GUIDE DES BONNES PRATIQUES EN INTELLIGENCE ARTIFICIELLE :

SEPT PRINCIPES POUR UNE UTILISATION RESPONSABLE DES DONNÉES

Février 2023

Me Vincent Gautrais
Me Anne Tchiniaev
Me Émilie Guiraud

Chaire L.R. Wilson
DROIT DES TECHNOLOGIES DE L'INFORMATION ET DU COMMERCE ÉLECTRONIQUE
UNIVERSITÉ DE MONTRÉAL

CENTRE DE RECHERCHE EN DROIT PUBLIC

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

À propos des auteurs

Direction du projet :

- Me Vincent Gautrais est professeur titulaire à la Faculté de droit de l'Université de Montréal, chercheur au CRDP et à l'OBVIA, avocat et titulaire de la chaire L.R. Wilson en droit du commerce électronique. www.gautrais.com; vincent.gautrais@umontrea.ca

Rédaction :

- Me Anne Tchiniaev été auxiliaire de recherche au Laboratoire de cyberjustice de l'Université de Montréal. Elle est désormais Conseillère en politique législative à Environnement et Changement climatique Canada.
- Me Émilie Guiraud a été auxiliaire de recherche à l'OBVIA et a effectué son stage du Barreau du Québec sous la direction du professeur Vincent Gautrais. emilie.guiraud.1@ulaval.ca

Comité aviseur :

- Pr Karim Benyekhlef (Faculté de droit, Université de Montréal)
- Pre Céline Castets-Renard (Faculté de droit, section droit civil, Université d'Ottawa)
- Pr Pierre-Luc Déziel (Faculté de droit, Université Laval).

À propos des partenaires

OBVIA

L'Observatoire sur les impacts sociétaux de l'IA et du numérique (OBVIA) est un réseau de recherche ouvert qui fédère les expertises de plus de 260 chercheuses et chercheurs. Au moyen d'une interrogation critique, l'OBVIA a pour mission d'identifier les enjeux sociétaux de l'IA et du numérique et de contribuer à des solutions qui placent les êtres vivants et la biosphère au centre de leur cycle de développement et d'utilisation. La communauté de recherche de l'OBVIA, en collaboration avec la société civile, les acteurs publics, l'industrie et les développeurs, produit des connaissances ouvertes et soutient le renforcement des capabilités individuelles et collectives.

Chaire L.R. Wilson en droit du commerce électronique

Associée au Centre de recherche en droit public de la Faculté de droit de l'Université de Montréal, la Chaire L.R. Wilson en droit du commerce électronique s'intéresse depuis 2003 à l'étude des mutations du droit et des autres normativités encadrant les échanges numériques.

Centre de recherche en droit public (CDRP)

Le CRDP est le plus vieux centre de recherche en droit au Canada. Basé à la Faculté de droit de l'Université de Montréal, il est un regroupement stratégique pluri-universitaire (Université McGill – Université Laval) financé par les Fonds de recherche du Québec et dont les recherches s'articulent de façon pluridisciplinaire autour de la thématique « Justice et changements ».

TABLE DES MATIÈRES

MISE EN CONTEXTE DE LA PRÉSENTE « VERSION 0.2 »

Bonnes pratiques. L'intelligence artificielle (« IA ») est à la mode… Elle suscite passions tant sur ses possibilités que sur ses risques. Afin de compléter le silence parfois coupable parfois nécessaire du droit lié à ce domaine, celui-ci se limitant souvent à des intitulés généraux, il importe de tenter d'objectiver les manières de faire en proposant un guide de bonnes pratiques que les entreprises et organismes publics devraient suivre lorsqu'ils entendent mettre en place une utilisation algorithmique des données par un Système d'intelligence artificielle (« SIA »).

Inspirations. Évidemment, le premier regard fut dirigé vers les textes de lois. Cependant, les textes formels sont souvent assez peu spécifiques quant aux obligations à suivre. Aussi, le présent document s'est donc inspiré de plusieurs textes, de droit informel, volontaires, qui se sont peu à peu développés à travers la planète. Plus exactement, une dizaine de documents nous sont apparus particulièrement pertinents (voir les références à la page xx) parmi la presque centaine que nous avons pu consulter.

Attraits de la diligence. En dépit du caractère indicatif du présent document, il nous est seulement apparu que toute approche diligente de la part d'un SIA est assurément un moyen de développer tant sa conformité juridique que la confiance vis-à-vis des personnes concernées. De surcroît, il apparaît communément consacré qu'un opérateur diligent de SIA se doit d'élaborer au préalable des règles de bonnes pratiques quant à la manière de faire « parler ses données ». Cette documentation interne constitue en effet « le centre de gravité normatif » qu'un SIA met en place afin d'encadrer l'usage des algorithmes.

Pluralité des perspectives. Ce document entend aussi envisager la personne concernée de façon plurielle. En effet, selon la loi applicable, l'utilisation algorithmique des données va toucher la personne concernée sous différents statuts. Évidemment, c'est d'abord en tant qu'**individu** protégé par les lois sur la protection des données personnelles. Mais plusieurs de ces questions concerne également la **personne**, notamment au regard des libertés fondamentales défendues, par exemple, dans les chartes. On peut aussi ajouter la perspective du **consommateur** qui bénéficie de protection tant dans les lois sur la protection du consommateur que sur celles touchant à la concurrence. Ce texte se veut donc une approche transversale, globale, au-delà des cloisonnements législatifs.

