

Intelligence artificielle et protection de la vie privée

La perspective des consommateurs

RAPPORT DE RECHERCHE

Rapport réalisé par Option consommateurs en collaboration avec Maya Cachecho, Ph.D.,
Sandrine Prom Tep, Ph.D., Evelyne Jean-Bouchard, Ph.D. et Pablo Jose Garcia

et présenté au Commissariat à la protection de la vie privée du Canada

2021

Ce projet a été financé par le Commissariat à la protection de la vie privée du Canada (CPVP); les opinions exprimées ici sont celles de l'auteur et ne reflètent pas nécessairement celles du CPVP.

La reproduction de ce rapport, tout ou partie, est autorisée, à condition que la source soit mentionnée. Sa reproduction ou toute allusion à son contenu à des fins publicitaires ou lucratives sont toutefois strictement interdites.

Dépôt légal
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISBN 978-2-89716-067-8

Option consommateurs
50, rue Sainte-Catherine Ouest, bureau 440
Montréal (Québec)
H2X 3V4
Téléphone : 514 598-7288
Télécopieur : 514 598-8511

Courriel : info@option-consommateurs.org
Site Internet : www.option-consommateurs.org

Table des matières

Option consommateurs	v
Remerciements	vi
Résumé	vii
Introduction	8
Objectifs de la recherche et méthodologie.....	8
1. Contexte	9
1.1. Une définition de l'IA	9
1.2. L'éveil d'une industrie	10
1.3. Des promesses innombrables	11
2. L'IA et les consommateurs	13
2.1. Les rouages du traitement de données	14
2.1.1. Une large collecte de données	14
2.1.2. Une information parcellaire sur l'IA	15
2.1.3. Un encadrement volontariste.....	17
2.1.4. Le contrôle limité des consommateurs	18
2.2. Portrait des applications de l'IA	19
2.2.1. Personnaliser l'expérience-utilisateur	19
2.2.2. Prédire les tendances du marché	19
2.2.3. Donner accès à l'information.....	20
2.2.4. Faciliter la vie des consommateurs	21
2.2.5. Se protéger des menaces.....	22
2.2.6. Reconnaître les images et les visages.....	22
2.2.7. Interagir avec les consommateurs.....	23
2.2.8. Conseiller les consommateurs.....	24
2.2.9. Prendre des décisions automatisées	25
3. Les enjeux de l'IA pour les consommateurs	26
3.1. Une intrusion dans la vie privée.....	26
3.2. Des systèmes opaques	27
3.3. Le risque de préjudice économique	28
3.3.1. Des techniques de persuasion invasives.....	28
3.3.2. Personnaliser les prix en ligne	29
3.3.3. Fausser le libre-marché	31
3.4. Le risque de discrimination	31
3.5. Erreurs et faux positifs	33
4. Regard sur le cadre juridique canadien	34
4.1. Des données protégées par la loi.....	34
4.2. Les droits individuels des consommateurs	35
4.2.1. Les écueils du consentement dans l'environnement de l'IA	36
4.2.2. Mieux informer : le droit à une explication	37
4.2.3. Améliorer le consentement : le droit de contester	38
4.3. L'encadrement des utilisations et des effets de l'IA	39
4.3.1. Des balises ténues.....	39
4.3.2. Le droit à l'égalité	40
4.3.3. Des interdictions à clarifier	41
4.4. Les écueils de la mise en œuvre de la loi	42
4.4.1. La transparence des systèmes d'IA et la prévention des préjudices.....	42

4.4.2. Le besoin de normes contraignantes.....	43
5. S’inspirer de l’étranger	45
5.1. Europe : un cadre inspirant à plusieurs égards.....	45
5.1.1. Des obligations d’information bonifiées.....	45
5.1.2. Écarter le consentement... à certaines conditions	46
5.1.3. Le droit d’opposition et de révision.....	46
5.2. États-Unis : un cadre minimaliste	47
Conclusion et recommandations	50

Option consommateurs

MISSION

Option consommateurs est une association à but non lucratif qui a pour mission de promouvoir et de défendre les droits et les intérêts des consommateurs et de veiller à ce qu'ils soient respectés.

HISTORIQUE

Issue du mouvement des associations coopératives d'économie familiale (ACEF), et plus particulièrement de l'ACEF de Montréal, Option consommateurs existe depuis 1983. En 1999, elle a regroupé ses activités avec l'Association des consommateurs du Québec (ACQ) qui existait depuis plus de 50 ans et accomplissait la même mission qu'elle.

PRINCIPALES ACTIVITÉS

Option consommateurs aide les consommateurs qui vivent des difficultés, les reçoit en consultation budgétaire et donne des séances d'information sur le budget, l'endettement, le droit de la consommation et la protection de la vie privée.

Chaque année, nous réalisons des recherches sur des enjeux de consommation d'importance. Nous intervenons également auprès des décideurs et des médias pour dénoncer des situations inacceptables. Lorsque nécessaire, nous intentons des actions collectives contre des commerçants.

MEMBERSHIP

Pour faire changer les choses, les actions d'Option consommateurs sont multiples : recherches, actions collectives et pressions auprès des instances gouvernementales et des entreprises. Vous pouvez nous aider à en faire plus en devenant membre d'Option consommateurs au www.option-consommateurs.org.

Remerciements

Cette recherche a été réalisée par l'équipe d'Option consommateurs, avec le soutien de Sandrine Prom Tep, Ph.D., professeure agrégée au Département de marketing et l'École des Sciences de la Gestion de l'UQAM, Maya Cachecho, Ph.D., chercheure et coordonnatrice scientifique du projet ADAJ et Centre de recherche en droit public, Evelyne Jean-Bouchard, Ph.D., chercheure postdoctorale au Centre de recherche en droit public, ainsi que Pablo Jose Garcia, étudiant à la Maîtrise en sciences de la gestion (marketing) à l'UQAM.

Nous tenons également à remercier les employés, stagiaires et bénévoles qui oeuvrent à Option consommateurs et qui, de près ou de loin, ont collaboré à cette recherche. Une part appréciable de cette recherche repose sur des entrevues avec des experts du domaine de l'IA et du droit. Option consommateurs tient également à remercier tous ces experts d'avoir généreusement accepté d'accorder une entrevue.

Résumé

L'intelligence artificielle (IA) occupe une place grandissante dans la vie des consommateurs canadiens. L'IA peut notamment contribuer à personnaliser l'expérience-utilisateur, prédire les comportements des consommateurs, donner accès à l'information, interagir avec la clientèle ou prendre des décisions automatisées quant à l'accès à un service.

Les entreprises en ligne recueillent une quantité phénoménale de données sur les consommateurs, mais ne donnent que de l'information parcellaire quant au traitement de ces données par leurs systèmes d'IA. Quelques entreprises affirment avoir adopté des principes encadrant leur utilisation de l'IA, mais ce cadre reste fondé sur l'autoréglementation. Par ailleurs, le contrôle qu'elles offrent aux consommateurs sur leurs renseignements personnels reste limité.

L'IA comporte des avantages pour les consommateurs, mais elle pose aussi des risques d'atteinte à la vie privée, d'exclusion de groupes vulnérables, d'exploitation économique des consommateurs ou simplement de faux positifs. De plus, l'IA exacerbe l'asymétrie d'information entre les consommateurs et les commerçants, en raison de l'opacité du traitement de données qu'elle effectue.

L'emploi de l'IA dans un contexte commercial expose la désuétude des lois canadiennes sur la protection des renseignements personnels. En guise de solutions, Option consommateurs propose notamment de bonifier les droits individuels des consommateurs pour leur permettre d'obtenir une explication quant au résultat d'un traitement de données et d'en demander la révision, d'interdire expressément les utilisations de renseignements personnels ayant pour effet de causer une discrimination illicite ou une exploitation économique des consommateurs, et de renforcer les pouvoirs des autorités d'application de la loi.

Introduction

Au cours des dernières années, l'intelligence artificielle (IA) a connu une croissance phénoménale et s'est intégrée progressivement dans une myriade de secteurs économiques. Désormais, elle entre en interaction avec les consommateurs d'une multitude de façons. Faire une recherche sur le web, interagir avec un assistant vocal, demander l'itinéraire à son navigateur de bord, traduire un texte en ligne sont autant d'exemples de services propulsés par l'IA.

Malgré les promesses de l'IA, son utilisation par les entreprises présente des risques pour les consommateurs. Atteinte à la vie privée, discrimination, exploitation économique, exclusion, opacité, faux positifs : les enjeux soulevés par l'IA sont nombreux pour les consommateurs. Pourtant, alors que les lois canadiennes sur la protection des renseignements personnels n'ont pas été conçues pour encadrer cette technologie, son déploiement se poursuit inéluctablement dans le secteur privé.

Objectifs de la recherche et méthodologie

Ce rapport s'intéresse à la perspective des consommateurs face à l'intelligence artificielle. Compte tenu de la place grandissante qu'occupe l'IA chez les entreprises, nous avons voulu en savoir davantage sur l'ampleur du phénomène, sur les avantages et les risques que comporte l'utilisation de l'IA dans un cadre commercial, de même que sur les meilleures solutions pour protéger adéquatement les consommateurs dans cet environnement.

Pour ce faire, nous avons documenté les applications de l'IA par les plus importantes entreprises offrant des services en ligne au Canada (section 2). Cette analyse nous a ensuite permis d'identifier les enjeux que soulève le déploiement de l'IA dans ces entreprises, du point de vue des consommateurs (section 3). Finalement, pour trouver des pistes de solutions, nous avons exploré le droit applicable en matière de protection des renseignements personnels, au Canada et à l'étranger (section 4).

Afin d'éclairer notre analyse, nous avons réalisé des entrevues avec des juristes et des experts du domaine de l'IA. Nous avons interviewé Hugo Cyr, professeur titulaire à la Faculté de science politique et de droit à l'UQAM, Karine Gentelet, professeure agrégée à l'UQO et titulaire de la Chaire Abéona-ENS-OBVIA en intelligence artificielle et justice sociale, Martin Gibert, chercheur en éthique de l'intelligence artificielle à l'Université de Montréal, Audrey Houle, juriste spécialisée en technologies numériques, Richard Khoury, professeur agrégé au Département d'informatique et de génie logiciel de l'Université Laval, Sarit Kimberly Mizrahi, doctorante à l'Université de Montréal, Marc Lacoursière, professeur titulaire à la faculté de droit de l'Université Laval, ainsi que John Lawford, directeur général du Centre pour la défense de l'intérêt public.

1. Contexte

1.1. Une définition de l'IA

L'intelligence artificielle est une notion imprécise qui n'a pas de définition unique. L'IA peut désigner des concepts différents, ayant différents niveaux de sophistication et employant divers procédés techniques.

Dans son expression la plus simple, on peut considérer que l'IA réfère à tout système informatique en mesure d'effectuer des tâches généralement associées à l'intelligence humaine¹. L'IA tend à imiter des fonctions cognitives de l'humain telles que la perception, l'apprentissage, la résolution de problèmes ou la compréhension du langage². En pratique, l'IA est toutefois bien loin de parvenir à reproduire l'intelligence de l'humain de manière convaincante. L'IA d'aujourd'hui est dite « étroite », ou « appliquée », et sert à effectuer une ou plusieurs tâches spécifiques, comme servir d'opposant dans des jeux de société, effectuer de la reconnaissance d'images ou interpréter le langage humain³.

Les procédés techniques utilisés pour supporter l'IA peuvent également varier. Les développements récents de l'IA font principalement appel à l'apprentissage automatique (*machine learning*), par lequel des algorithmes traitent d'immenses quantités de données et sont capables d'apprendre de leurs propres erreurs ou succès pour améliorer continuellement leur efficacité. L'apprentissage profond (*deep learning*) est un type plus sophistiqué d'apprentissage automatique. Sa « profondeur » provient de diverses couches de « neurones artificiels » qui permettent aux logiciels de traiter de plus grandes quantités de données simultanément, avec divers niveaux d'abstraction⁴. Cette technologie permet d'identifier des corrélations dans les données qu'il serait difficilement possible de découvrir avec des fonctions statistiques traditionnelles.

En somme, tout comme l'intelligence humaine, l'IA reste un concept polysémique et diffus. De surcroît, la définition de l'IA est fuyante, c'est-à-dire que les progrès technologiques semblent

¹ B. J. COPELAND, « Artificial intelligence », *Encyclopedia Britannica*, 11 août 2020, <https://www.britannica.com/technology/artificial-intelligence>; Matthew U. SCHERER, « Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies », (2016) 29-2 *Harvard Journal of Law & Technology* 354, p. 362. Si ces définitions décrivent l'IA par ses différentes applications, d'autres définitions décrivent plutôt l'IA comme un domaine d'étude. C'est le cas de la définition proposée par l'Office de la langue française, qui décrit l'IA comme un champ interdisciplinaire théorique et pratique « qui a pour objet la compréhension de mécanismes de la cognition et de la réflexion, et leur imitation par un dispositif matériel et logiciel, à des fins d'assistance ou de substitution à des activités humaines ». Voir : COMMISSION D'ENRICHISSEMENT DE LA LANGUE FRANÇAISE, *Vocabulaire de l'intelligence artificielle (liste de termes, expressions et définitions adoptés)*, Journal officiel électronique authentifié, n° 0285, 9 décembre 2018, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037783813>

² UNESCO, *Steering AI and Advanced ICTs for Knowledge Societies: A Rights, Openness, Access, and Multi-stakeholder Perspective*, UNESCO Publishing, 2019, p. 24

³ Ryan CALO, « Artificial Intelligence Policy: A Primer and Roadmap », (2018) 3:2 *U of Bologna L Rev* 180, p. 187; Iria GIUFFRIDA, Fredric LEDERER et Nicolas VERMEYS, « A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law », (2018) 68:3 *Case W Res L Rev* 747, p. 751-756; OCDE, *L'intelligence artificielle dans la société*, Éditions OCDE, 2019, p. 24

⁴ Muhammad TALHA, Shaikat ALI, Sajid SHAH, F.G. KHAN et Javed IQBAL, « Integration of Big Data and Deep Learning », dans *Deep Learning: Convergence to Big Data Analytics*, Springer, 2019, p. 43-52

constamment la repousser vers des technologies de plus en plus avancées⁵. Cela dit, dans une perspective de protection du consommateur, les distinctions entre les divers niveaux d'IA et les techniques qui les supportent apparaissent superfétatoires. En effet, bien que certains types d'algorithmes employés par les entreprises ne soient pas nécessairement considérés comme de l'IA selon certaines définitions, leur mise en application dans un contexte commercial soulève des enjeux relativement similaires du point de vue du public⁶.

En conséquence, pour les fins de la présente recherche, il paraît plus judicieux de se rabattre sur une définition large et englobante de l'IA. Nous considérerons donc comme des systèmes d'IA autant l'apprentissage automatique que d'autres formes d'algorithmes complexes employés qui traitent automatiquement des données personnelles; ces systèmes peuvent notamment être utilisés par les entreprises pour personnaliser les services fournis aux consommateurs, faire des prévisions sur leurs comportements, leur faire des recommandations ou même prendre des décisions sur eux⁷.

1.2. L'éveil d'une industrie

Dès les années 1950, des auteurs évoquaient l'idée d'une machine en mesure de reproduire l'intelligence humaine⁸. Cependant, imiter les processus cognitifs de l'humain, comme la capacité de comprendre le langage ou de reconnaître les images, n'est pas mince affaire. Pendant des décennies, l'IA a achoppé à obtenir des résultats convaincants et a connu plusieurs périodes de stagnation.

Au tournant des années 2010, en raison de la combinaison de plusieurs facteurs, on assistera à une sortie de cet « hiver » de l'IA⁹. Parmi ces facteurs, notons l'accroissement exponentiel de la puissance de calcul des ordinateurs, qui rendra possible les techniques d'apprentissage profond. De même, le développement du web permettra de générer une quantité jamais égalée de données; ces données massives¹⁰ (*Big Data*) pourront nourrir l'exploration de données¹¹ (*data mining*) propulsée par l'IA.

⁵ Matthew U. SCHERER, « Regulating Artificial Intelligences Systems: Risks, Challenges, Competencies, and Strategies », (2016) 29-2 *Harvard Journal of Law & Technology* 354, p. 360-361

⁶ CNIL, *Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, France, décembre 2017, p. 18

⁷ Cette définition vise à s'arrimer à la définition de « système d'IA » proposée par l'OCDE, qui le définit comme « un système automatisé qui, pour un ensemble donné d'objectifs définis par l'homme, est en mesure d'établir des prévisions, de formuler des recommandations, ou de prendre des décisions influant sur des environnements réels ou virtuels ». Voir : OCDE, *L'intelligence artificielle dans la société*, Éditions OCDE, 2019, p. 26

⁸ Alan TURING, « Computing machinery and intelligence », (1950) 59 *MIND* 433; James MOOR, « The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years *AI Magazine* », (2006) 27-4 *AI Magazine* 87

⁹ Kevin KELLY, *The Three Breakthroughs That Have Finally Unleashed AI on the World*, WIRED, 27 octobre 2014, <https://www.wired.com/2014/10/future-of-artificial-intelligence/>

¹⁰ La firme de recherche Gartner définit le *Big Data* comme étant : « Un actif de données à fort volume, à grande vitesse et de grande variété qui exige des moyens novateurs et rentables de traitement de l'information qui permettent une meilleure compréhension, prise de décision et une automatisation de certains processus ». Voir : <https://www.gartner.com/en/information-technology/glossary/big-data>

¹¹ L'Office québécois de la langue française (OQLF) définit l'exploration de données comme étant un « processus de recherche et d'analyse qui permet de trouver des corrélations cachées ou des informations nouvelles, ou encore, de dégager certaines tendances ». Voir : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8375476

Ces percées permettront à l'IA de faire une entrée accélérée dans les entreprises. Les géants du numérique – Google, Facebook, Apple, Amazon et Microsoft – emploient désormais à large échelle l'IA dans leurs activités courantes. Ces grandes firmes se sont dotées de divisions dédiées à la recherche et au développement en IA, telles que Google AI et Facebook AI, et multiplient les acquisitions d'entreprises dans ce domaine¹². Google donne un aperçu impressionnant de ses travaux en ce domaine, notamment en publiant diverses expérimentations qu'elle effectue avec l'apprentissage automatique¹³.

