racism »<sup>53</sup>. Ainsi, j'estime qu'un système similaire aux « principes Gladue »<sup>54</sup>

---

<sup>50</sup> CE, *Règlement (CE) 679/2016 de la Commission du 27 janvier 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, [2016] JO, L 119/4, art 15(1)h) [RGPD].

<sup>51</sup> *Ibid.*

<sup>52</sup> *Ibid.*, art 22.

<sup>53</sup> Leslie, *supra* note 12 à la p 41.

<sup>54</sup> R. c. *Gladue*, [1999] 1 RCS 688; Marie-Ève Sylvestre et Julie Perreault, « L'obligation judiciaire de tenir compte du statut autochtone et les principes Gladue » (2017), en ligne (pdf): CERP QC < <https://cutt.ly/AF5pZNN> >.

pourrait être instauré pour éviter d'indûment discriminer certaines populations lors de la confection d'algorithmes. Cette proposition d'idée pourrait prendre la forme d'une liste de contrôle obligatoire à laquelle les développeurs d'IA devront se soumettre aux étapes préliminaires de la création d'algorithmes. Cette liste pourra notamment comporter certaines contraintes, comme des quotas de personnes sous-représentées devant prendre part au projet, une parité entre les femmes et les hommes, etc. J'estime que cette solution pourra permettre de combattre de manière efficace le problème des biais algorithmiques.

- **Vers un changement de paradigme juridique en matière de protection des données ?**

Ensuite, comme il a été examiné précédemment, dans le cadre de l'investigation de la GRC, la critique principale formulée à l'égard de celle-ci était l'utilisation de photos recueillies illégalement par l'application *Clearview AI* (sans le consentement des usagers de l'internet). À cet effet, en matière de protection des données, au palier fédéral canadien, il existe la LPRPDE, une loi qui s'ancre dans un modèle de choix du consommateur, « notice-and-choice »<sup>55</sup>. Suivant ce modèle, les données des individus « may not be used for a different purpose without the individual's knowledge and consent, or unless there is a separate statutory justification »<sup>56</sup>. Ainsi, le consommateur moyen voulant accéder à un site internet par exemple, aura comme obligation de consentir par le biais d'une bannière, aux politiques de confidentialité dudit site. Toutefois, en raison de la nature générale, peu informative et ennuyeuse des conditions d'usage, plusieurs consommateurs décident de consentir sans même prendre connaissance des conditions, une

---

<sup>55</sup> Robert Sloan et Richard Wagner, « Beyond Notice and Choice: Privacy, Norms, and Consent » (2014) 14:1 High Tech LJ 340 à la p 359 ; David Thompson, « "I Agreed to What?": A Call for Enforcement of Clarity in the Presentation of Privacy Policies » (2012) 35:1 Hastings Comm & Ent LJ 203 à la p 204.

<sup>56</sup> *Bennett*, supra note 47.

pratique qui démontre donc d'après nous, la futilité d'un tel modèle de protection des données<sup>57</sup>.

Préalablement, à mon sens, une réponse moins draconienne à ce problème (conservant la valeur normative du consentement) est envisageable si nous suivons une proposition du rapport *Big Data and Privacy: A Technological Perspective*<sup>58</sup>, présentée à la maison blanche. Les auteurs du rapport proposent de créer une tierce partie qui sera chargée de recueillir un ensemble de standards de préférence en matière de vie privée des membres du public. Ensuite, chaque fois qu'un site web ou organe gouvernemental aura besoin de recueillir l'information privée des membres du public, ceux-ci devront se fier au standard préétabli pour déterminer si cette collecte de données a été autorisée d'avance. Suivant ce modèle, nous évitons un consentement répété et vide provenant des consommateurs.

À l'inverse, face à ce constat flagrant, quant à l'inefficacité de la législation contemporaine, nous considérons qu'il peut aussi être pertinent de transférer un fardeau plus important en matière de protection des données aux compagnies profitant de ces mêmes données. En effet, c'est cette même idée du renversement de fardeau qui a récemment fait surface dans le cadre du rapport de la *proposition européenne sur l'IA*<sup>59</sup>. Certes, il ne s'agit qu'une proposition non-contraignante, mais son implémentation pourrait constituer, un changement de paradigme massif attendu depuis longtemps par les auteurs de ce milieu. Effectivement, pour l'auteur Van der Sloot par

---

<sup>57</sup> Daniel Solove, « Privacy Self-Management and the Consent Dilemma » (2013) 126:7 Harv L Rev 1880 ; François Rigaux, « La protection de la vie privée et des autres biens de la personnalité », 1e éd, Bruxelles, Éditions Bruylant, 1991 à la p 621 ; Sloan, *supra* note 55, aux pp 16-19.

<sup>58</sup> É-U, President's Council of Advisors on Science and Technology, *Report to the president - Big Data and Privacy: A Technological Perspective*, Committee Print, 2014 à la p XII ; Robert Gellman, « Is there a role for consent in privacy? » (30 juin 2021), en ligne (blogue): IAPP < <https://cutt.ly/WF5hrwz> >.