Approche sociale. Également, il nous semble impérieux d'envisager l'encadrement des SIA sous le spectre d'une approche plus globale, plus sociale. Trop souvent, l'encadrement du numérique s'appuie sur les modalités de contrôle que les partenaires, dont les usagers, sont susceptibles d'avoir sur les données; sur leurs données. Avec l'intelligence artificielle, sa complexité inhérente et à certains égards son caractère quelque peu occulte, il est difficile de croire que l'on puisse autant individualiser les rapports ainsi créés. Ceux-ci doivent donc être considérés dans leur ensemble en vérifiant leur pertinence sociétale, leur justification sociale.

Œuvre évolutive. Le présent document est une version 0.2 (après une première version de 2021) qui a déjà intégré plusieurs changements en lien avec ce domaine en pleine évolution. En premier lieu, et surtout, il importait d'intégrer des modifications législatives qui sont apparues récemment tant en ce qui a trait à la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[1] (« L25 ») au Québec qu'au regard du projet de Loi C-27[2] au fédéral. En second lieu, nous avons tenté de mettre en application ce guide des bonnes pratiques avec un Modèle d'évaluation des facteurs relatifs à la circulation des données (V. Gautrais et N. Aubin – mai 2022) basé justement sur celles-ci. L'application de ces dernières nous a amené à les modifier, certains principes étant ainsi fusionnés, évitant par le fait même plusieurs répétitions.

Œuvre itérative. Justement, sur le plan pratique, le présent guide des bonnes pratiques vise à poser le doigt là où le curseur des obligations des opérateurs de SIA doit se poser. Au regard de la généralité tant des normes formelles qu'informelles, il y a donc une certaine subjectivité, une subjectivité certaine même, sur les mesures mises de l'avant dans le présent guide des bonnes pratiques. Aussi, fort de cela, il importe que ce guide, qui n'est qu'une version 0.2, puisse bénéficier des retours de la communauté. Des sollicitations ont déjà été entreprises et d'autres seront proposées afin de recevoir des commentaires de la part de personnes provenant tant des milieux universitaires, gouvernementaux que commerciaux, notamment technologiques. Pour ce faire, une itération sera favorisée tant au regard de questionnements généraux et ouverts que d'interrogations plus ciblées et dirigées. À cet égard, nous souhaitons chaleureusement remercier plusieurs juristes de la Commission d'accès à l'information (et tout particulièrement Me Noami Ayotte) pour leurs commentaires fort éclairants au présent document. Ceci étant dit, et si besoin était, cette interaction ne constitue pas approbation de leur part et ce document est une œuvre de doctrine visant à densifier les obligations des parties prenantes impliquées dans les SIA.

Œuvre collective. Ce document est le produit d'une recherche universitaire effectuée à plusieurs, sous le regard expert d'un comité scientifique issu de chercheurs appartenant à l'OBVIA (Pr. Karim Benyekhlef, Pre. Céline Castets-Renard, Pr. Pierre-Luc Déziel). Il a aussi été rendu possible grâce au concours de Me. Anne Tchiniaev qui a été directement impliquée dans la rédaction de la première version (2021). La deuxième version a quant à elle bénéficié du soutien d'Émilie Guiraud afin d'intégrer les modifications précitées. L'ensemble de la recherche a enfin été effectué sous la coordination de Guillaume Macaux.

Vincent Gautrais

Février 2023

1 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c 25

2 *Projet de Loi C-27 édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, Première session, quarante-quatrième législature, 70-71 Elizabeth II, 2021-2022, Chambre des communes du canada

INTRODUCTION

Ce document propose une liste de bonnes pratiques pour les entreprises et les organismes publics qui Ce document propose une liste de bonnes pratiques pour les entreprises et les organismes publics qui utilisent l'IA. Il est divisé en 7 sections représentant 7 principes relatifs à l'utilisation des données et à la protection des renseignements personnels dans un contexte d'IA. Chaque section débute avec un énoncé explicatif général du principe en question. Ensuite, les bonnes pratiques exposées dans chacune des sections sont suivies de sources législatives et documentaires. Évidemment, nous avons tenu compte des nouveaux changements introduits en 2021 **par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*** dont l'application s'échelonne jusqu'en septembre 2024. Dans ce document, **les obligations légales sont résumées à haut niveau et seuls les principaux articles de loi pertinents sont mentionnés**. Pour des informations plus détaillées, le lecteur peut se référer au site Web de la Commission d'accès à l'information. Sinon, et au regard de ce mélanges de références formelles et informelles, les sources sont listées en fonction de leur force contraignante.

Les premières sources sont en noir. Ce sont les sources législatives applicables en vigueur auxquelles il faut se conformer. Les lois applicables sont le *Code civil du Québec*[3] (« C.c.Q. »), la *Loi sur la protection des renseignements personnels dans le secteur privé*[4] (« Loi sur le secteur privé »), et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[5] (« Loi sur l'accès aux documents »)[6].

Les sources suivantes, en police bleu foncée, sont les sources législatives applicables qui ne sont pas en vigueur présentement. On parle ici de la *Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois*[7] (« projet de loi fédéral C-27 »).

Les dernières sources, en police bleu pâle, sont des documents provenant de différents pays énonçant une variété de bonnes pratiques, sans force contraignante. Tout de même, ces bonnes pratiques servent à favoriser la confiance des personnes concernées.