L'IA n'est toutefois pas seulement réservée qu'aux grandes entreprises. Ces technologies sont aussi accessibles à de plus petites entreprises, sous forme de service fourni à des tiers. Des entreprises telles que la montréalaise Lightspeed ou la torontoise Shopify offrent ainsi la possibilité aux détaillants d'intégrer toutes leurs opérations au sein d'une seule plateforme propulsée par l'IA¹⁴. Les géants du numérique permettent aussi à de plus petites entreprises d'utiliser leurs capacités en IA, sous forme de service¹⁵.

En somme, si l'IA est une idée ancienne, son déploiement à grande échelle dans le secteur privé est un phénomène plutôt récent. Les débouchés commerciaux de l'IA restent cependant loin des scénarios de science-fiction qui mettent en scène des superordinateurs omniscients devenus malveillants. Les utilisations de l'IA sont bien plus subtiles, voire banales, se traduisant en des systèmes informatiques qui, de mille et une façons, contribuent à optimiser les activités des entreprises.

1.3. Des promesses innombrables

Loin d'être une curiosité confinée aux laboratoires informatiques, l'IA fait désormais partie intégrante de la vie des consommateurs. En fait, tout comme l'intelligence humaine, ses applications semblent illimitées. S'il faut en croire les promesses de l'industrie, l'IA pourra notamment supporter le secteur agricole dans les pays en voie de développement¹⁶, prédire les

¹² Par exemple, en 2014, a acquis la firme *DeepMind*, qui emploie l'IA dans divers secteurs tels que le transport, l'efficacité énergétique de ses centrales de serveurs ainsi que le domaine médical. Voir : Amy THOMSON, « Google Waives \$1.5 Billion DeepMind Loan as AI Costs Mount », *Bloomberg*, 17 décembre 2020, <https://www.bloomberg.com/news/articles/2020-12-17/deepmind-says-2019-revenue-jumped-158-on-ai-research-work>. Récentement, Apple a acquis la jeune pousse *Xnor AI* afin d'intégrer dans ses appareils des processeurs capables de supporter des logiciels utilisant l'IA. Voir : Will KNIGHT, « Apple's Latest Deal Shows How AI Is Moving Right Onto Devices », *Wired*, 17 janvier 2020, <https://www.wired.com/story/apples-deal-shows-ai-moving-devices/>

¹³ <https://experiments.withgoogle.com/collection/ai>

¹⁴ BANQUE DE DÉVELOPPEMENT DU CANADA, *Free and low-cost e-commerce software for your business*, avril 2020, <https://www.bdc.ca/en/articles-tools/technology/free-low-cost-applications/e-commerce-free-low-cost-options>

¹⁵ Voir, par exemple, la liste de « produits d'IA et de machine learning » publiée par Google : <https://cloud.google.com/products/ai>. Google offre aussi la plateforme TensorFlow, un outil d'apprentissage automatique disponible en code source ouvert : <https://www.tensorflow.org/>. De son côté, Facebook partage en code source ouvert l'outil PyTorch : https://ai.facebook.com/tools?utm_source=hp#frameworks-and-tools. Amazon offre également des services d'IA pour les développeurs : <https://aws.amazon.com/fr/machine-learning/ai-services/>

¹⁶ <https://blog.google/technology/ai/machine-learning-meets-african-agriculture/>

inondations¹⁷, contribuer aux efforts de préservation de la faune¹⁸, combattre la désinformation¹⁹, trouver de nouvelles exoplanètes²⁰, être employée à des fins artistiques²¹, voire même contribuer à prévenir des suicides²².

Les promesses sont particulièrement nombreuses dans le domaine de la santé. Des systèmes d'IA permettent de comparer de larges bases de données entre elles pour identifier des anomalies génétiques chez des personnes présentant des symptômes similaires, et qui auraient autrement échappé à l'œil humain. Par exemple, en 2020, la filiale *DeepMind* de Google a réussi à entraîner un robot capable de détecter le cancer du sein avec un degré de précision semblable à celui d'un expert, tout en ayant un taux de faux positifs plus faible que les humains²³.

L'IA pourrait également être mise à profit par le secteur public. Des systèmes d'IA pourraient ainsi faciliter l'obtention de services gouvernementaux, par exemple en automatisant la délivrance de permis²⁴. Dans le domaine judiciaire, l'IA pourrait accompagner les juges dans leur prise de décision, notamment pour déterminer la sentence la plus appropriée à donner à une personne déclarée coupable. De manière particulièrement controversée, l'IA pourrait même être employée pour automatiser des drones militaires ou être employée de diverses manières dans le cadre de conflits armés²⁵.

Le domaine de la consommation n'échappe pas à la tendance. L'IA permet d'améliorer la qualité et l'efficacité des services que les consommateurs reçoivent, en tenant compte de leurs préférences et de leurs besoins. Elle permet aussi de rendre autonomes des appareils, par exemple en permettant à des véhicules de circuler sur les rues sans conducteur. De plus en plus, les services qu'offrent les grandes entreprises dans l'environnement numérique – dont Google, Facebook, Apple et Microsoft – sont ainsi propulsés par une forme ou une autre d'IA, qu'il s'agisse de techniques d'apprentissage profond ou d'autres algorithmes complexes de traitement des données.

¹⁷ <https://blog.google/technology/ai/tracking-our-progress-on-flood-forecasting/>

¹⁸ <https://news.microsoft.com/features/artificial-intelligence-makes-a-splash-in-efforts-to-protect-alaskas-ice-seals-and-beluga-whales/>

¹⁹ <https://blog.google/outreach-initiatives/google-org/fullfact-and-google-fight-misinformation/>

²⁰ <https://blog.google/technology/ai/hunting-planets-machine-learning/>

²¹ <https://ai.facebook.com/research/publications/a-universal-music-translation-network>

²² <https://blog.google/outreach-initiatives/google-org/trevor-project/>

²³ Nicole KOBIE, « DeepMind's new AI can spot breast cancer just as well as your doctor », *Wired*, 1^{er} janvier 2020, <https://www.wired.co.uk/article/deepmind-google-ai-breast-cancer>

²⁴ Aviv GAON et Ian STEDMAN, « A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada », (2019) 56-4 *Alta L Rev* 1137, p. 1150-1151

²⁵ *Id.*, p. 1154-1155

2. L'IA et les consommateurs

L'un des objectifs de cette recherche consiste à documenter les applications de l'IA par les plus importantes entreprises offrant des services en ligne au Canada. Pour y parvenir, nous avons employé plusieurs démarches méthodologiques complémentaires, incluant l'analyse des politiques de confidentialité et des sites web d'entreprises, la recherche documentaire ainsi que des entrevues avec des experts. Bien que ces démarches n'aient pas permis d'identifier avec précision chaque service propulsé par l'IA dans chaque entreprise sélectionnée, elles ont permis d'en donner une vue d'ensemble utile pour cerner les enjeux pour les consommateurs.

Pour les fins de notre analyse, nous avons sélectionné des entreprises parmi les plus importantes offrant des services en ligne aux consommateurs canadiens. Compte tenu de leur empreinte incontournable sur le web, nous avons d'abord sélectionné les grandes entreprises technologiques : Google, Facebook, Apple et Microsoft. Nous avons ajouté à cette sélection deux autres types d'entreprises qui occupent une place importante dans les activités économiques des consommateurs, soit les détaillants en ligne et les institutions financières. Pour chacune de ces catégories, nous avons sélectionné les quatre entreprises les plus populaires auprès des consommateurs canadiens²⁶.

Entreprise	Catégorie
Google	Entreprise numérique
Facebook	
Apple	
Microsoft	
Amazon	Commerce de détail
Walmart	
Costco	
La Baie d'Hudson	Institution financière
Banque Royale du Canada	
Banque TD	
Banque Scotia	
Banque de Montréal	

Nous avons analysé l'offre de service de chacune de ces entreprises en parcourant les représentations faites sur leurs sites Internet de même que leurs politiques de confidentialité.

Un premier constat de cette analyse tient en ce que le niveau de transparence varie d'une entreprise à l'autre. En plus de leur politique de confidentialité, de grandes entreprises telles que Google, Apple et Microsoft publient des pages web qui expliquent davantage la nature et

²⁶ Pour identifier les commerçants les plus populaires dans ces catégories, nous avons recouru aux classements effectués par la firme Statista. Voir : STATISTA, *Top online stores in Canada in 2019, by e-commerce net sales*, 2021, <https://www.statista.com/statistics/871090/canada-top-online-stores-canada-ecommercedb/>; STATISTA, *Largest banks in Canada in 2020, by total assets*, 2021, <https://www.statista.com/statistics/434554/leading-banks-in-canada-assets/>

l'utilisation des données collectées. À l'opposé, de plus petites entreprises, dont Costco et La Baie, offrent bien moins d'information au public quant à leurs pratiques.

2.1. Les rouages du traitement de données

Déterminer l'ampleur exacte des services propulsés par l'IA dans le secteur privé est un exercice imprécis, notamment en raison du peu d'information sur les traitements de données effectués par les entreprises. Si les entreprises recueillent une quantité phénoménale de données pour diverses utilisations (section 2.1.1), la part de l'IA dans cette équation reste difficile à déterminer (section 2.1.2). Malgré ce flou, certaines entreprises publient de l'information quant aux principes volontaires qu'elles ont adopté pour encadrer leurs systèmes d'IA (2.1.3). Finalement, le contrôle des consommateurs quant au traitement de leurs données reste limité (2.1.4).

2.1.1. Une large collecte de données

Les politiques de confidentialité des entreprises sont sans équivoque quant à la collecte massive de données qu'elles effectuent²⁷. Toutes énoncent de longues listes de renseignements pouvant être recueillis lors de l'utilisation de leurs services, notamment l'information fournie directement par l'utilisateur, les données techniques sur les appareils utilisés, l'historique web ou la géolocalisation. De même, diverses données biométriques peuvent également être recueillies, telles que les empreintes digitales, l'image du visage ou celle de l'iris²⁸.

En guise d'illustration, par la simple connexion du consommateur à son compte Google, cette firme peut recueillir toute l'information associée à ce compte via ses services tels que les courriels, les lieux géolocalisés dans Google Maps ou les mots-clefs recherchés sur le web. Amazon, de son côté, explique que la voix du consommateur peut être analysée pour en faire une empreinte lorsqu'il utilise l'assistant vocal :

« Alexa se sert d'enregistrements de votre voix afin de bâtir un profil acoustique des caractéristiques de votre voix. Alexa enregistre votre profil vocal dans le nuage et l'utilise pour vous reconnaître lorsque vous lui parlez. Cela lui permet de vous appeler par votre nom et de personnaliser votre expérience.²⁹ »

Les institutions financières peuvent également recueillir nombre de renseignements sur les consommateurs. En plus des données financières délicates qu'elles détiennent pour fournir leurs services, ces entreprises affirment aussi que les internautes qui visitent leur site web

²⁷ Cette large captation des données des internautes, déjà bien documentée dans la littérature. Voir : Alexandre PLOURDE, *Le prix de la gratuité : doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne?*, Option consommateurs, 2015, p. 18-22

²⁸ Le CPVP définit la biométrie comme étant « un éventail de techniques, d'appareils et de systèmes permettant aux machines de reconnaître des personnes ou de confirmer ou d'authentifier leur identité ». Voir : CPVP, *Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée*, février 2011. En ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/reenseignements-sur-la-sante-reenseignements-genetiques-et-autres-reenseignements-sur-le-corps/gd_bio_201102/

²⁹ <https://www.amazon.ca/-/fr/gp/help/customer/display.html?nodeId=201602230>

peuvent faire l'objet d'une collecte de données sur leurs activités en ligne, notamment à des fins publicitaires.

Certaines entreprises, dont Google et Facebook, ont également la capacité de pister les internautes sur de nombreux sites et applications tiers. Facebook reçoit ainsi une multitude de données d'un grand nombre d'applications mobiles, et peut toutes les rattacher à un identifiant unique³⁰. Enfin, notons que plusieurs ont intégré leurs services dans une myriade d'objets connectés, qui peuvent encore là être des points de collecte de données³¹.

Les entreprises énoncent de nombreuses utilisations qu'elles peuvent faire des données recueillies, allant de la simple fourniture de leurs services à la personnalisation, en passant par la reconnaissance faciale, l'analyse de statistiques ou la recherche. Plusieurs expliquent qu'elles peuvent, ce faisant, combiner les données recueillies. C'est le cas de Microsoft, qui l'exprime en ces termes :

« nous combinons les données que nous recueillons dans différents contextes (par exemple, provenant de votre utilisation de deux produits Microsoft). Par exemple, il se peut que Cortana utilise des informations de [votre] calendrier pour suggérer des éléments d'action dans un e-mail d'avertissement et que Microsoft Store utilise des informations sur des applications et des services pour recommander des applications personnalisées.³² »

En somme, utiliser les services web de ces entreprises est synonyme d'une collecte massive de données, qui pourront ensuite servir à dresser un profil détaillé d'une personne et qui pourront faire l'objet d'un traitement visant des fins larges et généralement formulées en des termes vagues.

2.1.2. Une information parcellaire sur l'IA

Si les politiques des entreprises étudiées mentionnent une vaste utilisation de la nuée de données qu'elles recueillent, elles donnent assez peu d'indications quant aux technologies exactes qui en permettent le traitement et aux facteurs qu'elles prennent en compte.

Quelques entreprises expliquent que les données qu'elles recueillent font l'objet d'un « traitement automatique », d'une analyse par des « algorithmes », ou qu'elles sont traitées avec des techniques d'« apprentissage automatique ». Google, à titre d'exemple, l'exprime en ces termes :

« Nous utilisons des systèmes automatisés qui analysent vos contenus afin de vous fournir, entre autres, des résultats de recherche personnalisés, des annonces

³⁰ Reuben BINNS et al., *Measuring Third-party Tracker Power across Web and Mobile*, ACM Transactions on Internet Technology, 2018; PRIVACY INTERNATIONAL, *How Apps on Android Share Data with Facebook (even if you don't have a Facebook account)*, 2018

³¹ Alexandre PLOURDE, « Retour vers le futur : l'internet des objets et la protection de la vie privée », dans BARREAU DU QUÉBEC, *Développements récents en droit à la vie privée*, 2019, vol. 465, Éditions Yvon Blais, p. 33-66

³² <https://privacy.microsoft.com/fr-fr/privacystatement>

personnalisées ou d'autres fonctionnalités adaptées à votre utilisation de nos services. Nous analysons en outre vos contenus pour nous aider à détecter des abus comme les pourriels, les logiciels malveillants et les contenus illégaux. Nous utilisons également des algorithmes pour reconnaître les modèles dans les données.³³ »

Microsoft évoque plus directement l'intelligence artificielle dans ses politiques, expliquant que son traitement automatisé des données comprend des méthodes d'IA :

« nos méthodes automatisées comprennent l'intelligence artificielle (IA), que nous considérons comme un ensemble de technologies qui permettent aux ordinateurs de percevoir, d'apprendre, de déduire et d'aider à prendre des décisions pour résoudre les problèmes de manière similaire à ce que les personnes font.³⁴ »

Certaines entreprises, dont Amazon et Microsoft, expliquent aussi que le traitement automatisé peut être accompagné d'une vérification faite par des humains, dite « manuelle ». Microsoft poursuit ainsi en ces termes :

« Pour créer, former et améliorer la précision de nos méthodes de traitement automatisées (notamment l'IA), nous examinons manuellement certaines des prédictions et déductions produites par les méthodes automatisées par rapport aux données sous-jacentes à partir desquelles les prévisions et les déductions ont été effectuées. Par exemple, nous examinons manuellement les extraits de code courts d'un petit échantillon de données vocales.³⁵ »

Notre recherche ne nous a pas permis d'identifier les intrants exacts dans ces systèmes d'IA et les critères précis qui guident leurs décisions. Au mieux, les entreprises énoncent occasionnellement des facteurs qui peuvent être pris en compte dans leurs analyses. Par exemple, Facebook indique que l'ordre des publications dans le fil d'actualité de l'utilisateur est influencé par ses interactions antérieures avec d'autres publications, le nombre de réactions qu'une publication reçoit ou son caractère récent³⁶. Amazon divulgue également quelques facteurs qui influent sur les recommandations d'achats faites au consommateur :

« Nous examinons les articles que vous avez achetés, les articles que vous avez indiqué posséder et les articles auxquels vous avez accordé une note. Nous comparons vos activités sur notre site à celles des autres clients, ce qui nous permet de vous recommander d'autres articles potentiellement intéressants sur Votre Amazon. [...] Vos recommandations changent régulièrement, en fonction d'un certain nombre de facteurs, comme lorsque vous achetez ou évaluez un nouvel article, et selon l'évolution des champs d'intérêt d'autres clients comme vous.³⁷ »

³³ <https://policies.google.com/privacy?hl=fr>

³⁴ <https://privacy.microsoft.com/fr-fr/privacystatement>

³⁵ <https://privacy.microsoft.com/fr-fr/privacystatement>

³⁶ <https://www.facebook.com/help/520348825116417>

³⁷ https://www.amazon.ca/-/fr/gp/help/customer/display.html/ref=help_search_1-2?ie=UTF8&nodeld=GE4KRSZ4KAZZB4BV&qid=1624382868&sr=1-2

En somme, les représentations des entreprises confirment l'emploi à grande échelle de systèmes de traitement automatisé des données des consommateurs, qui pourraient être qualifiés d'IA au sens du présent rapport. Toutefois, les entreprises donnent peu de détails quant aux données exactes qui nourrissent ces systèmes et les facteurs qu'ils prennent en considération.

2.1.3. Un encadrement volontariste

Même si on ne connaît pas les pratiques exactes des entreprises quant au traitement de données, certaines publient de l'information quant à l'encadrement de leurs systèmes d'IA.