<sup>59</sup> Commission Européenne, « Proposition De Règlement Du Parlement Européen Et Du Conseil Etablissant Des Règles Harmonisées Concernant L'intelligence Artificielle (Législation Sur L'intelligence Artificielle) Et Modifiant Certains Actes Législatifs De L'union » (2021), en ligne (pdf): EUR-Lex < <https://cutt.ly/9Gw5ilF> >.

exemple, l'emploi du phénomène « Big Data » dans des technologies telles *Clearview AI*, suscite au sein de nos sociétés :

fundamental tension between the traditional legal and philosophical discourse and the new technological reality: while the traditional discourse focuses on individual rights and individual interests, data processing often affects a structural and societal interest and, in many ways, transcends the individual<sup>60</sup>

Pour remédier à cette problématique, Van der Sloot propose la « agent-based theorie »<sup>61</sup>, une doctrine opérant un changement de paradigme selon laquelle « the focus is no longer on concrete individual interests, but on the general interest of being protected against abuse of power and on the positive obligation of states to use their power to facilitate human flourishing »<sup>62</sup>. Dorénavant, le fardeau est renversé, et l'acteur (celui profitant des données), est affecté d'obligations positives d'agir de manière juste et raisonnable (fair and conscionable<sup>63</sup>) selon « soft law, general ethical rules, and general duties of care »<sup>64</sup>. Corrélativement, le fardeau qui existait jadis sur les épaules du public est quant à lui allégé<sup>65</sup>. En un mot, suivant cette doctrine « préventive de dégâts », les actions de l'acteur, que ça soit l'état ou une compagnie privée, sont minutieusement examinées pour éviter des abus de pouvoir émanant de l'accès à des quantités massives de données

<sup>60</sup> Bart van der Sloot, « The Individual In The Big Data Era: Moving Towards an Agent-Based Privacy Paradigm » dans Bart van der Sloot et al, dir, *Exploring the Boundaries of Big Data*, 1e éd, Amsterdam, Amsterdam University Press, 2016, 177 à la p 184 [Van der Sloot, « Paradigm »].

<sup>61</sup> *Ibid* à la p 192.

<sup>62</sup> *Ibid* à la p 196.

<sup>63</sup> John Rothchild, « Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else) » (2018) 66:559 Clev St L Rev 559 aux pp 639-46.

<sup>64</sup> Van der Sloot, « Paradigm », *supra* note 60 à la p 199.

<sup>65</sup> D'après cette ligne de pensée, « le consentement ne constitue pas un fondement juridique valable pour la plupart des échanges de données » : (Christophe Lazaro et Daniel Le Métayer, « Le consentement au traitement des données à caractère personnel : une perspective comparative sur l'autonomie du sujet » (2015) 48:3 RJT 765 à la p 805).

privées. L'implémentation d'une pratique similaire dans le contexte canadien aurait d'après moi, évité le problème précité entourant la GRC.

○ **La vie privée et l'extraterritorialité**

Enfin, brièvement et parallèlement à la dernière sous-partie, le débat sur la vie privée soulève aussi un problème de compétence judiciaire. C'est notamment le cas de l'utilisation des données d'un national, par une force policière étrangère, à l'image de la situation précitée de la banque d'images de *Clearview AI*. Dans le contexte canadien, il ne semble pas encore avoir de législation traitant de ce problème. Ainsi, à notre avis, il serait souhaitable que la législature canadienne s'inspire de l'article 3 du *Règlement Général sur la Protection des Données* (ci-après RGPD) afin de fournir une protection à portée extraterritoriale aux Canadiens dont les données se trouvent à l'étranger. En somme, précisons que l'extraterritorialité est une vaste problématique pouvant faire l'objet d'une recherche à elle seule ; en traiter dans un espace si limité ne rendrait pas justice à la complexité du sujet et ses tendances jurisprudentielles récentes<sup>66</sup>.

## **Conclusion**

Pour conclure, il y a donc lieu de reconnaître que la réglementation de l'IA est une nécessité de premier plan dans nos sociétés modernes afin d'éviter plusieurs problématiques tels la discrimination ou l'usage abusif des données. Dans le contexte canadien, il reste encore plusieurs ajustements à faire, et l'état doit donc tenter de mettre à niveau sa législation suivant certains modèles européens tel le RGPD, qui offrent des mécanismes de sauvegarde aux justiciables. De même, si la législation semble avoir atteint sa limite d'utilité face à certaines problématiques modernes, telle la gestion des données, l'état doit songer à un changement de paradigme afin

---

<sup>66</sup> Karen Eltis, « L'extraterritorialité, l'intelligence artificielle et la justice : Une étude préliminaire The Extraterritorial Automatization of Justice : Will the Black Box decide? AI and Bias in Judicial Decision Making from a Comparative Perspective » (2021), en ligne (pdf): SSRN < <https://cutt.ly/DF515d8> > ; *Google Inc. c. Equustek Solutions Inc*, 2017 CSC 34; *Douez c. Facebook, Inc*, 2017 CSC 33.

d'adopter des solutions davantage créatives pour y répondre, à l'image de la récente *proposition européenne sur l'IA*.

Néanmoins, en raison de la démocratisation du numérique dans nos sociétés modernes, il faut garder à l'esprit que la technologie évolue à un rythme effréné. Ainsi, les technologies d'aujourd'hui et leurs solutions corrélatives ne seront plus celles de demain. Effectivement, l'analyse prédictive est efficace de nos jours par exemple, mais il est concevable qu'elle a un potentiel de nous piéger dans nos circonstances actuelles, une perspective effrayante pour l'évolution de la jurisprudence. Similairement, est-ce que la neutralité est nécessaire pour faire avancer l'égalité des systèmes algorithmiques, ou est-il plus adapté de porter une attention particulière à la mise en contexte et la compassion, reliée à la reconnaissance de la dignité ? L'état qui trouvera donc une juste balance entre l'encadrement législatif et la prolifération de la technologie aura par conséquent accès à son véritable potentiel. Il s'agit d'un jeu risqué à suivre de près dans les années qui arrivent, car la technologie, au-delà de toucher les droits des justiciables, est aussi devenu plus récemment, un outil important de géopolitique<sup>67</sup>.

---

<sup>67</sup> Paresh Dave et Jeffrey Dastin, « Exclusive: Ukraine has started using Clearview AI's facial recognition during war », *Reuters* (14 mars 2022) en ligne: < <https://cutt.ly/tF5zdUa> >.