3 *Code civil du Québec*, RLRQ c CCQ-1991
4 *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1
5 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1
6 Pour diverses raisons (temps, spécificités, élaboration de textes en cours (comme le projet de loi 3), nous avons exclu, pour le moment, de considérer les lois propres au domaines de la santé).
7 PL C-27, *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, 1e sess, 44 lég, 2021-2022.

1 RESPONSABILITÉ

Que ce soit dans les lois ou les textes de nature plus informelle, on constate une hausse sensible des obligations des prestataires collectant, conservant, utilisant les données. Que ce doit en terme de documentation ou de ressources humaines, les parties prenantes doivent désormais prendre au sérieux la gestion des données.

1.1 Personne responsable

1.1.1 Obligations légales générales

La personne ayant **la plus haute autorité** au sein de l'organisme public ou de l'entreprise exerce la fonction de **responsable de la protection des renseignements personnels.** Le ou la responsable assure le respect et la mise en œuvre des obligations en la matière. Cette fonction peut être déléguée par écrit. Parmi les fonctions à assurer, cette personne doit établir les règles de gouvernance, formuler des avis et conseils, déclarer des incidents, répondre aux demandes des individus, etc.

- **art. 8[8] de la Loi sur l'accès aux documents;**
- **art. 3.1[9] de la Loi sur le secteur privé;**
- **art. 33 du projet de loi C-27 – Partie 3 Loi sur l'intelligence artificielle et les données**

Le titre et **les coordonnées** du ou de la responsable doivent être **publiées sur le site Internet de l'organisation** ou, à défaut d'avoir un site, rendus accessibles par tout autre moyen approprié. Ces coordonnées doivent permettre une communication effective entre le responsable et toute personne ayant un intérêt à se renseigner sur l'utilisation des renseignements personnels.

- **art. 17 et 65[10] de la Loi sur l'accès aux documents;**
- **art. 3.1[11] et 8[12] de la Loi sur le secteur privé;**

Pour aller plus loin :

- **Commission d'accès à l'information (CAI), Feuille de route des entreprises responsables.**
- **CAI, Section *Entreprises privées*.**
- **CAI, Liste des responsables d'application de la Loi sur l'accès (secteur public).**

8 Entrée en vigueur : 22 sept. 2022
9 Entrée en vigueur : 22 sept. 2022
10 Entrée en vigueur : 22 sept. 2023
11 Entrée en vigueur : 22 sept. 2022
12 Entrée en vigueur : 22 sept. 2023

1.1.2 Bonnes pratiques pour les SIA

Responsable en IA

À l'instar du responsable des renseignements personnels, il est loisible de désigner **aussi un responsable en IA**, que ce poste soit ou non la même personne. Celle-ci devra s'assurer de **connaître, comprendre et gérer les enjeux spécifiques à l'utilisation d'IA** et idéalement devra être **consultée dès le début d'un projet**.

En fonction des règles de gouvernance déjà existantes dans certaines organisations13, elle est ainsi chargée d'évaluer l'aspect éthique des projets et la conformité réglementaire de l'utilisation d'IA. Elle doit approuver l'utilisation d'IA pour un projet. Sa responsabilité s'étend aussi à l'IA fournie par des contractants externes.

Pour aller plus loin :

- **art. 63.6 de la Loi sur l'accès aux documents;**
- **art. 3.4 de la Loi sur le secteur privé;**
- art. 5 à 9 du projet de loi C-27 – Partie 3 Loi sur l'intelligence artificielle et les données;
- Information Commissioner's Office (Royaume-Uni) 2020;
- Monetary Authority of Singapore (Singapour) 2019, p.10;
- Commission européenne (Union européenne (« UE »)) 2018, p. 8 – 11, p.35-36;
- European Commission (EU) 2020, p.12
- International Technology Law Association (International) 2019, p.293, 302

Coordonnées

Rendez ses coordonnées accessibles pour que le public puisse la rejoindre facilement en cas de questions sur l'utilisation de l'IA par votre organisation. Il en va de la transparence de vos pratiques, qui sert à la confiance des citoyens.

Pour aller plus loin :

International Technology Law Association (International) 2019, p.293

13 À titre d'exemple, voir notamment la Loi sur la gouvernance et la gestion des ressources informationnnelles des organismes publics et des entreprises du Gouvernement, Chapitre G-1.03.

1.2 Gouvernance, expertise et documentation

1.2.1 Obligations légales générales

Des **règles, politiques et pratiques encadrant la gouvernance d'un organisme public ou d'une entreprise doivent être établies** à l'égard des renseignements personnels, principalement afin d'en assurer la protection. Ces politiques et pratiques doivent prévoir, entre autres, les **rôles et responsabilités des membres du personnel** tout au long du cycle de vie des renseignements ainsi qu'un processus de traitement des plaintes relatives à la protection de ceux-ci.

- **art. 63.3[14] de la Loi sur l'accès aux documents;**
- **art. 3.2[15] de la Loi sur le secteur privé;**
- **art. 62 du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs**

Les organismes publics doivent aussi constituer un **comité sur l'accès à l'information et la protection des renseignements personnels**. Ce comité devra, notamment, approuver les règles encadrant la gouvernance de l'organisme public à l'égard des renseignements personnels.

- **art. 8.1[16] et 63.3[17] de la Loi sur l'accès aux documents;**
- **art. 2 du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels**

Les organismes publics ont aussi plusieurs **obligations de documentation**. En effet, un organisme public doit inscrire dans un registre certaines communications de renseignements personnels ainsi qu'une entente de collecte de renseignements personnels. Un organisme public doit également établir et maintenir à jour un inventaire de ses fichiers de renseignements personnels.