Microsoft et Google annoncent ainsi avoir adopté des principes pour guider le déploiement de l'IA³⁸. Google énonce notamment que l'IA doit être socialement bénéfique, qu'elle ne doit pas créer ou renforcer des biais inéquitables, qu'elle doit être sécuritaire et incorporer les principes de vie privée par design³⁹. Ces principes mentionnent également l'imputabilité et la transparence :

« We will design AI systems that provide appropriate opportunities for feedback, relevant explanations, and appeal. [...] We will incorporate our privacy principles in the development and use of our AI technologies. We will give opportunity for notice and consent, encourage architectures with privacy safeguards, and provide appropriate transparency and control over the use of data.⁴⁰ »

Ces deux entreprises affirment aussi avoir développé des processus internes et des outils techniques pour mettre en œuvre ces principes⁴¹. Par exemple, Microsoft explique avoir un « Office de l'IA responsable » ayant pour mission, entre autres, faire appliquer ses principes d'IA responsable au sein de l'entreprise⁴². Puisqu'elles rendent disponibles leurs systèmes d'IA à des développeurs tiers, plusieurs entreprises publient également de la documentation destinée à guider ces entreprises à faire une utilisation responsable de leurs systèmes⁴³.

Certes louables, il reste que ces efforts pour encadrer l'utilisation de l'IA sont fondées sur une approche volontariste. Ultimement, cette autoréglementation ne peut reposer que sur la confiance des consommateurs et le bon vouloir des entreprises, sans pouvoir faire l'objet de sanctions d'autorités publiques. Cela laisse à craindre que les forces du marché puissent amener les entreprises à négliger leurs engagements dans des situations où leur intérêt économique sera en jeu⁴⁴.

³⁸ <https://www.microsoft.com/en-us/ai/responsible-ai>

³⁹ <https://ai.google/principles/>

⁴⁰ <https://ai.google/principles/>

⁴¹ Voir : <https://ai.google/responsibilities/review-process/>; <https://ai.google/responsibilities/responsible-ai-practices/>

⁴² <https://www.microsoft.com/en-us/ai/our-approach>

⁴³ Voir : <https://www.microsoft.com/en-us/ai/responsible-ai-resources>; <https://pair.withgoogle.com/guidebook>

⁴⁴ Notons que l'organisme Ranking Digital Rights affirme que les plateformes en ligne ne mènent pas d'études d'impact robustes pour détecter les biais que pourraient avoir leurs systèmes d'IA en matière publicitaire. Voir : <https://rankingdigitalrights.org/index2020/key-findings>

2.1.4. Le contrôle limité des consommateurs

Les entreprises offrent certains choix aux consommateurs quant à la collecte et à l'utilisation de leurs données personnelles.

D'abord, quelques entreprises donnent un contrôle quant à la collecte de données qu'elles effectuent. Google offre des paramètres pour désactiver l'historique des activités de l'internaute et de son positionnement géographique⁴⁵. Facebook, de son côté, explique aux consommateurs comment désactiver la collecte de certaines données, comme la géolocalisation⁴⁶. Apple permet à l'utilisateur de configurer l'information qui est collectée ou partagée dans ses appareils; de plus, une notification de sécurité apparaît lorsqu'Apple a besoin d'une permission particulière pour une fonctionnalité ou pour une application⁴⁷.

Ensuite, certaines entreprises donnent la possibilité aux consommateurs de refuser que leurs données soient utilisées pour personnaliser les publicités. C'est le cas, par exemple, de Microsoft et Google, qui permettent aux consommateurs de désactiver les publicités ciblées⁴⁸. À noter, toutefois, que ce paramètre n'empêchera pas l'entreprise de recueillir les données et de les utiliser à d'autres fins.

Bien qu'intéressantes, les options offertes par les entreprises comportent des limites. D'abord, on constate que le contrôle sur la collecte des données n'est pas absolu pour le consommateur; dans bien des cas, comme chez Facebook, le consommateur doit accepter une large collecte de ses données pour bénéficier du service. Sa seule option est donc de ne pas utiliser ce service, une avenue difficilement envisageable dans un contexte où l'environnement des plateformes en ligne est peu concurrentiel. Ensuite, la plupart des entreprises configurent leurs systèmes de façon à maximiser, par défaut, la collecte. Selon une étude de l'association de consommateurs norvégienne Forbrukerradet, les interfaces des entreprises technologiques sont ainsi conçues de façon à amener les consommateurs, par défaut, à choisir les paramètres les moins respectueux de leur vie privée⁴⁹.

Finalement, on trouve bien peu d'options quant à la possibilité de remettre en question les résultats des systèmes d'IA, ou encore pour choisir les critères qui sont pris en considération dans leurs analyses. Tout au plus, face à l'utilisation de toutes ces technologies automatisées, Apple cherche à rassurer les consommateurs en affirmant laconiquement qu'elle « n'utilise pas d'algorithmes ni de profilage pour prendre des décisions susceptibles de vous affecter de façon significative sans possibilité d'une vérification par un être humain.⁵⁰ » On reste toutefois imprécis de savoir quel type de décision pourra être considérée comme ayant un impact significatif.

⁴⁵ <https://myaccount.google.com/dashboard>

⁴⁶ https://www.facebook.com/help/275925085769221?helpref=faq_content

⁴⁷ <https://www.apple.com/privacy/control/>

⁴⁸ <https://account.microsoft.com/privacy/ad-settings/>

⁴⁹ FORBRUKERRADET, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*, 2018

⁵⁰ <https://www.apple.com/ca/fr/legal/privacy/fr-ca/>

2.2. Portrait des applications de l'IA

Les débouchés de l'IA dans un contexte commercial sont vastes. Notre analyse montre que l'IA, entendue dans son sens large, propulse une myriade de services numériques offerts aux consommateurs. Bien que notre analyse ne permette pas de décrire chaque application de l'IA par chaque entreprise, elle permet de témoigner de l'importance que prend désormais cette technologie dans les relations entre les commerçants et les consommateurs.

2.2.1. Personnaliser l'expérience-utilisateur

L'une des applications les plus répandues de l'IA tient sans contredit dans la personnalisation des services fournis aux consommateurs.

La personnalisation est une tactique marketing visant à adapter l'offre à chaque client, pour rendre le service plus attrayant ou pour augmenter les ventes. En analysant les activités et le profil d'un internaute, une entreprise peut lui suggérer du contenu, lui faire des recommandations d'achat ou lui présenter des contenus plus susceptibles de l'intéresser.

Les recommandations d'achat chez Amazon en sont un exemple éloquent. En se basant sur l'historique d'achats et de recherche d'un internaute, cette personnalisation permet à Amazon de suggérer des biens adaptés aux besoins des consommateurs et des produits complémentaires lors d'un achat. On pourra ainsi proposer des câbles et des adaptateurs lors de l'achat d'un téléviseur, ou un tapis protecteur lors de l'achat d'une chaise de bureau.

L'IA permet également aux commerçants de créer des environnements personnalisés, qui incitent les consommateurs à rester plus longtemps sur leur plateforme. Sur Facebook, l'IA permet ainsi de déterminer quelles publications afficher pour susciter le plus d'intérêt chez les utilisateurs, et ainsi optimiser leur interaction avec la plateforme⁵¹.

L'IA est aussi mise à profit pour cibler les publicités présentées aux internautes. La plupart des entreprises faisant partie de notre sélection mentionnent qu'elles participent à des réseaux de publicité comportementale en ligne, dans laquelle les annonces présentées aux internautes sont personnalisées en fonction de leur profil en ligne. Ce traitement des données des consommateurs à des fins commerciales est d'ailleurs au cœur des modèles d'affaires de Facebook et Google.

2.2.2. Prédire les tendances du marché

L'IA permet non seulement de personnaliser l'expérience-utilisateur avec une grande efficacité; elle permet aussi aux entreprises d'anticiper les prochaines actions ou les besoins futurs des consommateurs.

⁵¹ Karen HAO, *How Facebook got addicted to spreading misinformation*, MIT Technology review, 11 mars 2021, <https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/>

Cette détection des tendances permet notamment aux entreprises de déployer des tactiques dites de « *customerization* », où la personnalisation s'étend aux processus opérationnels régissant la chaîne d'approvisionnement⁵². Par exemple, Amazon est en mesure de prédire le comportement des consommateurs en analysant les renseignements provenant de diverses bases de données⁵³. Grâce au pouvoir prédictif de l'IA, cette firme serait en mesure de déterminer, par exemple, que des parents choisiront d'acheter des figurines d'une émission de télévision si les cotes d'écoute augmentent sur sa plateforme de diffusion PrimeVideo, et ainsi ajuster la production de ces biens et en optimiser la distribution, de manière proactive.

2.2.3. Donner accès à l'information

L'IA permet d'organiser des quantités phénoménales d'information, d'analyser cette information et d'y accéder en une fraction de seconde. Ces capacités sont fort utiles pour les consommateurs, qui peuvent ainsi trouver rapidement ce qu'ils cherchent.

Les moteurs de recherche web en sont l'illustration la plus éloquente⁵⁴. Essentiellement, un moteur de recherche indexe le web à l'aide de « robots », puis rattache des mots-clefs à chacune des milliards de pages ainsi répertoriées. Au terme de ces démarches, des algorithmes sophistiqués analysent les pages pour les classer et déterminer les meilleurs résultats de recherche pour une requête⁵⁵. Google l'explique en ces termes :

« Ces systèmes de classement sont composés non pas d'un, mais de toute une série d'algorithmes. Pour vous donner les informations les plus utiles, les algorithmes de recherche tiennent compte de nombreux facteurs, tels que les mots utilisés dans votre requête, la pertinence et la facilité d'utilisation des pages, le niveau d'expertise des sources, votre position et vos paramètres. La pondération appliquée à chaque facteur varie en fonction de la nature de votre requête. Par exemple, l'actualisation du contenu joue un rôle plus important dans la réponse aux requêtes concernant un sujet d'actualité que dans le cas de définitions du dictionnaire.⁵⁶ »

Outre les moteurs de recherche, plusieurs autres services en ligne pouvant être propulsés par l'IA sont devenus des outils indispensables dans la société de l'information. Songeons par exemple aux services de traduction, qui sont en mesure de « comprendre » le langage pour le traduire⁵⁷. En guise d'illustration, Amazon a mis en service une toute nouvelle fonctionnalité

⁵² Jerry WIND et Arvind RANGASWAMY, « Customerization: The next revolution in mass customization », (2001) 15-1 *Journal of Interactive Marketing* 13

⁵³ Tony HAITAO CUI et al., « Informational Challenges in Omnichannel Marketing: Remedies and Future Research », (2020) 85-1 *Journal of Marketing* 103

⁵⁴ Kevin KELLY, *The Three Breakthroughs That Have Finally Unleashed AI on the World*, 27 octobre 2014, Wired, <https://www.wired.com/2014/10/future-of-artificial-intelligence/>

⁵⁵ <https://www.google.com/search/howsearchworks/crawling-indexing/>

⁵⁶ <https://www.google.com/search/howsearchworks/algorithms/>

⁵⁷ <https://policies.google.com/privacy?hl=fr>

d'Alexa qui permet de traduire une conversation en temps réel en recourant à la reconnaissance vocale et textuelle, afin d'obtenir une traduction fluide et exacte⁵⁸.

L'IA peut aussi servir au consommateur pour se repérer et en apprendre davantage sur le lieu où il se trouve. Par exemple, Google Maps peut estimer la difficulté qu'aura une personne à trouver un stationnement pour son véhicule dans une zone géographique, ou encore planifier l'itinéraire optimal pour un déplacement⁵⁹.

2.2.4. Faciliter la vie des consommateurs

De façon presque imperceptible pour les consommateurs, l'IA est mise à profit pour rendre les services des entreprises plus fluides, rapides et intuitifs.

L'IA permet d'abord d'optimiser la logistique des entreprises. Amazon utilise notamment des robots travaillant de pair avec des humains pour traiter et expédier plus efficacement les commandes dans ses entrepôts⁶⁰. La firme envisage également d'instaurer un service de livraison à domicile par drones autonomes⁶¹. De telles technologies permettent à la firme de gagner en efficacité et ainsi livrer les biens aux consommateurs plus rapidement, tout en diminuant le risque d'erreur.

L'IA permet aussi d'augmenter la convivialité des services. Par exemple, Apple utilise l'IA pour améliorer la qualité des photos prises avec ses appareils⁶² ou pour détecter automatiquement les activités que fait une personne et s'y adapter⁶³. De son côté, Microsoft utilise l'IA pour rendre ses logiciels plus faciles d'utilisation⁶⁴, par exemple en permettant à une personne d'entrer automatiquement des données sur une feuille de calcul simplement en prenant une photo d'une base de données ou d'un tableau⁶⁵.

Notons par ailleurs l'IA peut également être employée dans des magasins ayant pignon sur rue. En y installant des caméras et en traitant les images avec l'IA, Walmart dit ainsi pouvoir déterminer à quel moment ses étalages doivent être regarnis, et ainsi mieux gérer son

⁵⁸ Shirin SALEEM et Roland MAAS, *How Alexa's new Live Translation for conversations works*, Amazon Science, 14 décembre 2020, <https://www.amazon.science/blog/how-alexa-s-new-live-translation-for-conversations-works>

⁵⁹ <https://blog.google/technology/ai/13-ways-youre-using-ai-your-daily-life/>

⁶⁰ Matt SIMON, *Inside the Amazon Warehouse Where Humans and Machines Become One*, Wired, 5 juin 2019, <https://www.wired.com/story/amazon-warehouse-robots/>

⁶¹ <https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011>

⁶² James VINCENT, *Apple's AI plan: a thousand small conveniences*, The Verge, 25 juin 2020, <https://www.theverge.com/2020/6/25/21301511/apple-ai-machine-learning-features-wwdc-2020-convenience>

⁶³ Par exemple, la Apple Watch est en mesure de déterminer si son porteur se lave les mains. Voir : Samuel AXON, *Here's why Apple believes it's an AI leader—and why it says critics have it all wrong*, Arstechnica, 6 août 2020, <https://arstechnica.com/gadgets/2020/08/apple-explains-how-it-uses-machine-learning-across-ios-and-soon-macos/>

⁶⁴ <https://blogs.microsoft.com/ai/microsoft-365-intelligent-workday-productivity/>

⁶⁵ Sarah MASON, *Smart spreadsheets? Features in Microsoft Excel that use artificial intelligence*, Artificial Intelligence in plain English, 18 octobre 2020, <https://medium.com/ai-in-plain-english/smart-spreadsheets-features-in-microsoft-excel-that-use-artificial-intelligence-e6908088f727>

inventaire⁶⁶. Aux États-Unis, les magasins Amazon Go peuvent détecter automatiquement quels produits les consommateurs ont pris sur les étagères et les porter à leur compte automatiquement, ce qui leur évite de s'arrêter à une caisse enregistreuse avant de quitter l'établissement.

2.2.5. Se protéger des menaces

L'IA peut jouer un rôle important pour détecter et prévenir la fraude ou d'autres menaces qui peuvent porter préjudice au public.

L'ensemble des institutions financières énoncent qu'elles peuvent utiliser les renseignements personnels des consommateurs « aux fins de la prévention, de l'enraiment ou de la détection des fraudes ou des crimes.⁶⁷ » Pour ces fins, l'IA peut être mise à profit de diverses façons, notamment pour détecter automatiquement des opérations suspectes dans le compte d'un client ou pour déployer des modèles prédictifs de fraude⁶⁸.

L'IA peut aussi être mise à partie pour combattre une multitude de nuisances sur le web, telles que le contenu illégal, haineux ou radicalisant. Google fait ainsi appel à des systèmes d'IA pour filtrer les pourriels⁶⁹. Chez Facebook, l'IA est employée pour bloquer les contenus obscènes ou graphiques du fil de contenu des utilisateurs. Facebook utilise aussi l'IA pour limiter l'exposition de ses modérateurs à ce type de contenus, qui sont parfois insoutenables à regarder⁷⁰.

Enfin, soulignons que l'IA peut aussi aider à combattre les menaces créées... par l'IA elle-même. Facebook propose ainsi d'utiliser l'IA pour détecter les hypertrucages (*deepfakes*), à savoir des vidéos dans lesquelles le visage d'une personne tierce a été intégré de manière très convaincante grâce à l'IA⁷¹. De telles vidéos peuvent être utilisées à des fins préjudiciables pour le public, notamment pour véhiculer de la désinformation.

2.2.6. Reconnaître les images et les visages

L'IA est également employée par les entreprises pour effectuer de la reconnaissance d'images et de visages. L'apprentissage profond permet aux logiciels d'analyser des millions d'images semblables, selon divers traits caractéristiques communs, de façon à reconnaître automatiquement une image qui leur est soumise. En guise d'illustration, le système d'IA pourra reconnaître qu'un chat a du poil, des oreilles pointues, quatre pattes et un nez en triangle. Ceci

⁶⁶ <https://corporate.walmart.com/newsroom/2019/04/25/walmarts-new-intelligent-retail-lab-shows-a-glimpse-into-the-future-of-retail-irl>

⁶⁷ <https://www.rbc.com/rensperssecurite/ca/index.html>

⁶⁸ Anne Shirley LEBEL, Ivan TCHOTOURIAN et Marc LACOURSIÈRE, « Défi de l'encadrement juridique de l'intelligence artificielle dans l'industrie bancaire et des valeurs mobilières : l'exemple des services de paiement et des conseillers-robots », 30-3 *Les Cahiers de propriété intellectuelle* 1003, p. 1010-1011

⁶⁹ <https://blog.google/technology/safety-security/fighting-phishing-smarter-protections/>

⁷⁰ Casey NEWTON, « Les éboueurs du Web », *L'actualité*, 4 mars 2020, <https://lactualite.com/societe/les-eboueurs-du-web/>

⁷¹ <https://ai.facebook.com/blog/deepfake-detection-challenge>

lui permettra ensuite de catégoriser ou de reconnaître des chats dans des images, indépendamment du décor.