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, chapitre G-1.03.

- **art. 67.3[18] et 76 de la Loi sur l'accès aux documents**

Pour aller plus loin :

- **CAI,** Politiques et pratiques de gouvernance**;**
- **CAI,** La tenue d'un registre des communications des renseignements personnels**;**

14 Entrée en vigueur : 22 sept. 2023
15 Entrée en vigueur : 22 sept. 2023
16 Entrée en vigueur : 22 sept. 2023
17 Entrée en vigueur : 22 sept. 2023
18 Entrée en vigueur : 22 sept. 2022

1.2.2 Bonnes pratiques pour les SIA

Stratégie SIA

Idéalement, vos politiques et pratiques de gouvernance en matière de protection des renseignements personnels devraient être **alignées à une stratégie de gouvernance et de gestion de risque de l'IA**. Une synergie entre ces deux outils de gouvernance facilitera vos opérations.

Expertise

Vous devez mettre en place des **équipes de qualité avec des expertises variées pour les projets nécessitant l'utilisation d'IA.** En ce sens, il est essentiel d'établir des descriptions de responsabilités en fonction des besoins de tels projets.

Pour aller plus loin :

- Gov. UK (Royaume-Uni) 2020;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.21-27

Formation

Dans un objectif d'apprentissage en continu, vous devez **mettre en place des formations concernant la conception, le fonctionnement et le déploiement d'un SIA.** Les équipes concernées devraient comprendre le rôle et le cycle de vie des renseignements personnels traités par un SIA afin d'en assurer la bonne gestion.

Pour aller plus loin :

- European Commission (EU) 2020, p.22;
- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.3.5.;
- International Technology Law Association (International) 2019, p.293

Stratégie SIA

Vos politiques, pratiques et mesures établies pour veiller à la protection des renseignements personnels devraient **être alignées à une stratégie de gouvernance et de gestion de risque d'IA.**

Pour aller plus loin :

- **art. 8 et 9 du projet de loi fédéral C-27 – Partie 3 Loi sur l'intelligence artificielle et les données;**
- Information Commissioner's Office (Royaume-Uni) 2020;
- International Technology Law Association (International) 2019, p.290, 293

Documentation

Documentez et tenez des registres détaillés de chaque projet afin de démontrer la conformité aux obligations légales concernant la protection des renseignements personnels.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Gov. UK (Royaume-Uni) 2020

Auditabilité Enfin, **consultez des experts** afin d'obtenir une évaluation du SIA. Vous pouvez également **développer des mécanismes afin d'assurer son auditabilité.** Ces mécanismes pourraient inclure la traçabilité du développement, l'accès aux dossiers, ou encore la documentation des sources des données d'entraînement. Lorsqu'un audit doit être fait par un tiers indépendant, vous devriez lui transmettre **toute information nécessaire** sur le fonctionnement du SIA.

Pour aller plus loin :

- Commission européenne (UE) 2018, p .36-37;
- European Commission (EU) 2020, p.21;
- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, § 6.3

1.3 Évaluation des facteurs relatifs à la circulation des données

1.3.1 Obligations légales générales

La loi prévoit plusieurs circonstances dans lesquelles une **évaluation des facteurs relatifs à la vie privée** doit être effectuée. C'est le cas, par exemple, pour tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

- **art. 63.5[19], 64[20], 67.2.1[21], 68[22] et 70.1[23] de la Loi sur l'accès aux documents;**
- **art. 3.3[24], 17[25] et 21[26] de la Loi sur le secteur privé;**

La **réalisation d'une EFVP doit être proportionnée** à la sensibilité des renseignements personnels, à la finalité de leur utilisation, ainsi qu'à leur quantité, répartition et support. Elle exige l'implication des personnes dédiées précitées.

- **art. 63.5[27] de la Loi sur l'accès aux documents;**
- **art. 3.3[28] de la Loi sur le secteur privé;**

Pour aller plus loin :

- **Commission d'accès à l'information, Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée.**

19 Entrée en vigueur : 22 sept. 2023
20 Entrée en vigueur : 22 sept. 2023
21 Entrée en vigueur : 22 sept. 2022
22 Entrée en vigueur : 22 sept. 2023
23 Entrée en vigueur : 22 sept. 2023
24 Entrée en vigueur : 22 sept. 2023
25 Entrée en vigueur : 22 sept. 2023
26 Entrée en vigueur : 22 sept. 2022
27 Entrée en vigueur : 22 sept. 2023
28 Entrée en vigueur : 22 sept. 2023

1.3.2. Bonnes pratiques pour les SIA

Conformité

Tout comme les évaluations des facteurs relatifs à la vie privée29, où elle est obligatoire dans certaines circonstances, **les évaluations des facteurs relatifs à la circulation des données** sont d'excellents moyens de démontrer la diligence employée pour gérer vos données pour l'IA. Vous gagneriez à les utiliser.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Commission européenne (UE) 2018, p.10 à 13;
- European Commission (EU) 2020, p.12;
- Gov. UK (Royaume-Uni) 2020

Gestion de risque

Vous devez procéder à une évaluation afin d'**identifier les risques au droit à la vie privée** ainsi que les manières d'adresser et d'atténuer chacun de ces risques.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Consultations

Vous devez consulter le ou la responsable en IA **dès le début de la conception du SIA.**

Il est aussi essentiel que votre organisation consulte, en parallèle, **toute organisation ayant contribué au SIA**, incluant les fournisseurs de modèles. Dans la mesure du possible, consultez **les individus concernés et les parties prenantes**, et incluez leurs points de vue dans les évaluations.