Ces technologies trouvent, encore là, une myriade d'applications. Le service Google Photos fait appel à l'IA pour organiser les souvenirs d'une personne ou créer des animations à partir de ses photos⁷². De son côté, Facebook explique notamment qu'elle met à profit des technologies de reconnaissance faciale pour identifier ses utilisateurs dans des vidéos ou des photos :

« La reconnaissance faciale sert à analyser les photos et les vidéos sur Facebook dans lesquelles, d'après nous, vous êtes susceptible d'apparaître, comme votre photo de profil ou les photos et les vidéos sur lesquelles vous avez été identifié(e). L'objectif est de créer un numéro qui vous est propre, appelé modèle. Lorsque vous activez la reconnaissance faciale, nous créons votre modèle et l'utilisons comme point de comparaison avec d'autres photos, vidéos ou d'autres contenus utilisant l'appareil photo (comme les vidéos en direct) pour déterminer si vous apparaissez dans ce contenu.⁷³ »

Tout comme Facebook, Apple utilise les technologies de reconnaissance faciale dans de nombreux produits, notamment pour son système d'authentification Face ID. Grâce à l'apprentissage automatique, ce système est en mesure de reconnaître le visage de l'utilisateur et de lui donner accès à son appareil⁷⁴.

2.2.7. Interagir avec les consommateurs

L'IA peut comprendre ce que disent les humains et même simuler des interactions avec eux. Des technologies telles que le traitement du langage naturel, qui permettent de saisir les nuances du langage humain, sont ainsi intégrées dans de multiples services offerts aux consommateurs.

L'un des débouchés les plus marquants de cette technologie tient dans les assistants virtuels produits par les géants du numérique, qu'il s'agisse de Siri, Alexa, Assistant Google ou Cortana. Ces assistants sont en mesure de faire la différence entre une requête d'information, par exemple lorsque l'on demande la météo, ou une requête d'action, comme lorsque l'on demande de jouer une chanson, puis y répondre. Par exemple, Cortana peut programmer des rendez-vous, lire des courriels ou consulter l'horaire de la journée entièrement par commande vocale⁷⁵.

Comme l'explique Amazon, toutes ces fonctionnalités sont rendues possibles par une IA qui cherche constamment à se perfectionner :

« Alexa est conçue pour devenir plus intelligente chaque jour. Par exemple, nous utilisons vos demandes faites à Alexa pour former nos systèmes de reconnaissance

⁷² <https://blog.google/products/photos/new-memories-features-look-back/>

⁷³ <https://www.facebook.com/help/122175507864081?ref=dp>

⁷⁴ <https://support.apple.com/en-us/HT208108>

⁷⁵ <https://www.microsoft.com/en-us/microsoft-365/blog/2020/05/27/making-easier-stay-caught-cortana-microsoft-365/>

vocale et de compréhension du langage naturel en utilisant l'apprentissage automatique. Le fait de former Alexa avec des demandes réelles d'un éventail diversifié de clients est nécessaire pour qu'Alexa réagisse correctement à la variation des structures du discours, des dialectes, des accents, et du vocabulaire de nos clients et des environnements acoustiques où nos clients utilisent Alexa.⁷⁶ »

De tels systèmes d'interaction avec les consommateurs peuvent aussi être employés pour propulser des agents conversationnels avec lesquels le consommateur peut clavarder (*chatbot*)⁷⁷. Utilisées dans le cadre du service à la clientèle, ces capacités de l'IA permettent notamment de distinguer des requêtes pouvant facilement être traitées par un système informatique, comme fournir les heures d'ouverture d'un commerce, et celles nécessitant une intervention humaine.

2.2.8. Conseiller les consommateurs

L'IA permet non seulement aux entreprises d'interagir avec les consommateurs; elle peut carrément leur donner des conseils sur ce qu'ils devraient faire ou non, et sur les meilleurs choix qui s'offrent à eux.

Les conseillers financiers automatisés sont un exemple marquant de cette application de l'IA. Ces « conseillers-robots », apparus au cours de la dernière décennie, sont des plateformes sur lesquelles le consommateur répond à des questions pour broser son profil financier; en fonction de ces réponses, il conseillera le client quant aux produits et aux stratégies financiers à choisir⁷⁸.

De tels conseillers-robots sont offerts par des institutions financières. Par exemple, le service Portefeuille futé BMO affirme utiliser « des algorithmes évolués pour augmenter vos rendements tout en respectant votre tolérance au risque⁷⁹ ». De son côté, la banque RBC offre la plateforme Nomi, qui donne, à l'aide d'une « technologie prédictive », des conseils financiers ou budgétaires :

« Qui a dit que la gestion d'un budget devait être compliquée ? Laissez à NOMI le soin de vous recommander un budget en fonction de vos habitudes personnelles de consommation et d'épargne – et vous aider à le respecter !⁸⁰ »

Pour les consommateurs, de telles plateformes peuvent contribuer à démocratiser l'accès aux services financiers, de manière conviviale et peu coûteuse. En effet, plusieurs de ces services n'exigent pas ou peu de mise de fonds, et ne demandent pas de commissions importantes.

⁷⁶ <https://www.amazon.ca/-/fr/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V>

⁷⁷ Graeme MCLEAN et Kofi OSEI-FRIMPONG, « Chat now... examining the variables influencing the use of online live chat », 146 *Technological Forecasting & Social Change* 55

⁷⁸ Anne Shirley LEBEL, Ivan TCHOTOURIAN et Marc LACOURSIÈRE, « Défi de l'encadrement juridique de l'intelligence artificielle dans l'industrie bancaire et des valeurs mobilières : l'exemple des services de paiement et des conseillers-robots », 30-3 *Les Cahiers de propriété intellectuelle* 1003, p. 1013-1014

⁷⁹ <https://www.bmo.com/principal/particuliers/investissements/placements-en-ligne/portefeuille-fute/fonctionnement/>

⁸⁰ <https://www.rbcroyalbank.com/fr/mobile/feature/nomi/budgets/>

2.2.9. Prendre des décisions automatisées

L'IA peut faire davantage que des suggestions et des recommandations aux consommateurs. Elle peut carrément servir à prendre des décisions sur eux, de manière complètement automatisée.

Il n'est pas nouveau que les commerçants emploient des méthodes automatisées pour prendre une décision quant à l'admissibilité d'un consommateur à un service. Depuis des décennies, des entreprises utilisent ainsi les pointages qui sont tirés du dossier de crédit dans l'octroi de crédit ou pour fixer automatiquement une prime d'assurance, entre autres exemples⁸¹. De manière similaire au pointage de crédit, l'IA pourrait ainsi être employée dans le domaine des services financiers pour décider automatiquement de l'octroi de crédit à un consommateur ou pour déterminer les conditions auxquelles un service lui est offert⁸².

L'IA peut aussi être utilisée pour exclure un consommateur d'un service qu'il utilise déjà. Ainsi, sur les médias sociaux, l'IA peut déterminer automatiquement si ce que publie un internaute contrevient aux politiques de l'entreprise – et choisir d'exclure de cette personne de la plateforme. Facebook, par exemple, explique qu'elle recourt à l'IA pour analyser la conformité des contenus publiés par ses utilisateurs à ses normes de communauté :

« Nous investissons dans l'intelligence artificielle en vue de renforcer ces mesures à grande échelle. [...] Cette technologie nous aide à agir de manière proactive en signalant du contenu à examiner et, dans certains cas, en prenant des mesures automatiques.⁸³ »

À l'opposé, l'IA pourrait aussi être mise à partie par les consommateurs eux-mêmes, pour automatiser leurs achats⁸⁴. Par exemple, on pourrait envisager des plateformes qui commandent automatiquement des biens lorsqu'il vient à en manquer dans les stocks du consommateur.

⁸¹ Andrew SMITH, *Using Artificial Intelligence and Algorithms*, Federal Trade Commission, 8 avril 2020, <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms>

⁸² Matthew A. BRUCKNER, « The Promise and Perils of Algorithmic Lenders' Use of Big Data », (2018) 93 *Chi.-Kent L. Rev.* 3; Anne Shirley LEBEL, Ivan TCHOTOURIAN et Marc LACOURSIÈRE, « Défi de l'encadrement juridique de l'intelligence artificielle dans l'industrie bancaire et des valeurs mobilières : l'exemple des services de paiement et des conseillers-robots », 30-3 *Les Cahiers de propriété intellectuelle* 1003, p. 1011

⁸³ <https://www.facebook.com/business/help/373506759931554?id=1769156093197771>

⁸⁴ Michal GAL et Niva ELKIN-KOREN, « Algorithmic Consumers », (2017) 30-2 *Harvard Journal of Law and Technology* 309

3. Les enjeux de l'IA pour les consommateurs

L'IA apporte son lot d'avantages pour les consommateurs. Elle leur permet d'obtenir des services personnalisés et faciles à utiliser, d'accéder à une quantité phénoménale d'information, voire même d'obtenir des conseils. Toutefois, cette technologie n'est pas sans risque. Même si ses débouchés dans un contexte de consommation peuvent sembler parfois banals, ils menacent d'exposer les consommateurs à l'exclusion, à l'exploitation économique ou à des atteintes à leurs droits fondamentaux.

3.1. Une intrusion dans la vie privée

En raison des grandes quantités de données qu'elle requiert pour apprendre et devenir performante, l'IA est en forte tension avec le droit à la vie privée. Pour nourrir leurs algorithmes, les entreprises colligent des données sur les consommateurs non seulement sur leurs propres plateformes, mais également sur des sites web tiers, sur des applications mobiles, ou via des objets connectés (voir section 2.1.1).

Il va sans dire que la captation en continu des renseignements personnels des consommateurs, et leur profilage à des fins commerciales, constitue une intrusion importante dans leur intimité. L'omniprésence de la collecte de données effectuée par les géants technologiques leur permet d'en apprendre long sur les habitudes, les préférences, les comportements ainsi que les allées et venues des consommateurs⁸⁵. De surcroît, l'IA est capable de créer de nouvelles connaissances à partir des données récoltées; ces inférences, encore là, peuvent révéler des parts de l'intimité d'une personne.

L'ampleur de la collecte de données personnelles dans le contexte des modèles d'affaires numériques essuie de nombreuses critiques, notamment quant à la validité du modèle de consentement employé par les entreprises (section 4.2) et quant aux limites que le cadre légal impose à ces pratiques (section 4.3). Ajoutons que les mécanismes de contrôle offerts aux consommateurs ne permettent ni de refuser complètement le pistage dont ils font l'objet, ni de s'opposer au résultat du traitement de leurs données par l'IA (section 2.3).

Par ailleurs, une telle collecte de données personnelles multiplie les risques de bris de sécurité ou d'accès non autorisé aux données. Des bases de données ne sont pas à l'abri des malveillants ou des accidents de sécurité, et la richesse des informations qu'elles contiennent pourraient exposer les consommateurs à des préjudices économiques ou à des atteintes à leur réputation⁸⁶. De plus, les données recueillies pourraient faire l'objet d'un accès non autorisé par des employés de l'entreprise ou par des tiers.

⁸⁵ Aviv GAON et Ian STEDMAN, « A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada », (2019) 56-4 *Alta L Rev* 1137, p. 1145-1146

⁸⁶ CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, *Évaluation des cybermenaces nationales 2020*, Centre de la sécurité des télécommunications, 2020, p. 12

3.2. Des systèmes opaques

L'IA exacerbe l'asymétrie d'information entre les consommateurs et les entreprises. Non seulement une part importante de la collecte de données qui nourrissent les systèmes d'IA s'effectue à l'insu des consommateurs, mais les rouages de l'analyse effectuée par ces systèmes restent généralement opaques.

Comment décide-t-on des contenus qui sont présentés au consommateur? Quels sont les facteurs pris en compte pour leur faire des recommandations ou pour prendre des décisions à leur égard? Mystère. Les entreprises, on l'a vu, donnent peu d'explications quant aux facteurs qui entrent en compte dans ces décisions. Dans le meilleur des cas, on peut obtenir de l'information parcellaire sur ces questions. De surcroît, les formules et les facteurs qui déterminent le traitement des données peuvent être sujet à changement sans préavis⁸⁷.

L'opacité des systèmes d'IA peut prendre plusieurs formes. La plus évidente tient dans le fait que le code source des algorithmes est généralement inconnu du public⁸⁸. En effet, la plupart des entreprises ne divulguent pas le code informatique qui sous-tend leurs systèmes, considérant qu'il s'agit là d'un secret commercial. Or, l'impossibilité d'analyser le code source est une entrave importante pour les États et la société civile qui souhaiteraient en comprendre les effets potentiellement préjudiciables⁸⁹.

Cela dit, l'opacité des systèmes d'IA est une question qui dépasse le simple accès aux codes sources des entreprises. En effet, même si ces codes informatiques étaient rendus publics, il faut convenir que leur complexité pose de sérieuses limites à leur compréhensibilité. Rappelons que les systèmes d'IA peuvent agir de manière autonome, en fondant leurs analyses sur le traitement d'une quantité phénoménale de données. Les décisions et les solutions auxquelles ils parviennent ne sont pas limitées par le raisonnement « humain »⁹⁰. Il apparaît donc ténu de chercher à prévoir comment ils agiront lorsqu'ils seront appliqués à une base de données, et comment ils arriveront à une solution précise.

En fait, même les entreprises qui ont créé les systèmes d'IA peuvent ignorer comment ils en arrivent à leurs conclusions. En somme, un système d'IA peut constituer une « boîte noire », c'est-à-dire qu'il est incapable de fournir une explication sur ses conclusions. Dans ce contexte, on ne peut guère remettre en question les décisions prises par les algorithmes; pire encore, les défauts dans la conception de ces systèmes pourraient être indétectables pour les créateurs de ces systèmes eux-mêmes⁹¹.

⁸⁷ Kaveh WADDELL, *Tech Companies Too Secretive About Algorithms That Curate Feeds, Study Says*, Consumer Reports, 24 février 2021, <https://www.consumerreports.org/consumer-protection/tech-companies-too-secretive-about-algorithms-that-curate-feeds/>

⁸⁸ Jenna BURRELL, « How the machine thinks: Understanding opacity in machine learning algorithms », (2016) 3-1 *Big Data & Society* 1, p. 1-2

⁸⁹ *Id.*

⁹⁰ Matthew U. SCHERER, « Regulating Artificial Intelligences Systems: Risks, Challenges, Competencies, and Strategies », (2016) 29-2 *Harvard Journal of Law & Technology* 354, p. 365

⁹¹ *Id.*, p. 372

3.3. Le risque de préjudice économique

Dans le commerce en ligne, l'IA pourrait donner l'occasion à des entreprises de tirer un avantage économique indu des consommateurs. À cet égard, trois risques de préjudice économique envers les consommateurs accaparent davantage notre attention : le recours à des techniques de persuasion invasives (3.3.1), la personnalisation des prix (3.3.2) et les entraves à la libre-concurrence (3.3.3).

3.3.1. Des techniques de persuasion invasives

Depuis longtemps, les entreprises ciblent les consommateurs afin de leur présenter des publicités ou des offres qui correspondent le plus possible à leur profil – et qui ont donc de meilleures chances de succès. Par exemple, les sollicitations postales peuvent cibler des personnes grâce à des renseignements tirés de leur dossier de crédit⁹²; ou encore, un vendeur dans un magasin peut, en observant un consommateur, identifier les arguments les plus susceptibles de le convaincre de faire un achat⁹³.

Avant l'ère numérique, la personnalisation commerciale restait un exercice fastidieux et imparfait. L'IA change toutefois la donne. Combinée aux mégadonnées, l'IA permet désormais d'automatiser la personnalisation et de la déployer à une échelle jamais égalée⁹⁴. Dans le commerce en ligne, des entreprises peuvent maintenant identifier les biais ou les vulnérabilités spécifiques d'un consommateur et s'en servir, en temps réel, dans le cadre de diverses tactiques marketing⁹⁵.

L'IA peut en effet révéler les intérêts, les biais et les vulnérabilités d'un consommateur. En guise d'illustration, un document préparé pour des publicitaires par Facebook expliquait qu'elle pouvait cibler de jeunes utilisateurs durant des moments de vulnérabilité particulièrement critiques, par exemple lorsqu'ils se sentent « incapables », « insécures », « stressés » ou « anxieux »⁹⁶. Grâce à une connaissance si intime des consommateurs, une entreprise pourrait créer des messages publicitaires au contenu hyperpersonnalisé, présenté à un auditoire qui y sera hautement réceptif⁹⁷. L'IA pourrait également être employée pour amener les consommateurs à faire des achats qu'ils n'auraient pas fait autrement ou à les attirer vers des espaces commerciaux où ils ne seraient pas allés autrement⁹⁸.

Les techniques de persuasion propulsées par l'IA pourraient même aller plus loin, en cherchant à influencer les états d'âme des consommateurs pour les rendre plus réceptifs aux arguments de

⁹² Aaron RIEKE et al., *Data Brokers In An Open Society*, Open Society Foundation, 2016, p. 5-6

⁹³ Shaun B. SPENCER, « The Problem of Online Manipulation » (2020) 3 *U Ill L Rev* 959, p. 966-967

⁹⁴ *Id.*, p. 962

⁹⁵ Ryan CALO, « Digital Market Manipulation », (2014) 82 *Geo Wash L Rev* 995, p. 1003

⁹⁶ Shaun B. SPENCER, « The Problem of Online Manipulation » (2020) 3 *U Ill L Rev* 959, p. 975-976

⁹⁷ Stéphane AMARISY, « L'IA et l'hyperpersonnalisation du marketing », *Stratégies*, 23 octobre 2018, <https://www.strategies.fr/blogs-opinions/idees-tribunes/4019542W/l-ia-et-l-hyperpersonnalisation-du-marketing.html>

⁹⁸ Shaun B. SPENCER, « The Problem of Online Manipulation » (2020) 3 *U Ill L Rev* 959, p. 962-975

vente qui leur seront ensuite présentés⁹⁹. Ainsi, des expériences ont montré l'immense potentiel des médias sociaux pour influencer les émotions des consommateurs, simplement par le choix des publications affichées sur le fil des internautes¹⁰⁰. Le scandale de Cambridge Analytica illustre de même le degré élevé de sophistication que peuvent atteindre les méthodes d'influence de masse. Dans cette affaire, une entreprise a employé des outils d'apprentissage profond et les données de millions d'utilisateurs de Facebook pour identifier des individus qui pourraient être influencés lors des élections américaines¹⁰¹. Une fois ces personnes identifiées, la firme a lancé une campagne d'influence les ciblant, à leur insu.

Dans un contexte de consommation, on peut imaginer que de telles capacités d'influence pourraient grandement accroître le succès de campagnes publicitaires des entreprises, par exemple en ciblant des personnes ayant perdu leur emploi ou éprouvant des difficultés financières pour leur offrir du crédit, ou encore en présentant des offres à durée limitée à des consommateurs ayant un profil psychologique réceptif aux représentations qui créent un sentiment d'urgence. Or, de telles méthodes de persuasion menacent d'effriter la capacité des consommateurs de faire des choix éclairés, de manière autonome, en amplifiant le déséquilibre informationnel entre les commerçants et les consommateurs. D'un côté, le commerçant peut acquérir une connaissance précise des vulnérabilités et désirs du consommateur; de l'autre côté, le consommateur ignore complètement les processus d'analyse de ses données et les tactiques marketing raffinées qui le ciblent.

À noter que de telles formes de préjudices économiques envers les consommateurs n'ont pas à être le fruit d'actes intentionnels des commerçants; ils peuvent tout simplement résulter de l'analyse par une IA qui aurait pour effet d'identifier les corrélations les plus efficaces pour influencer les comportements des consommateurs. Par exemple, des commerçants peuvent mettre en place des tests aléatoires qui ne visent pas nécessairement à exploiter les biais cognitifs des consommateurs, mais qui aboutissent tout de même à ce résultat par la simple efficacité de l'analyse effectuée par l'IA¹⁰².

3.3.2. Personnaliser les prix en ligne

L'IA rend possible diverses pratiques relatives aux prix annoncés aux consommateurs dans le commerce en ligne¹⁰³. Un commerçant pourrait ainsi effectuer de la tarification dynamique, une pratique qui consiste à faire varier les prix en fonction du contexte, comme le moment de la

⁹⁹ S. C. MATZ et al., *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, Proceedings of the National Academy of Sciences Nov 2017, 114 (48) 12714-12719; DOI: 10.1073/pnas.1710966114

¹⁰⁰ Adam D.I. KRAMER, Jamie E. GUILLROY et Jeffrey T. HANCOCK, *Experimental Evidence of Massive Scale Emotional Contagion through Social Networks*, (2014) 111-24 Proceedings of the National Academy of Science of the United States of America 8788. De même, les algorithmes des médias sociaux ont été accusés de prioriser l'engagement des utilisateurs avec la plateforme, quitte à promouvoir, ce faisant, la controverse, la désinformation et l'extrémisme. Voir : Karen HAO, *How Facebook got addicted to spreading misinformation*, MIT Technology review, 11 mars 2021, <https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/>

¹⁰¹ Nicholas CONFESSORE, « Cambridge Analytica and Facebook: The Scandal and the Fallout So Far », *The New York Times*, 4 avril 2018

¹⁰² Shaun B. SPENCER, « The Problem of Online Manipulation » (2020) 3 *U Ill L Rev* 959

¹⁰³ Ginger ZHE JIN, *Artificial Intelligence and Consumer Privacy*, University of Maryland & NBER, 2018, p. 8

journée, ou l'offre et la demande. Il pourrait aussi recourir à la discrimination par les prix, soit l'affichage de prix différents, à différents consommateurs, selon leur profil.

En fonction de l'historique web d'une personne, de ses caractéristiques personnelles ou d'autres informations sur les appareils qu'elle utilise, un système d'IA pourrait détecter son besoin urgent de se procurer un bien et lui demander un prix plus élevé pour ce bien. Par exemple, Uber a découvert que les consommateurs dont le niveau de la batterie est faible sur leur appareil mobile sont généralement prêts à payer plus cher pour leur course, car ils craignent de ne pas trouver de transporteur avant que leur appareil ne tombe en panne¹⁰⁴.

En pratique, le phénomène de la discrimination des prix reste encore mal documenté. Un sondage réalisé en 2018 indique néanmoins que, parmi les commerçants ayant adopté l'IA pour personnaliser l'expérience-client, 40 % utilisent cette technologie pour personnaliser les prix et les promotions en temps réel¹⁰⁵. De même, des études rapportent des cas où les prix annoncés sur certains sites web ont varié en fonction de caractéristiques propres aux internautes, telles que leur localisation géographique ou encore le fait d'être connecté comme membre d'un site¹⁰⁶.

Outre l'affichage de prix différenciés, d'autres pratiques de personnalisation relatives aux prix pourraient être rendues possibles par l'IA, telles que la tarification au goutte-à-goutte (*drip pricing*), par laquelle un prix ne comportant pas toutes ses composantes est annoncé pour attirer les consommateurs¹⁰⁷. L'IA pourrait aussi permettre de moduler les résultats de recherche pour un article, en présentant des biens dont le prix moyen varie selon le profil de l'internaute lorsqu'il effectue une recherche pour un article sur le site d'un commerçant¹⁰⁸.

Cela dit, bien que de telles pratiques relatives à l'affichage des prix soient techniquement réalisables grâce à l'IA, la mesure dans laquelle les entreprises y recourent reste encore mal documentée. Par exemple, dans une étude ayant identifié des pratiques de discrimination des prix, les chercheurs concluent que ces pratiques ne représentent que moins de 2 % des cas¹⁰⁹. Quoi qu'il en soit, cette forme de personnalisation de l'expérience-client laisse craindre que les consommateurs puissent subir des préjudices économiques par l'usage de l'IA dans un contexte commercial, notamment en annihilant leur capacité de comparer les prix des commerçants en ligne ou en les empêchant de profiter des meilleurs soldes.

¹⁰⁴ Jordan GOLSON, *Uber knows you'll probably pay surge pricing if your battery is about to die*, The Verge, 20 mai 2016, <https://www.theverge.com/2016/5/20/11721890/uber-surge-pricing-low-battery>

¹⁰⁵ OCDE, *Personalised Pricing in the Digital Era*, DAF/COMP(2018)13, 2018, p. 15

¹⁰⁶ Par exemple, une enquête du Wall Street Journal de 2012 avait montré que Staples personnalisait les prix affichés sur son site web en fonction de la localisation géographique des consommateurs, qui était déduite à partir de leur adresse IP. Voir : Jennifer VALENTINO-DEVRIES, Jeremy SINGER-VINE et Ashkan SOLTANI, *Websites Vary Prices, Deals Based on Users' Information*, Wall Street Journal, 24 décembre 2012

¹⁰⁷ EUROPEAN COMMISSION, *Consumer vulnerability across key markets in the European Union*, 2016, p. 308

¹⁰⁸ Aniko HANNAK, Gary SOELLER, David LAZER, Alan MISLOVE, Christo WILSON, *Measuring Price Discrimination and Steering on E-commerce Web Sites*, Proceedings of the 2014 Conference on Internet Measurement, 2014

¹⁰⁹ *Id.* De même, d'autres études mènent à des résultats parfois non concluants. Voir : Thomas HUPPERICH, Dennis TATANG, Nicolai WILKOP, Thorsten HOLZ, CODASPY '18 Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, *An Empirical Study on Price Differentiation Based on System Fingerprints*, 2018; Thomas VISSERS, Nick NIKIFORAKIS, Nataliia BIELOVA, Wouter JOOSEN, *Crying Wolf? On the Price Discrimination of Online Airline Tickets*, 2014

3.3.3. Fausser le libre-marché

L'emploi de l'IA dans le commerce en ligne pose également des risques de collusion par les entreprises. Sur Internet, les commerçants peuvent ajuster instantanément les prix qu'ils annoncent, tout en surveillant en continu les prix annoncés par leurs concurrents. En mettant à profit l'IA, ils pourraient ainsi coordonner automatiquement leurs prix, de façon à les hausser artificiellement¹¹⁰ – faussant ainsi le jeu de la concurrence et privant les consommateurs de la capacité de magasiner les meilleurs soldes.

Cette « collusion algorithmique » pourrait prendre plusieurs formes. Les entreprises pourraient simplement développer des systèmes d'IA visant à surveiller leurs concurrents en ligne et à ajuster leurs prix automatiquement. Les entreprises pourraient aussi se coordonner implicitement, en employant les mêmes systèmes d'IA pour fixer leurs prix de manière dynamique, qui auraient donc le même comportement en matière de fixation des prix. Par exemple, en 2015, les autorités américaines ont épinglé des revendeurs sur Amazon qui employaient un même algorithme pour coordonner leurs prix¹¹¹.

L'une des façons les plus troublantes par laquelle cette collusion pourrait prendre forme reste le recours à une IA de fixation de prix complètement autonome, qui « déciderait » elle-même de développer des mécanismes de concertation des offres sans intervention humaine¹¹². Dans de telles circonstances, ce serait le simple déploiement du système d'IA qui aurait pour effet de créer une forme de cartel, sans toutefois que cela soit intentionnel par les entreprises.

3.4. Le risque de discrimination

En remplaçant les humains par des ordinateurs, on pourrait penser que l'IA permet d'éliminer les biais et les préjugés, et qu'elle limite ainsi les prises de décisions discriminatoires. Après tout, les programmes informatiques ne sont pas entravés par les idées préconçues qu'ont les humains, et ils devraient normalement fonder leurs décisions sur des critères purement objectifs.

Toutefois, la pratique met rudement à l'épreuve cet idéal. Loin d'être neutres et objectifs en toutes circonstances, les systèmes d'IA sont susceptibles de devenir des outils d'exclusion, en faisant des corrélations qui exacerbent les injustices et inégalités préexistantes plutôt qu'en les éliminant¹¹³. Pour les consommateurs, l'IA soulève ainsi la question des risques de discrimination, qui se traduisent par l'exclusion ou l'accès inégal à des biens ou des services¹¹⁴.

¹¹⁰ OECD, *Algorithms and Collusion: Competition Policy in the Digital Age*, 2017, p. 22

¹¹¹ *Id.*, p. 23

¹¹² *Id.*, p. 31-32

¹¹³ AUSTRALIAN HUMAN RIGHTS COMMISSION AND WORLD ECONOMIC FORUM, *Artificial Intelligence: Governance and Leadership*, 1^{er} février 2019, p. 9

¹¹⁴ Aviv GAON et Ian STEDMAN, « A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada », (2019) 56-4 *Alta L Rev* 1137, p. 1144-1145

Un problème fondamental des systèmes d'IA tient dans la qualité des données qu'ils emploient. L'IA peut être nourrie de données qui ne sont pas représentatives de la diversité humaine ou qui reflètent des biais ou des préjugés, tels que le sexisme et le racisme¹¹⁵. Par exemple, si l'on demande uniquement à des hommes de dessiner une chaussure afin d'entraîner un système d'IA à reconnaître des chaussures, il est envisageable que cet algorithme ne pourra pas reconnaître des chaussures de femmes¹¹⁶. De surcroît, les algorithmes d'IA peuvent recourir à des critères discriminatoires pour prendre leurs décisions, marginalisant d'autant plus ces groupes.

Par ailleurs, un système d'IA pourrait être déployé dans un contexte inapproprié, par exemple dans un contexte culturel différent de celui dans lequel il a été initialement créé. Certaines langues, comme l'anglais, sont ainsi largement surreprésentées dans les bases de données, ce qui réduit la performance des systèmes d'IA à l'égard d'autres langues¹¹⁷. Pourtant, malgré ces limitations des systèmes d'IA, des utilisateurs pourraient supposer que les prédictions de l'IA sont plus justes et plus précises (et donc plus fiables) que celles faites par des humains – et y prêter davantage foi.

Aux États-Unis, de nombreux cas ont été rapportés de systèmes d'IA ayant des effets discriminatoires selon l'origine ethnique d'une personne. Une étude a ainsi révélé que des systèmes commerciaux de reconnaissance faciale présentaient des taux d'erreurs élevés à l'égard des personnes noires¹¹⁸. Similairement, le logiciel *Vision AI* de Google a reconnu la main d'une personne noire tenant un capteur de température comme étant une arme à feu, alors que pour la main d'une personne blanche, le logiciel a catégorisé l'image comme un appareil électronique¹¹⁹. Chez Amazon, un algorithme a fait en sorte que des quartiers habités majoritairement par des personnes noires étaient exclus du service Amazon Prime¹²⁰. En 2015, une enquête a révélé que la modulation des prix qu'un commerçant effectuait en fonction de la localisation des consommateurs avait pour effet que les personnes d'origine asiatique se voyaient annoncer des prix plus élevés que les autres consommateurs¹²¹.

Les systèmes d'IA pourraient aussi faire des corrélations préjudiciables en fonction d'autres caractéristiques, notamment la condition économique ou le genre. Par exemple, en 2015, une

¹¹⁵ Jocelyn MACLURE et Marie-Noëlle SAINT-PIERRE, « Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques », (2018) 30-3 *Les Cahiers de propriété intellectuelle* 741, p. 755-756

¹¹⁶ Exemple inspiré de : <https://www.youtube.com/watch?v=59bMh59JQDo>

¹¹⁷ Hugo CYR, Sébastien GAMBS et Marie-Jean MEURS, *Pour un développement plus égalitaire de l'IA*, Policy Options, 12 février 2018, <https://policypoptions.irpp.org/magazines/february-2018/pour-un-developpement-plus-egalitaire-de-lia/>

¹¹⁸ Joy BUOLAMWINI et Timnit GEBRU, « Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification », (2018) 81 *Proceedings of Machine Learning Research* 1

¹¹⁹ Nicolas KAYSER-BRILL, *Google apologizes after its Vision AI produced racist results*, Algorithm Watch, 7 avril 2020, <https://algorithmwatch.org/en/story/google-vision-racism/>

¹²⁰ David INGOLD et Spencer SOPER, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, Bloomberg, 21 avril 2016, <https://www.bloomberg.com/graphics/2016-amazon-same-day/>

¹²¹ Jeff LARSON, Surya MATTU et Julia ANGWIN, *Unintended Consequences of Geographic Targeting*, Technology Science 2015090103, 2015. D'autres exemples peuvent être cités, notamment dans le milieu de la justice ou de la santé. Voir : Julia ANGWIN, Jeff LARSON, Surya MATTU et Lauren KIRCHNER, *Machine Bias*, ProPublica, 23 mai 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; Andrew SMITH, *Using Artificial Intelligence and Algorithms*, Federal Trade Commission, 8 avril 2020, <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms>

étude de la Carnegie Mellon University a montré que moins de femmes que d'hommes se faisaient présenter des annonces en ligne pour des emplois dont le salaire était supérieur à 200 000 \$¹²². En somme, les systèmes d'IA employés dans des contextes commerciaux pose le risque d'exclure des personnes appartenant à certains groupes protégés ou vulnérables, notamment en se faisant refuser l'octroi d'un service ou en se voyant imposer des modalités moins avantageuses.

3.5. Erreurs et faux positifs

Finalement, les systèmes d'IA sont imparfaits et peuvent générer des résultats erronés. En raison de données inexactes ou de processus d'analyse défectueux, l'IA pourrait ainsi faire des prédictions ou prendre des décisions mal fondées¹²³.

Bien entendu, il n'y a guère de conséquences préjudiciables lorsqu'un algorithme de recommandation qui propose à une personne un film qui ne l'intéresse absolument pas. Toutefois, les systèmes d'IA pourraient prendre des décisions ayant des répercussions importantes si elles s'avèrent erronées. Par exemple, un système d'IA pourrait, par erreur, exclure automatiquement un internaute d'une plateforme en ligne, identifier que les activités qu'elle fait sont frauduleuses ou lui imposer des conditions économiques désavantageuses, par exemple dans l'octroi d'un service financier. En 2021, ce fut ainsi le cas des membres d'un band de punk rock, qui furent exclus de Facebook en raison de leur association erronée à des mouvements conspirationnistes¹²⁴.

Un autre type d'erreur des systèmes d'IA pourrait résulter d'une mauvaise interprétation des données qu'ils perçoivent de leur environnement, à l'aide de leurs capteurs. C'est un risque que souligne d'ailleurs Amazon quant aux assistants virtuels :

« Dans certains cas, votre appareil doté d'Alexa peut interpréter un autre mot ou un autre son comme le mot de réveil (par exemple, le nom « Alex » ou si quelqu'un dit « Alexa » à la radio ou à la télévision). Quand cela se produit, nous appelons ça un « faux réveil ». Nous avons une équipe de scientifiques et d'ingénieurs de renommée mondiale qui se consacrent à l'amélioration continue de notre technologie de détection des mots de réveil et à la prévention des faux réveils¹²⁵ ».

C'est dire que les erreurs commises par les systèmes d'IA peuvent avoir non seulement des impacts sur les décisions prises à l'égard d'un consommateur; elles pourraient résulter en la collecte ou la divulgation non autorisées de données.

¹²² Bryon SPICE, *Questioning the Fairness of Targeting Ads Online*, Carnegie Mellon University, 7 juillet 2015, <https://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html>

¹²³ Iria GIUFFRIDA, Fredric LEDERER et Nicolas VERMEYS, « A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law », (2018) 68-3 *Case W Res L Rev* 747, p. 754

¹²⁴ ELECTRONIC FRONTIER FOUNDATION, *Facebook Treats Punk Rockers Like Crazy Conspiracy Theorists, Kicks Them Offline*, 2021, <https://www.eff.org/takedowns/facebook-treats-punk-rockers-crazy-conspiracy-theorists-kicks-them-offline>

¹²⁵ <https://www.amazon.ca/-/fr/gp/help/customer/display.html?nodeId=201602230>

4. Regard sur le cadre juridique canadien

L'IA soulève de multiples enjeux qui ébranlent le droit canadien. Pour parvenir à protéger les consommateurs dans ce nouvel environnement, de nombreux champs du droit devront vraisemblablement être mis à partie, notamment le droit de la consommation, la responsabilité civile, le droit de la concurrence ou encore la propriété intellectuelle.

La protection de la vie privée, bien entendu, est centrale dans cette remise en question du cadre juridique. En effet, l'IA expose la désuétude des lois canadiennes sur la protection des renseignements personnels, autant quant aux droits individuels des consommateurs, quant à l'encadrement des utilisations et des effets de l'IA, et quant à ses mécanismes de mise en œuvre¹²⁶.