De plus, ne négligez pas le recours à des services juridiques afin d'obtenir des avis juridiques sur **les exigences légales** vous concernant.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.3.8.;
- Gov. UK (Royaume-Uni) 2020

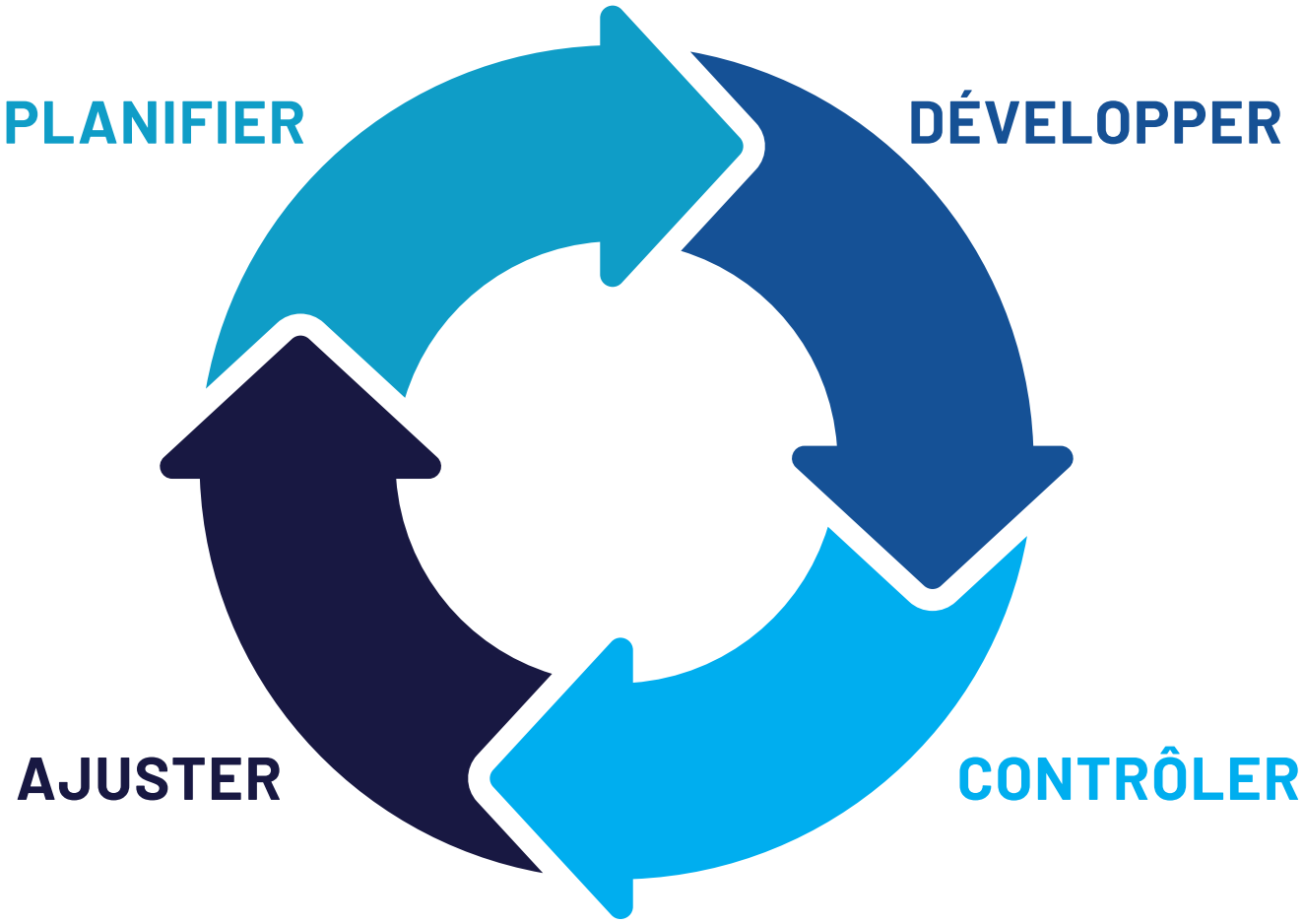
29 Commission d'accès à l'information, Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée, 10 mars 2021, en ligne : https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf

Réévaluation

En apprentissage automatique, une dérive de concept ou de modèle signifie que le SIA devient moins précis avec le temps. Ce genre de phénomène peut créer de nouveaux risques pour les utilisateurs. Il serait donc préférable pour vous de **réévaluer régulièrement un SIA** afin de pouvoir identifier quand le modèle a **besoin d'être réentraîné** et s'il a besoin de **nouvelles données**. Déterminer et documenter les seuils appropriés à atteindre avant de réévaluer un SIA.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- European Commission (EU) 2020, p.21-22



2 JUSTIFICATION SOCIALE

2.1 Objectif suffisamment important

2.1.1. Obligations légales générales

La circulation des renseignements personnels ne peut se faire sans tenir compte du contexte général dans lequel les renseignements sont collectés, conservés, communiqués, utilisés. Aussi, celui qui entend utiliser l'IA doit être en mesure de prouver que l'usage envisagé est **nécessaire et socialement acceptable**. Ainsi, en premier lieu, l'objectif doit être suffisamment important pour **justifier son utilisation.** En second lieu, il faut **évaluer les moyens mis en œuvre** afin qu'ils soient proportionnels à l'objectif précité. Finalement, il faut s'assurer que **l'utilisation et la conservation des renseignements personnels,** telles qu'envisagées, respectent la Loi.