4.1. Des données protégées par la loi

Les services commerciaux propulsés par l'IA reposent sur la collecte et l'analyse d'une quantité fulgurante de données personnelles. Cela emporte que les entreprises qui abreuvent de données ces systèmes doivent se conformer aux obligations de la *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après la « Loi fédérale ») ou à celles de lois provinciales équivalentes¹²⁷.

La Loi fédérale s'applique aux organisations du secteur privé qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales¹²⁸. Au sens de la loi, un « renseignement personnel » est une information concernant un individu identifiable¹²⁹. Un renseignement sera considéré comme concernant un « individu identifiable » dès lors qu'il y a une possibilité sérieuse qu'une personne puisse être identifiée au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres¹³⁰.

¹²⁶ Pour un tour d'horizon des enjeux juridiques soulevés par l'IA, voir : COMMISSION D'ACCÈS À L'INFORMATION, *Pour un développement responsable de l'intelligence artificielle qui respecte le droit à la vie privée et responsabilise tous les acteurs impliqués*, mémoire présenté à la Déclaration de Montréal pour une intelligence artificielle responsable, 29 mars 2018

¹²⁷ En vertu de l'article 26(2) b) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5 (ci-après « Loi fédérale »), le gouvernement fédéral peut, par décret, désigner une loi provinciale comme essentiellement similaire à la Loi fédérale. Les entreprises assujetties à des lois provinciales essentiellement similaires en matière de protection des renseignements personnels sont habituellement exonérées de la LPRPDE en ce qui a trait à la collecte, à l'utilisation ou à la communication de renseignements personnels au sein de cette province. Trois provinces, le Québec, l'Alberta et la Colombie-Britannique, ont adopté des lois qui ont été par la suite désignées comme essentiellement similaires : *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1 (ci-après « Loi du Québec »); *Personal Information Protection Act*, S.A. 2003, c. P-6.5 (ci-après « Loi de l'Alberta »); *Personal Information Protection Act*, S.B.C. 2003, c. 63 (ci-après « Loi de la Colombie-Britannique »). Voir : *Décret d'exclusion visant des organisations de la province de Québec*, DORS/2003-374; *Décret d'exclusion visant des organisations de la province d'Alberta*, DORS/2004-219; *Décret d'exclusion visant des organisations de la province de la Colombie-Britannique*, DORS/2004-220

¹²⁸ Loi fédérale, art. 4(1)(2)

¹²⁹ Loi fédérale, art. 2(1)

¹³⁰ *Gordon c. Canada (Ministre de la Santé)*, 2008 CF 258

Compte tenu de cette définition très large, bien des données numériques recueillies et traitées par les systèmes d'IA pourront être qualifiées de renseignements personnels au sens de la loi. Par exemple, l'adresse de protocole Internet (IP) sera considérée comme un renseignement personnel si elle peut être associée à un individu identifiable¹³¹, tout comme l'historique web¹³², ou des métadonnées générées par un internaute. On pourra également inclure dans cette définition des formes de renseignements biométriques comme les empreintes digitales, les empreintes vocales, ou des images d'une personne¹³³.

Par ailleurs, il va de soi que l'exploitation de toutes ces données par des systèmes d'IA appartenant à des entreprises privées constitue une activité commerciale¹³⁴. En guise d'illustration, le CPVP a conclu que Facebook se livrait à une activité commerciale car la collecte, l'utilisation et la communication de renseignements personnels en vue d'améliorer l'expérience des utilisateurs contribuent indirectement au succès du site à titre d'entreprise commerciale¹³⁵.

Le droit se montre donc clair à l'effet que les lois canadiennes sur la protection des renseignements personnels pourront généralement trouver application aux systèmes d'IA déployés par les entreprises privées exerçant leurs activités au Canada. En conséquence, ces entreprises devront respecter les obligations qu'on trouve dans ces lois.

4.2. Les droits individuels des consommateurs

Aux termes de la loi, les consommateurs disposent de certains droits face aux entreprises qui recueillent, utilisent ou communiquent leurs renseignements personnels. Toutefois, ces droits paraissent trop restreints pour faire face aux défis soulevés par l'IA, notamment à l'égard de la capacité du consommateur de s'opposer au traitement de ses renseignements personnels, d'obtenir une explication quant au résultat d'un traitement de données et de remettre en question les résultats de ce traitement.

¹³¹ Commissariat à la vie privée du Canada, *Résumé de conclusions d'enquête en vertu de la LPRPDE #25 – Un radiodiffuseur accusé de recueillir des renseignements personnels avec son site Web*, 20 novembre 2001. En ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2001/lprpde-2001-025/>

¹³² CPVP, *L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée*, Rapport des conclusions en vertu de la LPRPDE no 2014-001, 14 janvier 2014

¹³³ *Wansink c. TELUS Communications Inc*, 2007 CFA 21

¹³⁴ Selon la loi, une « activité commerciale » s'entend de toute activité régulière ainsi que de tout acte isolé, qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds. Voir : Loi fédérale, art. 2(1)

¹³⁵ CPVP, *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc.*, *Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-008*, 16 juillet 2009

4.2.1. Les écueils du consentement dans l'environnement de l'IA

Selon la Loi fédérale, une personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concerne et y consentir, que ce soit au moment de la collecte ou avant qu'une organisation utilise ces renseignements¹³⁶.

Les entreprises doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon à ce que la personne puisse raisonnablement comprendre de quelle manière ses renseignements personnels seront utilisés ou communiqués¹³⁷.

La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. Selon le CPVP, une entreprise devrait généralement obtenir un consentement explicite (*opt-in*) si les renseignements sont susceptibles d'être considérés comme sensibles. Un tel consentement pourrait être obtenu, par exemple, à l'aide de fenêtres contextuelles qui indiquent des informations essentielles. Lorsque les renseignements sont moins sensibles, un consentement implicite (*opt-out*) pourra être suffisant¹³⁸. Selon le CPVP, le consentement explicite reste la forme de consentement la plus adéquate et respectueuse à utiliser, même si le consentement implicite peut être acceptable dans des circonstances strictement définies¹³⁹.

Or, ce modèle pose de nombreux défis dans l'environnement numérique, où les entreprises obtiennent généralement le consentement du consommateur par l'entremise de politiques de confidentialité longues et complexes, que les internautes ne lisent généralement pas¹⁴⁰. Ces documents énoncent des finalités vagues et prospectives à l'utilisation des renseignements personnels, si larges en fait qu'elles autorisent ultimement les entreprises à les traiter comme bon leur semble (section 2.1)¹⁴¹. De surcroît, les consommateurs qui veulent souscrire aux services de ces entreprises n'ont guère le choix d'accepter leurs conditions d'utilisation. L'information et le contrôle des consommateurs sur leur vie privée, dans cet environnement, restent donc souvent illusoire.

Le consentement peut même devenir un sésame qui permet aux entreprises de faire ce qu'elles veulent des données personnelles des citoyens, pour peu qu'elles aient glissé quelques

¹³⁶ Loi fédérale, annexe 1, principe 4.3.1. À noter que la loi comporte certaines exceptions au consentement, par exemple lorsqu'on utilise les renseignements personnels pour répondre à une situation d'urgence mettant en danger la vie d'un individu.

¹³⁷ Loi fédérale, art. 6.1 et annexe 1, principe 4.3.2

¹³⁸ Loi fédérale, annexe 1, principes 4.3.4., 4.3.6

¹³⁹ CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, mai 2018, https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/. Voir également : CPVP, *Une banque n'obtient pas le consentement explicite de ses clients pour communiquer leurs renseignements personnels*, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2003-192, 23 juillet 2003; CPVP, *Un particulier laisse percer ses inquiétudes quant aux clauses de consentement sur un formulaire de demande de carte de crédit*, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2003-203, 5 août 2003

¹⁴⁰ Voir à cet effet : Uri BENOLIEL et Shmuel L. BECHER, « The Duty to Read the Unreadable », (2019) 60 *Boston College Law Review* 2255; Aleecia M. MCDONALD et Lorrie Faith CRANOR, « The cost of Reading Privacy Policies », (2008) 4 *ISJLP* 543

¹⁴¹ Ginger ZHE JIN, *Artificial Intelligence and Consumer Privacy*, University of Maryland & NBER, 2018, p. 1

mentions dans une politique de confidentialité. Le CPVP va jusqu'à affirmer que cette approche pourrait se montrer nuisible dans le cadre de l'IA :

« En fait, le consentement peut servir à légitimer des usages qui, objectivement, sont complètement déraisonnables et contraires à nos droits et valeurs. De plus, lorsque l'utilisation des données peut profiter à la société, le refus de donner son consentement peut parfois nuire à l'intérêt public.¹⁴² »

En conséquence, le modèle du consentement ne peut, à lui seul, protéger adéquatement le public contre les effets délétères possibles des systèmes d'IA, et il doit être accompagné d'autres balises juridiques permettant de protéger le public.

4.2.2. Mieux informer : le droit à une explication

Si la loi prévoit que les consommateurs doivent être informés adéquatement et consentir aux pratiques des entreprises, elle demeure perfectible pour leur fournir une information complète face à la complexité des systèmes d'IA.

Les systèmes d'IA sont opaques. Les consommateurs peuvent ignorer faire l'objet d'une décision automatisée, ou encore ne pas comprendre les rouages derrière ces décisions (section 3.2). Or, la Loi fédérale ne contient aucune disposition spécifique sur le droit d'une personne d'être informée de l'existence d'une prise de décision automatisée à son égard, pas plus qu'elle ne prévoit de droit à l'explication pour les consommateurs quant à la façon dont ces décisions ont été rendues.

Certes, la loi prévoit un droit d'accès aux renseignements personnels pour les consommateurs, par lequel une entreprise doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, ainsi que lui permettre de consulter ces renseignements¹⁴³. Toutefois, ce droit n'inclut pas la possibilité, pour le consommateur, de savoir comment une décision a été prise sur la base de ses renseignements personnels. En conséquence, un consommateur pourrait se voir refuser automatiquement un service par un système d'IA, ou se voir exclu d'une plateforme, sans qu'il ne puisse savoir *pourquoi*.

Bien entendu, puisque les entreprises elles-mêmes ne sont pas toujours en mesure d'expliquer les décisions prises de manière autonomes par l'IA, un « droit à l'explication » devrait être formulé de manière générale. En pratique, un tel droit pourrait donc exiger que l'entreprise fournisse au consommateur les facteurs et les motifs ayant déterminé la prise de décision, en plus des renseignements personnels ayant été utilisés par en arriver à ce résultat. Un tel droit permettrait non seulement au consommateur de mieux appréhender le processus qui a mené à la décision, mais aussi de contester cette décision s'il estime qu'elle est mal fondée.

¹⁴² CPVP, *Un cadre réglementaire pour l'IA : recommandations pour la réforme de la LPRPDE*, novembre 2020, https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/reg-fw_202011/

¹⁴³ Loi fédérale, annexe 1, principes 4.9, 4.9.1

4.2.3. Améliorer le consentement : le droit de contester

Un consommateur peut faire l'objet de décisions prises par des systèmes d'IA qui auront des répercussions importantes dans sa vie. Dès lors, non seulement est-il pertinent de lui expliquer la teneur de ces décisions, mais il devrait de plus avoir l'occasion de refuser ce traitement en certaines circonstances, et aussi de pouvoir remettre valablement en question le résultat de ce traitement automatisé s'il s'avère injuste.

La Loi fédérale prévoit déjà, pour le consommateur, le droit de retirer son consentement en tout temps, sous réserve de restrictions légales ou contractuelles et d'un préavis raisonnable¹⁴⁴. Théoriquement, cette faculté lui permet de refuser que ses renseignements personnels fassent l'objet d'un traitement automatisé par l'IA.

Toutefois, en pratique, refuser équivaut généralement à renoncer à utiliser un service – ou encore à payer plus cher pour y avoir accès. Par exemple, dans le domaine des assurances, un consommateur peut refuser que sa prime d'assurance soit fixée à partir de son pointage de crédit; néanmoins, il devra payer généralement bien plus cher s'il fait ce choix¹⁴⁵. En somme, si la Loi fédérale donne indirectement, par l'entremise du principe du consentement, un « droit d'opposition », l'exercice de ce droit peut résulter en l'exclusion du consommateur ou en un préjudice économique.

De même, la Loi fédérale ne permet pas au consommateur de remettre en question le résultat du traitement effectué par un système d'IA. Certes, la loi prévoit que les consommateurs peuvent contester le caractère exact, à jour et complet d'un renseignement personnel¹⁴⁶. Lorsqu'une personne démontre que des renseignements personnels sont inexacts ou incomplets, l'organisation doit les rectifier¹⁴⁷. Toutefois, ces dispositions ne permettent pas explicitement d'exiger qu'une personne humaine révise une décision prise automatiquement par un algorithme. C'est dire que, dès lors que le consommateur a donné son accord au traitement de données effectué par l'IA, sa capacité d'opposition quant au résultat de ce traitement pourrait se montrer fort limitée.

Finalement, au-delà du droit de révision, la loi est également muette quant à la possibilité, pour les consommateurs, de déterminer les critères sous-jacents aux systèmes d'IA¹⁴⁸. Les consommateurs ne disposent d'aucun droit quant à leur possibilité de choisir eux-mêmes des facteurs qui déterminent la personnalisation dont ils font l'objet, comme le type de contenu qui leur est proposé. Bref, le public n'a guère son mot à dire quant aux intrants dans les systèmes d'IA qui analysent leurs renseignements personnels.

¹⁴⁴ Loi fédérale, annexe 1, principe 4.3.8

¹⁴⁵ Stéphanie GRAMMOND, *Votre dossier de crédit peut tripler votre prime d'assurance*, La Presse, 20 septembre 2020, <https://www.lapresse.ca/affaires/finances-personnelles/2020-09-20/votre-dossier-de-credit-peut-tripler-votre-prime-d-assurance.php>

¹⁴⁶ Loi fédérale, annexe 1, principe 4.9

¹⁴⁷ Loi fédérale, annexe 1, principe 4.9.5

¹⁴⁸ Cette idée est notamment soulevée dans : Kaveh WADDELL, *Tech Companies Too Secretive About Algorithms That Curate Feeds*, *Study Says*, Consumer Reports, 24 février 2021, <https://www.consumerreports.org/consumer-protection/tech-companies-too-secretive-about-algorithms-that-curate-feeds/>

4.3. L'encadrement des utilisations et des effets de l'IA

4.3.1. Des balises ténues

Face aux défis collectifs que pose l'emploi de l'IA dans un contexte commercial, des solutions centrées exclusivement sur les droits individuels ne pourront suffire. Pour mitiger certains risques de l'IA, tels que le risque de discrimination et le risque de préjudice économique, des solutions visant à encadrer les pratiques des entreprises sont manifestement nécessaires. Or, les balises qu'offre actuellement la loi se montrent, dans le meilleur des cas, fort imprécises.

La loi pose des limites quant à la quantité et au type de renseignements qu'une entreprise peut recueillir et utiliser. La Loi fédérale prévoit ainsi qu'une entreprise ne peut recueillir que les renseignements personnels « nécessaires » à ses fins¹⁴⁹. Mais qu'est-ce qui est nécessaire, exactement, dans le contexte de l'IA?

La question reste ouverte. Les systèmes d'IA reposent sur la captation et l'analyse d'une quantité phénoménale de données, parmi lesquelles il est bien difficile de distinguer ce qui est « nécessaire » de ce qui ne l'est pas. Face à cette dissonance entre le fonctionnement des systèmes d'IA et les limites qu'impose la loi quant à la quantité de renseignements personnels recueillis, des auteurs suggèrent de repenser le cadre juridique en insistant davantage sur les finalités du traitement de données plutôt que sur le principe de limitation de la collecte¹⁵⁰.

À cet égard, l'une des pistes juridiques les plus prometteuses tient dans une disposition qui chapeaute la Loi fédérale : une entreprise « ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances¹⁵¹ ». Dans le cadre de l'IA, cette obligation pourrait faire en sorte d'interdire certaines utilisations illégitimes des renseignements personnels, et ce même si le consommateur y a donné son consentement. Bref, plutôt que de chercher à limiter les intrants dans les systèmes d'IA, la loi pourrait en encadrer davantage les extrants.

Pour déterminer si les fins d'une entreprise sont « acceptables dans les circonstances », les tribunaux ont soupesé plusieurs critères, notamment le caractère délicat des renseignements personnels en question, les besoins commerciaux légitimes de l'entreprise et la proportionnalité de l'atteinte à la vie privée par rapport à ses avantages¹⁵². Différentes pratiques des entreprises ont été considérées inacceptables au terme de cette évaluation, telles que de l'exigence de

¹⁴⁹ Loi fédérale, annexe 1, principe 4.4

¹⁵⁰ Pierre-Luc DÉZIEL, « Est-ce bien nécessaire? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans BARREAU DU QUÉBEC, *Développements récents en droit à la vie privée*, Éditions Yvon Blais, 2019

¹⁵¹ Loi fédérale, art. 5(3). Voir aussi : *Loi de Colombie-Britannique*, art. 4(1); *Loi de l'Alberta*, art. 6(1), 11(2), 16(2) et 19(2). Au Québec, on ne trouve pas de critère exprimé de manière semblable; toutefois, la loi prévoit qu'une entreprise qui constitue un dossier sur une personne « doit avoir un intérêt sérieux et légitime à le faire ». Voir : Loi du Québec, art. 4; *Code civil du Québec*, L.Q. 1991, c. 64, art. 37

¹⁵² CPVP, *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)*, mai 2018, https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gd_53_201805/; Timothy M. BANKS, *A Guide to the Personal Information Protection and Electronic Documents Act*, LexisNexis, 2018, p. 89-94

communiquer les mots de passe des comptes de réseaux sociaux dans un processus d'embauche ou encore la surveillance de masse des citoyens par une entité privée¹⁵³.

Dans un contexte de consommation, de telles balises pourraient être employées pour encadrer deux risques inhérents aux systèmes d'IA : le risque de discrimination (section 4.3.2) et le risque d'exploitation économique (section 4.3.3).

4.3.2. Le droit à l'égalité

Un système d'IA qui aurait pour effet de mener à une discrimination interdite en vertu des lois canadiennes sur les droits de la personne serait manifestement illégal – et un tel usage des données constituerait de même une fin inacceptable au sens de la Loi fédérale¹⁵⁴.

Selon la loi, la discrimination se définit comme une distinction, une exclusion ou une préférence ayant pour effet de détruire ou de compromettre le droit à l'égalité. Au Canada, diverses lois fédérales et provinciales interdisent de faire une distinction préjudiciable envers une personne sur la base de certains motifs¹⁵⁵. Les motifs prohibés ne sont pas exactement les mêmes d'une loi à l'autre, mais ils regroupent généralement l'origine nationale ou ethnique, la religion, l'âge, le sexe, l'orientation sexuelle, l'identité ou l'expression de genre, l'état matrimonial, la situation familiale, les caractéristiques génétiques ou le handicap¹⁵⁶.

La discrimination peut être directe ou indirecte. La discrimination directe en constitue la forme la plus flagrante; elle a lieu « lorsqu'une personne est soumise à un traitement différent reposant sur un motif de discrimination prohibé, et ce, de façon ouverte et avouée¹⁵⁷ ». La discrimination indirecte est plus subtile et se produit généralement sans intention. Dans ces cas, la situation discriminatoire découle plutôt de l'application uniforme d'une norme, d'une politique, d'une règle ou d'une pratique, neutre à première vue, ayant néanmoins un effet

¹⁵³ CPVP, *Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta*, Rapport de conclusions d'enquête en vertu de la LPRPDE no 2021-001, 2 février 2021, <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/>

¹⁵⁴ CPVP, *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)*, mai 2018, https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gd_53_201805/. Dans ce document, le CPVP mentionne aussi d'autres fins qu'il estime inacceptables, notamment la collecte, l'utilisation ou la communication qui autrement serait illégale, ou encore la collecte, l'utilisation ou la communication à des fins qui sont susceptibles de causer un préjudice grave à des individus.

¹⁵⁵ Voir notamment : *Loi canadienne sur les droits de la personne*, L.R.C. (1985), ch. H-6 (fédéral); *Charte des droits et libertés de la personne*, RLRQ, chap. C-12 (Québec); *Code des droits de la personne*, L.R.O. 1990, chap. H.19 (Ontario); *Human Rights Code*, [RSBC 1996] CHAPTER 210 (Colombie-Britannique); *Alberta Human Rights Act*, RSA 2000 c. A-25.5 (Alberta); *The Saskatchewan Human Rights Code*, S.S. 1979, c. S-24.1 (Saskatchewan); *The Human Rights Code*, C.C.S.M. c. H175 (Manitoba); *Loi sur les droits de la personne*, LRN-B 2011, c. 171 (Nouveau-Brunswick); *Human Rights Act*, RSNS 1989, c. 214 (Nouvelle-Écosse); *Human Rights Act*, RSPEI 1988, c. H-12 (Île-du-Prince-Édouard); *Human Rights Act*, 2010, SNL 2010, c H-13.1 (Terre-Neuve-et-Labrador)

¹⁵⁶ *Loi canadienne sur les droits de la personne*, L.R.C. (1985), ch. H-6, art. 3

¹⁵⁷ COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Profilage racial et discrimination systémique des jeunes racisés*, Rapport de la consultation sur le profilage racial et ses conséquences, 2011, p. 13

discriminatoire auprès d'un individu ou d'une catégorie d'individus en leur imposant des obligations, des peines ou des conditions restrictives non imposées à autrui¹⁵⁸.

En conséquence, au regard de la loi, une entreprise dont le traitement de renseignements personnels effectué par un système d'IA aurait pour effet de désavantager une personne sur la base de son appartenance à un groupe protégé pourrait agir dans l'illégalité. Comme on l'a vu précédemment, de nombreux cas ont été rapportés où des groupes ont été exclus par des systèmes d'IA (section 3.3.1); on peut dès lors penser que ces normes pourraient s'appliquer dans de telles situations.

4.3.3. Des interdictions à clarifier

Outre la discrimination illicite, les systèmes d'IA peuvent aussi entraîner d'autres situations préjudiciables pour les consommateurs. Les techniques de persuasion et de personnalisation hautement sophistiquées que permet l'IA pourraient résulter en de l'exploitation économique des consommateurs, dans laquelle on profiterait de la connaissance intime de leur situation pour tirer indument avantage d'eux (section 3.3).

Face à de telles situations, le droit se montre plus hésitant. D'emblée, les lois canadiennes sur la protection du consommateur n'encadrent généralement pas les techniques de persuasion en tant que telles. Les messages publicitaires doivent être véridiques et ne peuvent omettre un fait important; toutefois, les méthodes qu'emploient les commerçants pour convaincre les consommateurs restent largement à leur discrétion. Par ailleurs, si la *Loi sur la concurrence* interdit à des entreprises de faire de la collusion, encore faut-il parvenir à faire la difficile démonstration que des algorithmes autonomes ont facilité la commission de telles pratiques anticoncurrentielles¹⁵⁹.

Dans sa mouture actuelle, la Loi fédérale pourrait limiter certains usages abusifs de l'IA en les désignant comme étant « inacceptables ». Toutefois, délimiter le champ des pratiques commerciales inacceptables reste un exercice périlleux. Dans ses orientations sur la question, le CPVP suggère que le « profilage ou la catégorisation injuste ou contraire à l'éthique » et que le traitement de données personnelles susceptible « de causer un préjudice probable et grave à des individus », comme la « perte financière » pourraient être considérés comme inacceptables dans certaines circonstances¹⁶⁰. D'autres instruments normatifs volontaires peuvent également fournir des pistes de réponse. Par exemple, la *Déclaration de Montréal* prévoit que les systèmes d'IA « ne doivent pas construire de profils de préférences individuelles pour influencer le comportement des personnes concernées sans leur consentement libre et éclairé » et qu'ils

¹⁵⁸ Daniel CARPENTIER, *Avis sur les directives de l'assurance maladie du Québec en matière d'accommodement raisonnable*, Commission des droits de la personne et des droits de la jeunesse, 22 février 2010, p. 2-7

¹⁵⁹ Aviv GAON et Ian STEDMAN, « A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada », (2019) 56-4 *Alta L Rev* 1137, p. 1147; COMPETITION BUREAU, *Big data and Innovation: Implications for Competition Policy in Canada*, Draft Discussion Paper, 2017, [https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Big-Data-e.pdf/\\$file/Big-Data-e.pdf](https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Big-Data-e.pdf/$file/Big-Data-e.pdf)

¹⁶⁰ CPVP, *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)*, mai 2018, https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gd_53_201805/

doivent « contribuer à éliminer les relations de domination entre les personnes et les groupes fondées sur la différence de pouvoir, de richesses ou de connaissance.¹⁶¹ »

Autrement dit, si le droit peut offrir des prises pour interdire les préjudices économiques causés aux consommateurs par l'IA, ces situations devront manifestement être évaluées au cas par cas. Face à une telle incertitude du droit, on pourrait souhaiter que la loi contienne davantage de précisions pour clarifier ces interdictions.

4.4. Les écueils de la mise en œuvre de la loi

4.4.1. La transparence des systèmes d'IA et la prévention des préjudices

L'un des enjeux dégagés dans la présente étude tient dans le fait que les systèmes d'IA pourraient avoir des conséquences discriminatoires ou autrement préjudiciables envers les consommateurs. Si la loi peut offrir quelques remèdes lorsqu'une telle situation est révélée, il demeure que ces biais risquent de passer inaperçus ou de se répéter constamment si des mécanismes de transparence et de contrôle ne sont pas mis en œuvre.

Or, les algorithmes sont souvent des boîtes noires qui agissent de manière autonome, et dont les effets peuvent être inconnus même de leurs concepteurs. Dans un tel contexte, comment faire pour savoir s'ils ont des effets préjudiciables? Comment peut-on enquêter pour comprendre le fonctionnement et les effets des systèmes d'IA sur les consommateurs?

Certes, la Loi fédérale prévoit des obligations de transparence pour les entreprises. Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles au public¹⁶². De plus, une personne doit pouvoir obtenir sans effort déraisonnable de l'information au sujet des politiques et des pratiques d'une organisation, sous une forme compréhensible¹⁶³. Néanmoins, ces obligations paraissent incomplètes pour comprendre les rouages des systèmes d'IA et, surtout, leurs impacts.

D'emblée, la loi ne prévoit pas d'obligation de transparence quant aux algorithmes – en fait, le droit canadien pose même des entraves quant à la possibilité d'y avoir accès. Au regard du droit, un système d'IA pourrait ainsi être considéré comme un secret commercial, à savoir une information non accessible ayant une valeur commerciale, et pour laquelle le propriétaire prend des mesures pour la garder secrète¹⁶⁴. Un tel statut laisse planer un doute quant à la possibilité public d'y avoir accès ou d'en faire la rétroingénierie, par exemple à l'aide de robots qui étudieraient le comportement des systèmes d'IA sur des plateformes commerciales.

¹⁶¹ <https://www.declarationmontreal-iaresponsable.com/la-declaration>

¹⁶² Loi fédérale, annexe 1, principe 4.8

¹⁶³ Loi fédérale, annexe 1, principe 4.8.1

¹⁶⁴ Alexandra STEELE, « Les dessous des informations confidentielles et des secrets de commerce », dans BARREAU DU QUÉBEC, *Développements récents en droit de la non-concurrence*, 2009, vol. 313, Éditions Yvon Blais, 95-144; Isi CAULDER et Paul BLIZZARD, *Protecting and navigating intellectual property for artificial intelligence based technologies*, Bereskin & Parr, mai 2018

Bien entendu, l'accès aux codes sources des entreprises n'est guère une considération pour le consommateur moyen, qui n'a ni les ressources, ni le temps, ni les connaissances pour en étudier le fonctionnement. Toutefois, un tel accès donnerait à la société civile, aux organismes gouvernementaux et aux chercheurs l'opportunité d'examiner plus en détail ces systèmes, leurs effets et leurs conséquences.

Outre la question de la transparence, la loi ne prévoit pas explicitement de mesures de prévention quant aux systèmes d'IA. Ainsi, les entreprises n'ont pas l'obligation de tenir une analyse préalable de risque quant aux effets de leurs systèmes d'IA. De même, la loi n'incorpore pas les principes de protection des données dès la conception et de protection des données par défaut. Pourtant, des obligations de ce type contribueraient à s'assurer que les entreprises mitigent les risques de leurs systèmes d'IA en amont, de façon à prévenir leurs impacts préjudiciables. À cet égard, le gouvernement du Canada a déjà développé un outil d'évaluation d'incidence algorithmique qui pourrait se transposer dans le secteur privé¹⁶⁵.

De même, la loi reste muette quant à la surveillance des systèmes d'IA, une fois leur déploiement effectué. Encore là, bien des méthodes d'encadrement peuvent être envisagées, telle que la tenue d'études d'impacts pour identifier les biais de ces systèmes, ou encore la création de mécanismes externes de surveillance pour garantir la responsabilité des développeurs d'IA¹⁶⁶.

4.4.2. Le besoin de normes contraignantes

Face aux défis que pose l'IA, plusieurs solutions faisant appel à l'autoréglementation et à des principes éthiques ont été développées (section 2.1.3). De par le monde, il existe actuellement une pléthore de codes d'éthiques et d'instruments volontaires visant à établir des normes pour encadrer l'IA, chacun avec des approches distinctes, tels que la *Déclaration de Montréal*¹⁶⁷.

Si de telles lignes directrices peuvent effectivement fournir des pistes intéressantes dans le développement de systèmes d'IA, force est de constater qu'un cadre éthique constitue un outil d'adhésion volontaire pour les entreprises, sans mécanismes externes de mise en œuvre. Dans un contexte de rapports économiques asymétriques, de tels préceptes ne peuvent donc pas, à eux seuls, fournir au public des garanties élevées de protection. Même si le Canada se dotait d'un cadre harmonisé pour faire face aux défis que pose l'IA dans un contexte de consommation, ces normes ne seront guère utiles si les entreprises peuvent négliger de les suivre sans s'exposer à des sanctions.

Ici, rappelons que les organismes publics ayant pour mission d'appliquer les lois sur la protection de renseignements personnels disposent de peu d'instruments dissuasifs pour mettre en œuvre ces lois. Le CPVP, qui est chargé de l'application de la Loi fédérale, fait office d'ombudsman, c'est-à-dire qu'il reçoit des plaintes ou en prend l'initiative, enquête et règle les plaintes,

¹⁶⁵ Voir : <https://ouvert.canada.ca/aia-eia-js/?lang=fr>

¹⁶⁶ Pour un tour d'horizon de ces mécanismes, voir : ADA LOVELACE INSTITUTE, *Examining the Black Box*, 2020, <https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-DataKind-UK-Examining-the-Black-Box-Report-2020.pdf>

¹⁶⁷ Voir à cet égard : Jessica FJELD et al., *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, Berkman Klein Center for Internet & Society, 2020

effectue des vérifications et sensibilise le public aux questions relatives à la protection des renseignements personnels¹⁶⁸.

Toutefois, au terme d'une plainte, le CPVP n'a pas de pouvoir de contrainte face aux entreprises et ne peut leur imposer de sanctions pécuniaires¹⁶⁹. Pour contraindre une entreprise à modifier ses pratiques, la seule possibilité qui s'offre alors au CPVP est de s'adresser à la Cour fédérale, qui pourra rendre une décision contraignante¹⁷⁰. On peut dès lors imaginer une myriade de situations où une entreprise ferait preuve de négligence dans ses pratiques de collecte ou d'utilisation des renseignements personnels, sans que cela n'emporte la moindre conséquence juridique pour elle. Par exemple, dans l'affaire Clearview AI, le CPVP a estimé que l'entreprise avait illégalement mis en œuvre un véritable système de surveillance de masse des citoyens sans même obtenir leur consentement; pourtant, malgré la sévérité de la décision, l'entreprise n'a essuyé aucune sanction¹⁷¹.

Finalement, une mise en œuvre efficace de loi implique qu'elle puisse être interprétée de manière à donner prépondérance à la protection de la vie privée sur les intérêts commerciaux des entreprises. Or, la clause d'objet de la Loi fédérale propose plutôt un équilibre entre, d'une part, le « droit des individus à la vie privée » et, d'autre part, le « besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels »¹⁷². Dans le contexte de l'IA, où les mécanismes traditionnels d'information et de consentement perdent leur efficacité pour protéger le public, un tel équilibre mériterait assurément d'être revu¹⁷³.

¹⁶⁸ Loi fédérale, annexe 1, principe 4.10

¹⁶⁹ Loi fédérale, art. 13. À noter que les commissaires provinciaux disposent de pouvoirs d'ordonnance, contrairement au CPVP. Voir : Loi de l'Alberta, art. 52; Loi de la Colombie-Britannique, art. 52; Loi du Québec, art. 83

¹⁷⁰ Loi fédérale, art. 14-16

¹⁷¹ CPVP, *Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta*, Rapport de conclusions d'enquête en vertu de la LPRPDE no 2021-001, 2 février 2021

¹⁷² Loi fédérale, art. 3

¹⁷³ Voir à ce sujet : Mark LATONERO, *Governing Artificial Intelligence: Upholding Human Rights and Dignity*, Data and Society, 10 octobre 2018, <https://datasociety.net/library/governing-artificial-intelligence/>

5. S'inspirer de l'étranger

Pour trouver des propositions innovantes quant à l'encadrement de l'IA, le Canada pourrait tourner son regard vers l'étranger. À cet égard, l'Union européenne propose quelques solutions dignes d'intérêt, notamment quant à l'information et au droit d'opposition du consommateur (section 5.1). Toutefois, le droit américain contient actuellement peu de normes innovantes face à l'IA (section 5.2).

5.1. Europe : un cadre inspirant à plusieurs égards

Le *Règlement général sur la protection des données* (RGPD)¹⁷⁴ unifie le cadre juridique dans les États membres de l'UE quant au traitement des données à caractère personnel. Ce texte législatif compte sans conteste parmi les plus rigoureux au monde et comporte plusieurs dispositions d'intérêt dans une perspective d'encadrement de l'IA.

Le RGPD prévoit ainsi des sanctions élevées aux entreprises contrevenantes, la tenue d'études d'impact dans certaines circonstances et des dispositions faisant en sorte de protéger les consommateurs des conséquences discriminatoires découlant du traitement de leurs données personnelles. En particulier, nous soulignerons ici quelques droits individuels conférés par le RGPD qui pourraient être transposés dans le contexte canadien.

5.1.1. Des obligations d'information bonifiées

Lorsqu'elles recueillent leurs données personnelles, les entreprises assujetties au RGPD doivent fournir aux consommateurs plusieurs informations¹⁷⁵, notamment les catégories de données personnelles traitées, les finalités du traitement, ainsi que les droits dont ils disposent quant à ces données¹⁷⁶. Les responsables du traitement ne peuvent recueillir et traiter des données personnelles à des fins autres que celles qui ont été mentionnées aux consommateurs, à moins qu'ils ne leur fournissent des informations supplémentaires.

En particulier, une entreprise devra informer le consommateur de l'existence d'une prise de décision entièrement automatisée à son égard, incluant le profilage du consommateur¹⁷⁷. Pour ce faire, l'entreprise devra fournir « des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.¹⁷⁸ » Une telle obligation, qu'on ne trouve pas en droit canadien, permet au consommateur d'être informé qu'un système d'IA autonome traite ses données personnelles et d'obtenir des précisions sur son fonctionnement.

¹⁷⁴ *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, [2016] JO, L 119/1 (ci-après « RGPD »)

¹⁷⁵ RGPD, art. 5, 12, 13, 14, considérants 58-63

¹⁷⁶ RGPD, art. 13

¹⁷⁷ RGPD, art. 14

¹⁷⁸ *Id.*

5.1.2. Écarter le consentement... à certaines conditions

Le RGPD énonce que les entreprises ne peuvent traiter les données personnelles que s'il existe un « fondement » juridique qui autorise ce traitement¹⁷⁹. Parmi ces fondements, on compte non seulement le consentement de la personne concernée, mais aussi d'autres situations où le traitement est nécessaire pour des intérêts légitimes poursuivis par l'entreprise.