Les renseignements personnels recueillis doivent être **nécessaires aux fins préalablement déterminées.**

L'intérêt et les fins relatifs au recueil de renseignements personnels doivent être choisis **avant la collecte**. Il faut éviter de changer d'intérêt ou de fin au cours du projet. De plus, la collecte de renseignements personnels doit s'effectuer par un moyen licite.

- **R. c. Oakes, 1986 CSC 46;**
- **art. 4[30], 5[31], 8, 29[32] et 90.1[33] de la Loi sur le secteur privé;**
- **art. 64[34], 65, 158[35] de la Loi sur l'accès;**
- **art. 37 du C.c.Q.;**
- **art. 12, 13 du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs**

Pour aller plus loin :

- **Commission d'accès à l'information, Vers la conformité à la Loi sur le privé ;**
- **Commission d'accès à l'information, Bonnes questions à se poser! ;**
- **Commission d'accès à l'information, Biométrie : principes à respecter et obligations légales des organisations**
- **Commission d'accès à l'information, Protection des renseignements personnels**

30 Entrée en vigueur : 22 sept. 2023
31 Entrée en vigueur : 22 sept. 2023
32 Entrée en vigueur : 22 sept. 2023
33 Entrée en vigueur : 22 sept. 2023
34 Entrée en vigueur : 22 sept. 2023
35 Entrée en vigueur : 22 sept. 2023

2.1.2. Bonnes pratiques pour les SIA

Justifications

Au-delà de la nécessité et de la détermination de la finalité, il importe de vous assurer que les avantages rendus possibles par le SIA seront suffisamment importants pour justifier une telle utilisation des données.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Phases

Il est essentiel pour vous de déterminer un intérêt et des justifications spécifiques à chaque phase du cycle de vie d'un SIA. La phase de développement et la phase de déploiement d'un SIA devraient être évaluées séparément, car ces phases ont des objectifs et risques différents.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Documentation

Pour démontrer l'intérêt sérieux et les fins déterminées de votre projet, ceux-ci devraient être documentés afin de rendre compte de votre conformité à l'obligation légale. Si cela est possible et approprié, vous pouvez publier sur votre site l'intérêt et les fins relatifs à vos projets.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

2.2 Proportionnalité

2.2.1 Obligations légales générales

Dans certaines situations, une **évaluation des facteurs relatifs à la vie privée** est obligatoire et ce, tant en ce qui concerne les organismes publics que les établissements du secteur privé. Cette évaluation permet de s'assurer notamment que la **solution proposée soit proportionnée** à la sensibilité, la finalité de son utilisation et la quantité des renseignements ainsi qu'à leur répartition et leur support.

- **art. 63.5** [36] **de la Loi sur l'accès aux documents;**
- **art. 3.3** [37] **de la Loi sur le secteur privé;**

Pour aller plus loin :

- **Commission d'accès à l'information, La collecte de renseignements personnels;**
- **Commission d'accès à l'information, Vers la conformité à la Loi sur le privé**
- **Commission d'accès à l'information, Protection des renseignements personnels**
- **Commission d'accès à l'information, Évaluation des facteurs relatifs à la vie privée**
- **Commission d'accès à l'information, Guide d'accompagnement, Réaliser une évaluation des facteurs relatifs à la vie privée**

36 Entrée en vigueur : 22 sept. 2023
37 Entrée en vigueur : 22 sept. 2023

2.2.2 Bonnes pratiques pour les SIA

Évaluation de facteurs relatifs à la circulation des données

Que ce soit dans le secteur privé ou le secteur public, il essentiel pour vous de déterminer si les risques et les bénéfices de l'utilisation d'un SIA sont justifiées socialement. Pour ce faire, et selon les critères développés par la jurisprudence, il importe

- De vérifier un lien rationnel entre les objectifs et la solution proposée;
- De s'assurer que l'atteinte est minimale;
- Que les avantages surpassent les inconvénients.

Cette analyse peut notamment s'effectuer en comparantles résultats des décisions prises par des humains et les décisions automatisées.

Si vous procédez à une évaluation de facteurs relatifs à la circulation des données, cela représente un bon moyen de démontrer qu'il y a une justification sociale pour l'utilisation d'IA et qu'il n'y a pas de moyens moins intrusifs de parvenir aux fins déterminées que d'utiliser un SIA.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020
- **Commission d'accès à l'information, Guide d'accompagnement, Réaliser une évaluation des facteurs relatifs à la vie privée**

Minimisation des données

La minimisation des données s'inscrit dans ce même objectif. Vous pouvez identifier la quantité minimale de renseignements personnels nécessaires aux fins déterminées.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Commission européenne (UE) 2018, p.12;
- European Commission (EU) 2020, p.13;
- Gov. UK (Royaume-Uni) 2020

PHASE D'ENTRAÎNEMENT

Quelques techniques informatiques de minimisation des données

En apprentissage automatique, l'algorithme d'apprentissage est appliqué à une base de données avec des paramètres de données (élément de donnée qui est mesurable, c'est-à-dire nom, âge, genre, etc.). Plusieurs méthodes informatiques permettent de sélectionner les paramètres d'un modèle, et ainsi de les réduire aux paramètres nécessaires aux fins déterminées.

Perturbation, données synthétiques, confidentialité différentielle, apprentissage fédéré.