C'est dire que le RGPD permet à une entreprise, dans certaines circonstances, de recueillir et d'utiliser des données personnelles sans le consentement du consommateur. Toutefois, les entreprises qui souhaitent invoquer qu'un traitement de données est nécessaire à leurs intérêts légitimes doivent s'assurer qu'elles ne contreviennent pas aux droits fondamentaux de la personne concernée, et doivent offrir un mécanisme d'opposition aux consommateurs (voir section suivante)¹⁸⁰. Contrairement à la loi canadienne, le RGPD ne repose donc pas exclusivement sur le principe du consentement; toutefois, cette exemption limitée s'inscrit dans un contexte où le droit à la vie privée prévaut sur les intérêts commerciaux des entreprises.

En outre, dans les cas où le consentement est le fondement au traitement, le RGPD exige qu'il soit « explicite » et « positif »¹⁸¹. Le consentement devrait être donné par un acte positif clair à travers lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement de ses données à caractère personnel. Pour que le consentement soit éclairé, le consommateur « devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnelles¹⁸². »

5.1.3. Le droit d'opposition et de révision

Comme au Canada, le RGPD donne aux consommateurs la possibilité de refuser le traitement de leurs données personnelles en retirant le consentement qu'ils ont donné à une entreprise¹⁸³. De même, le RGPD donne aux consommateurs le droit de s'opposer au traitement de leurs données personnelles lorsque qu'il est basé sur l'intérêt légitime de l'entreprise¹⁸⁴. Dans ces cas, le responsable du traitement doit cesser de traiter les données à caractère personnel, à moins qu'il ne démontre qu'il existe des intérêts légitimes impérieux de poursuivre le traitement.

De plus, certaines dispositions du RGPD pourraient contribuer à prémunir un consommateur contre les préjudices économiques résultants de son refus de faire l'objet d'un traitement de données par l'IA. Ainsi, le RGPD prévoit que le consentement ne devrait pas être considéré comme libre si le consommateur « ne dispose pas d'une véritable liberté de choix ou n'est pas

¹⁷⁹ RGPD, art. 5-10, considérants 39-48

¹⁸⁰ RGPD, art. 6

¹⁸¹ RGPD, art. 4 (11), considérant 32

¹⁸² RGPD, considérant 42

¹⁸³ RGPD, art. 7 (3)

¹⁸⁴ RGPD, art. 21

en mesure de refuser ou de retirer son consentement sans subir de préjudice.¹⁸⁵ » De plus, le règlement ajoute que le consommateur est présumé ne pas avoir donné son consentement librement « si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.¹⁸⁶ »

Particularité européenne, le consommateur a le droit de refuser de faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage¹⁸⁷. Toutefois, une limitation importante de cette disposition tient en ce qu'elle ne s'applique que lorsque le traitement automatisé produit des effets juridiques concernant le consommateur ou l'affecte de manière significative de façon similaire¹⁸⁸.

5.2. États-Unis : un cadre minimaliste

Contrairement au cadre européen, le droit américain en matière de protection des renseignements personnels ne propose guère de mesures qui pourraient servir d'inspiration au Canada quant à l'encadrement de l'IA. En effet, le cadre juridique des États-Unis reste morcelé entre divers secteurs d'activité et juridictions, et les normes qu'il prévoit se montrent généralement plus timides qu'en Europe et au Canada.

Au niveau fédéral, quelques dispositions éparses pourraient trouver application dans le cadre de l'utilisation de l'IA par les entreprises. Aux termes du *Fair Credit Reporting Act*¹⁸⁹, une entreprise qui rassemble des renseignements sur un consommateur pour prendre une décision automatisée quant à son éligibilité à du crédit, un emploi, de l'assurance, un logement ou d'autres services similaires pourrait être considérée comme une « agence de crédit » et ainsi devoir respecter certaines obligations d'information¹⁹⁰. De plus, une entreprise qui n'informerait pas un consommateur qu'elle modifie les conditions de fourniture d'un service en fonction d'une décision prise par une IA pourrait contrevenir au *Federal Trade Commission Act*, qui interdit les pratiques commerciales fausses ou trompeuses¹⁹¹. Enfin, le *Civil Rights Act of 1964* et le *Equal Credit Opportunity Act* interdisent la discrimination sur la base de motifs tels que l'âge, le sexe ou l'origine ethnique – ainsi, un système d'IA ayant pour effet de discriminer selon ces motifs pourrait contrevenir à ces lois.

La juridiction étatique ayant fait l'objet de la plus grande attention au cours des dernières années est sans contredit la Californie, qui a adopté en 2018 le *California Consumer Privacy Act*¹⁹². Cette loi générale sur la protection des renseignements personnels garantit de nouveaux droits pour les consommateurs californiens, notamment le droit de connaître les renseignements personnels qu'une entreprise recueille à leur sujet et la manière dont ils sont

¹⁸⁵ RGPD, considérant 42

¹⁸⁶ RGPD, considérant 43

¹⁸⁷ RGPD, art. 22

¹⁸⁸ *Id.*

¹⁸⁹ 15 U.S.C. §§ 1681-1681x

¹⁹⁰ Andrew SMITH, *Using Artificial Intelligence and Algorithms*, FTC Bureau of Consumer Protection, 8 avril 2020, <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms>

¹⁹¹ 15 U.S.C. § 45(a)(1) (2012)

¹⁹² *California Consumer Protection Act*, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West) (ci-après « CCPA »)

utilisés et partagés¹⁹³; le droit de faire supprimer leurs renseignements personnels¹⁹⁴; le droit de refuser la vente de leurs renseignements personnels; et le droit à la non-discrimination dans le cadre de l'exercice de leurs droits reconnus par cette loi¹⁹⁵.

La loi californienne s'applique aux entreprises qui font affaire en Californie¹⁹⁶. Toutefois, contrairement aux lois canadiennes et européennes, la CCPA fixe des seuils qui déterminent les organisations qui y sont assujetties, de telle sorte que les plus petites entreprises pourront échapper à son application. Le champ d'application de la loi est ainsi restreint aux entreprises ayant un revenu annuel brut supérieur à 25 millions de dollars; ou qui traitent à des fins commerciales les renseignements personnels d'au moins 50 000 consommateurs, ménages ou appareils chaque année; ou encore qui tirent 50 % ou plus de leurs revenus annuels de la vente d'informations personnelles.

La CCPA prévoit notamment qu'une entreprise qui recueille des renseignements personnels doit obligatoirement informer les consommateurs des catégories de renseignements personnels qu'elle recueille et des fins pour lesquelles ils seront utilisés¹⁹⁷. Une part importante des droits conférés par la loi californienne concerne la « vente » de renseignements personnels des consommateurs à des tiers¹⁹⁸. Lorsqu'une entreprise souhaite vendre des renseignements personnels, elle doit donner aux consommateurs un droit de retrait, notamment en fournissant un lien vers une page web « *Do Not Sell My Personal Information* » où ils pourront exercer leur droit¹⁹⁹. En somme, la CCPA prévoit généralement un mécanisme de consentement négatif (*opt-out*) à la vente des informations personnelles pour les consommateurs, plutôt qu'une formule basée sur le consentement exprès²⁰⁰.

Disposition intéressante, la loi californienne prévoit que les consommateurs ne doivent pas faire l'objet de discrimination en raison de l'exercice de leurs droits²⁰¹. Cela implique notamment que des services ne doivent pas leur être refusés, qu'ils ne doivent pas être facturés à des prix ou à des taux différents pour des biens ou des services, ou qu'ils ne doivent pas obtenir un niveau ou une qualité de service différents. De même, on ne doit pas leur avoir suggéré qu'ils recevraient un prix ou un taux différent pour les biens ou les services. Face aux préjudices économiques que pourrait subir un consommateur qui refuse un traitement automatisé de ses données, une telle disposition pourrait inspirer le Canada.

¹⁹³ CCPA, section 1798.13

¹⁹⁴ CCPA, section 1798.105

¹⁹⁵ Voir : <https://oag.ca.gov/privacy/ccpa>

¹⁹⁶ CCPA, sections 1798.140 (c), (g)

¹⁹⁷ CCPA, section 1798.100 (b). Cette information doit être donnée avant ou lors de collecte de leurs données. Les entreprises ne peuvent pas collecter de renseignements personnels supplémentaires sans informer les consommateurs de la nature des informations qui seront collectées et le but de cette collecte.

¹⁹⁸ Aux termes du CCPA, la vente comprend « la location, la divulgation, la diffusion, la mise à disposition, le transfert ou la communication de toute autre manière d'informations personnelles à des fins financières ou autres ». La vente n'implique pas nécessairement un paiement à effectuer en échange d'informations personnelles.

¹⁹⁹ CCPA, sections 1798.130(a), 1798.135

²⁰⁰ CCPA, sections 1798.100(a)(b), 1798.105(b), 1798.110, 1798.115, 1798.120(b), 1798.130 et 1798.135

²⁰¹ CCPA, section 1798.125

En somme, la loi californienne reste limitée ne propose guère d'innovations permettant d'encadrer l'IA. D'emblée, cette loi n'adopte pas une véritable approche fondée sur les droits humains et considère implicitement la vie privée comme une commodité plutôt que comme un droit fondamental²⁰². Entre autres lacunes, elle n'impose pas l'élaboration d'une étude d'impact sur la vie privée aux entreprises et ne contient aucune disposition sur le droit d'une personne d'être informée de l'existence d'une prise de décision automatisée.

²⁰² Jeeyun Sophia BAIK, « Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA) », (2020) 52 *Telematics and Informatics* 101431

Conclusion et recommandations

Bien qu'il soit complexe d'en définir les pourtours et les ramifications exacts, il est indéniable que l'IA est désormais employée à grande échelle dans les rapports entre les commerçants et les consommateurs. L'IA, entendue dans son sens large, propulse une multitude de services chez les entreprises, permettant entre autres de personnaliser les services, de prédire les tendances, de donner accès à l'information, d'interagir avec les consommateurs ou encore de prendre des décisions sur eux.

Tous ces débouchés commerciaux de l'IA comportent des avantages pour les consommateurs, mais ils posent aussi des risques de protection de la vie privée, d'exclusion de groupes vulnérables, voire même d'exploitation économique des consommateurs. Loin d'être une technologie neutre et objective en toutes circonstances, l'IA peut reproduire des biais et renforcer des stéréotypes, faisant en sorte de discriminer illicitement des personnes en les excluant de services ou d'espaces commerciaux. Le déploiement commercial de l'IA peut également être source de préjudices économiques pour les consommateurs, qui pourraient faire l'objet de diverses techniques de persuasion invasives, de discrimination par les prix ou subir des comportements anticoncurrentiels. Ajoutant à la difficulté, les systèmes d'IA restent opaques, agissant souvent de manière autonome sans qu'on comprenne les rouages et les facteurs qui ont entraîné leurs décisions.

Dans ce contexte, l'emploi de l'IA par les commerçants pourrait leur procurer un avantage économique inédit, en accentuant significativement l'asymétrie d'information préexistante entre le consommateur et le commerçant. Traditionnellement, un commerçant peut user de son pouvoir économique et de sa connaissance approfondie de la marchandise qu'il vend et pour tirer un avantage du consommateur et pour imposer les modalités contractuelles d'une transaction. Désormais, l'IA lui permet également de connaître intimement les biais et les vulnérabilités de chacun de ses clients, et de s'en servir pour maximiser ses profits. En somme, laisser le développement de l'IA aux seules forces du marché menace d'éroder la sphère d'autonomie des consommateurs et leur capacité de faire des choix éclairés.

En réponse à ces enjeux, le droit canadien piétine par moments. Puisque les systèmes d'IA reposent sur la collecte et l'analyse des données massives dans un contexte commercial, les lois sur la protection des renseignements personnels constituent un instrument privilégié d'encadrement de l'IA. Cependant, elles manquent de mordant pour assurer une protection adéquate du public.

D'abord, on compte des lacunes dans les mécanismes d'information et de consentement des consommateurs. La loi ne prévoit pas le droit d'obtenir une explication quant à la façon dont les systèmes d'IA prennent des décisions sur les consommateurs. Une personne pourrait ainsi se voir refuser un service ou être exclue d'une plateforme sans qu'elle puisse connaître les raisons qui ont motivé cette décision. De plus, les consommateurs n'ont pas la faculté de demander qu'une telle décision puisse faire l'objet d'une révision humaine, de façon à ce que des décisions automatisées puissent être remises en question lorsqu'elles sont mal fondées. Le choix du consommateur peut également inclure la faculté, pour le consommateur, d'avoir son mot à dire quant aux critères qui déterminent certains choix qui sont faits à son égard, tels que la personnalisation; toutefois, encore là, le droit peine à proposer des solutions. Finalement, la

capacité de choisir implique aussi que le consommateur qui refuse le traitement par l'IA de ses renseignements personnels ne subisse pas de préjudice économique ou se voie refuser un service.

Au-delà du consentement et des droits individuels des consommateurs, l'IA soulève aussi la question de l'encadrement des utilisations que peuvent faire les entreprises des renseignements personnels. Ce domaine, qui reste encore balbutiant et exploratoire, mérite assurément qu'on propose des balises législatives plus précises. On sait qu'une entreprise effectuant un traitement de données qui aurait des effets discriminatoires au sens des chartes sur les droits et libertés serait illicite (section 4.3.2). Toutefois, l'IA peut emporter d'autres préjudices pour les consommateurs, notamment quant à leur exploitation économique, pour lesquels le droit se montre incertain. Afin qu'elle ait suffisamment de prise pour protéger le public, la loi doit mieux préciser les finalités interdites et les effets indésirables des systèmes d'IA.

Bien entendu, définir le champ de ce qui devrait être interdit ou non reste un exercice périlleux, particulièrement dans un contexte où l'on peine à comprendre l'IA et ses impacts. L'emploi de l'IA dans un contexte commercial reste un domaine parsemé d'opacité, autant quant aux technologies employées, aux intrants dans les systèmes, aux facteurs qu'ils prennent en compte, à leurs processus décisionnels et à leurs effets sur le public. Qu'il suffise de dire que certains usages de l'IA portant un préjudice économique aux consommateurs devraient clairement être interdits, notamment le recours à l'IA pour manipuler les consommateurs, pour identifier et exploiter leurs vulnérabilités, pour personnaliser les prix à leur insu ou pour limiter la libre-concurrence.

Pour poursuivre la recherche sur ces questions, les entreprises doivent être assujetties à des obligations de transparence élevées, permettant notamment aux chercheurs d'accéder aux algorithmes des systèmes d'IA pour en comprendre le fonctionnement. Rappelons par ailleurs que notre recherche s'est limitée à étudier les pratiques des entreprises en ligne; toutefois, l'usage de l'IA dans les espaces physiques, notamment le recours aux véhicules autonomes ou l'emploi de la reconnaissance faciale, posent encore là leur lot de difficultés d'encadrement.

De même, une mise en œuvre adéquate de la loi exige des pouvoirs et des ressources pour ce faire. Malheureusement, l'approche volontariste préconisée par les entreprises s'avère insuffisante pour garantir une protection des consommateurs; des mécanismes contraignants s'avèreront nécessaires pour évaluer les systèmes d'IA. De tels mécanismes pourraient inclure, par exemple, la tenue d'évaluation des facteurs relatifs à la vie privée avant leur déploiement, de même que des mécanismes permettant de surveiller leurs impacts après leur déploiement. Évidemment, les autorités chargées d'appliquer les lois sur la protection des renseignements personnels doivent disposer des pouvoirs nécessaires pour enquêter sur la conformité aux lois, pour émettre des ordonnances aux entreprises, de même que la capacité de sanctionner celles qui y contreviennent.

La présente recherche s'intéressait à l'IA dans une perspective de protection de la vie privée et reste incomplète pour traiter de l'enjeu, eu égard à l'ensemble de la protection du consommateur. Il ressort de notre étude que d'autres champs du droit devront aussi être mis à partie pour encadrer l'IA et protéger les consommateurs. Notre recherche permet toutefois de formuler des orientations que doit prendre la loi pour protéger adéquatement les consommateurs.

Dans ce contexte, nous émettons les recommandations suivantes :

Option consommateurs recommande aux gouvernements fédéral et provinciaux de modifier les lois sur la protection des renseignements personnels applicables aux entreprises de manière à y inclure des dispositions prévoyant :

- **le droit d’être informé d’une prise de décision automatisée et d’obtenir une explication sur cette prise de décision;**
- **le droit de demander une révision humaine d’une décision automatisée;**
- **l’interdiction de pénaliser financièrement ou d’exclure d’un service un consommateur qui a refusé ou s’est opposé au traitement automatique de ses renseignements personnels;**
- **le droit pour le consommateur, lorsque cela est possible, de choisir les facteurs qui entrent en compte dans la personnalisation des services effectuée par une IA;**
- **l’interdiction expresse des utilisations de renseignements personnels ayant pour effet, direct ou indirect, de causer une discrimination illicite ou une exploitation économique des consommateurs, notamment en prohibant le recours à l’IA visant :**
 - **à manipuler les consommateurs;**
 - **à identifier et exploiter leurs vulnérabilités;**
 - **à personnaliser les prix à leur insu;**
 - **ou à limiter la libre-concurrence;**
- **des obligations relatives à la tenue d’analyses de risque préalablement au déploiement de systèmes d’IA, par exemple via des évaluations des facteurs relatifs à la vie privée obligatoires;**
- **des obligations surveillance des systèmes d’IA après leur déploiement, par exemple via des études d’impact obligatoires;**
- **l’enchâssement du droit à la vie privée comme un droit ayant prépondérance sur les intérêts commerciaux des entreprises;**
- **l’accroissement substantiel des pouvoirs du Commissaire à la protection de la vie privée du Canada, y compris la mise en place d’un régime dissuasif de sanctions administratives pécuniaires et le pouvoir d’émettre des ordonnances contraignantes aux entreprises.**

Option consommateurs recommande également aux gouvernements de poursuivre la recherche sur l’emploi de l’IA dans un contexte commercial et ses impacts pour le public.