- Information Commissioner's Office (Royaume-Uni) 2020

2.3 Utilisation et conservation

2.3.1. Obligations légales générales

Plus souvent qu'autrement, un renseignement personnel doit être utilisé **conformément aux fins pour lesquelles il a été recueilli**. Il y sera fait exception si la personne concernée **consent à une utilisation pour une autre fin**. Toutefois, un renseignement personnel peut être utilisé à d'autres fins **sans le consentement** de la personne, par exemple, lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli ou quand le renseignement est anonymisé (et non simplement dépersonnalisé). Dans ce cas, il convient de s'assurer que la nouvelle fin a un lien pertinent et direct avec les fins pour lesquelles le renseignement a été recueilli.

- **art. 12[38], 90.1[39] de la Loi sur le secteur privé;**
- **art. 65.1[40], 158[41] de la Loi sur l'accès aux documents;**
- **art. 37 du C.c.Q.;**
- **art. 12 et 14 du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs**

À moins qu'un délai de conservation ne soit prévu par la loi, un renseignement personnel doit être **détruit ou anonymisé** lorsque les fins pour lesquelles il a été recueilli ou utilisé sont accomplies. À ce titre, il faut déterminer les périodes de conservation nécessaires ou prévues par la loi, et les **communiquer aux personnes concernées.**

- **art. 73[42], 158[43] et 159[44] de la Loi sur l'accès aux documents;**
- **art. 11[45], 23[46], 90.1[47] et 91[48] de la Loi sur le secteur privé;**

Pour aller plus loin :

- **Commission d'accès à l'information, Protection des renseignements personnels;**
- **Commission d'accès à l'information, Vers la conformité à la Loi sur le privé**
- **Commission d'accès à l'information, Consentement**
- **Commission d'accès à l'information, Communication de renseignements personnels sans le consentement**
- **Commission d'accès à l'information, Anonymisation**

38 Entrée en vigueur : 22 sept. 2023
39 Entrée en vigueur : 22 sept. 2023
40 Entrée en vigueur : 22 sept. 2023
41 Entrée en vigueur : 22 sept. 2023
42 Entrée en vigueur : 22 sept. 2023
43 Entrée en vigueur : 22 sept. 2023
44 Entrée en vigueur : 22 sept. 2023
45 Entrée en vigueur : 22 sept. 2023
46 Entrée en vigueur : 22 sept. 2023
47 Entrée en vigueur : 22 sept. 2023
48 Entrée en vigueur : 22 sept. 2023

2.3.2. Bonnes pratiques pour les SIA

Précision de SIA

Afin de vous assurer qu'un renseignement personnel est bel et bien utilisé aux fins prévues, il faut s'assurer que le SIA performe de la manière attendue. Le SIA doit être suffisamment précis, c'est-à-dire, que les résultats du SIA doivent correspondre aux étiquettes définies à l'aide des données de test. Il existe des mesures de précision statistique permettant de mesurer la performance des SIA. Par exemple, des mesures de précision et de rappel.

Afin de vous éviter des malentendus quant aux attentes relatives à la performance du SIA, il est souhaitable que vous étiquetiez clairement les données qui ne prétendent pas être factuelles, mais qui sont plutôt des inférences ou prédictions. Cela vous permettra de mesurer la performance du SIA de manière plus exacte.

Il vous est recommandé d'élaborer une procédure d'évaluation et de surveillance des données dès le départ et tout au long du cycle de vie du SIA afin de vous assurer non seulement de l'intégrité des données mais également que vos résultats ne soient injustement influencés.

D'autre part, il est pertinent pour vous d'identifier la manière de mesurer la performance du SIA et d'évaluer les conséquences possibles en cas de performance imprécise.

Pour atteindre ces objectifs, il vous est possible d'assurer une formation adéquate sur les exigences et les mesures de précision statistique aux membres de votre personnel responsables du projet. Dans le même sens, vous pouvez adopter une terminologie commune afin que les membres de votre personnel puissent l'utiliser lors de discussions concernant les mesures de performance de précision de SIA.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- University College London (Royaume-Uni) 2019;
- European Commission (EU) 2020, p.9-12

Fins compatibles

Une fin compatible pour des données d'entraînement pourrait être la nécessité de réentraîner un modèle de SIA. Cependant, ces données ne devraient être conservées que pour le temps nécessaire au réentraînement.

Pour aller plus loin :

- Gov. UK (Royaume-Uni) 2020

Conservation et anonymisation

Lorsqu'un renseignement personnel doit être anonymisé, vous pourriez avoir à démontrer qu'il a été désidentifié au plus grand degré possible. Pour cela, vous pouvez faire un test d'intrusion afin d'évaluer le risque de réidentification.

Pour aller plus loin :

- **art. 73[49] de la Loi sur l'accès aux documents;**
- **art. 23[50] de la Loi sur le secteur privé;**
- Information Commissioner's Office (Royaume-Uni) 2020;

Anonymisation : « Pour l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne. » (**art.23 de la Loi sur le secteur privé)**

Test d'intrusion : « Test visant à reproduire de manière contrôlée les conditions réelles d'une attaque sur un réseau ou un système d'information afin d'identifier les failles de sécurité et d'évaluer leur exploitabilité en vue de les corriger. » (Office québécois de la langue française, 2020)

- Gov. UK (Royaume-Uni) 2020

3 TRANSPARENCE

3.1 Information générale

3.3.1 Obligations légales générales

Les politiques et pratiques établies et mises en œuvre afin d'encadrer la gouvernance des renseignements personnels et de leur protection doivent être **publiées.**

Lorsqu'une personne recueille des renseignements personnels par un moyen technologique, elle doit **publier sur le site internet, ou diffuser** par tout moyen propre à atteindre les personnes concernées, **une politique de confidentialité** et l'avis dont toute modification à cette politique doit faire l'objet. Si ces renseignements personnels sont utilisés afin qu'une **décision fondée exclusivement sur un traitement automatisé soit rendue**, la personne concernée devrait être informée, au plus tard, au moment où elle est informée de cette décision.

- **art. 63.3[49], 63.4[50], 65.2[51] de la Loi sur l'accès aux documents;**
- **art. 3.2[52], 8.2 [53] et 12.1[54] de la Loi sur le secteur privé;**

La politique de confidentialité doit être rédigée en **termes simples et clairs.**

- **art. 63.4[55] de la Loi sur l'accès aux documents;**
- **art. 8.2[56] de la Loi sur le secteur privé**

Pour aller plus loin :

- **Commission d'accès à l'information, Espace évolutif – Modernisation des lois**
- **Commission d'accès à l'information, Transparence**
- **Commission d'accès à l'information, Politiques et pratiques de gouvernance**
- **Commission d'accès à l'information, Politique de confidentialité**

49 Entrée en vigueur : 22 sept. 2023
50 Entrée en vigueur : 22 sept. 2023
51 Entrée en vigueur : 22 sept. 2023
52 Entrée en vigueur : 22 sept. 2023
53 Entrée en vigueur : 22 sept. 2023
54 Entrée en vigueur : 22 sept. 2023
55 Entrée en vigueur : 22 sept. 2023
56 Entrée en vigueur : 22 sept. 2023

3.1.2 Bonnes pratiques pour les SIA

Information générale

Nous vous encourageons à faire des publications contenant de l'information générale sur le SIA. Cette information pourrait inclure une définition de l'IA, comment elle est utilisée afin de rendre des décisions, ses fonctions, quels sont les bénéfices et les risques de l'utilisation du SIA, et comment les risques sont atténués. Elle pourrait aussi inclure la raison pour laquelle un SIA est utilisé et comment le SIA est susceptible de causer un dommage aux personnes concernées.

Pour cela, il convient de vous assurer que les personnes concernées savent quand leurs renseignements personnels sont traités par un SIA à l'aide d'une communication générale et compréhensive. Il est alors essentiel pour vous d'inclure une explication suffisante des résultats communs des décisions.

Pour aller plus loin :

- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.15, 54, 57, 66;
- Monetary Authority of Singapore (Singapour) 2019, p.12-13
- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.2

Recours

Les utilisateurs du SIA ou personnes concernées par les décisions émises par votre SIA doivent avoir un recours en cas de manque de transparence ou de compréhension de votre organisme quant à votre utilisation de l'IA.

Pour aller plus loin :

- International Technology Law Association (International) 2019, p.294-295

3.2 Accès aux renseignements

3.2.1 Obligations légales générales

Lorsqu'une entreprise détient un renseignement personnel sur une personne, il doit lui en **confirmer l'existence et lui donner en donner l'accès**, sur demande de la personne concernée.

Lorsqu'il est question d'un renseignement personnel informatisé, il doit être communiqué sous la forme d'une **transcription écrite et intelligible**. Il doit aussi être communiqué dans un format technologique structuré et couramment utilisé, à moins que cela ne soulève des difficultés pratiques sérieuses.

- **art. 8[57], 16, 19[58], 27[59], 29[60], 32 à 34[61] et 90.1[62] de la Loi sur le secteur privé;**
- **art. 9, 10, 16, 17, 43[63], 83, 84[64], 85 et 158[65] de la Loi sur l'accès aux documents;**
- **art. 38 et 39 du C.c.Q.;**
- **art. 63 du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs**

Pour aller plus loin :

- **Commission d'accès à l'information, Accès aux documents**
- **Commission d'accès à l'information, Vers la conformité à la Loi sur le privé**

3.2.2 Bonnes pratiques pour les SIA

Accès au profil

Un des accès utiles pour votre organisme serait de permettre aux personnes concernées de visiter leur profil et les informations les concernant, incluant les détails des informations et les sources utilisées pour créer le profil.

Pour aller plus loin :

- Commission européenne (UE) 2018, p.18-19

57 Entrée en vigueur : 22 sept. 2023
58 Entrée en vigueur : 22 sept. 2023
59 Entrée en vigueur : 22 sept. 2023 et 22 sept. 2024
60 Entrée en vigueur : 22 sept. 2023
61 Entrée en vigueur : 22 sept. 2023
62 Entrée en vigueur : 22 sept. 2023
63 Entrée en vigueur : 22 sept. 2022
64 Entrée en vigueur : 22 sept. 2024
65 Entrée en vigueur : 22 sept. 2023

3.3 Usage de certaines technologies

3.3.1 Obligations légales générales

Les personnes concernées doivent être **informées de l'utilisation de technologie** comprenant des fonctions permettant de les **identifier, localiser ou d'effectuer un profilage de celle-ci**, avant la collecte de leurs renseignements. Elles devraient être désactivées par défaut.

- **art. 65.0.1[66] de la Loi sur l'accès aux documents ;**
- **art. 8.1 de la Loi sur le secteur privé[67]**

Les personnes concernées doivent être **informées lorsqu'une décision fondée exclusivement sur un traitement automatisé est prise**, ou avant qu'elle ne soit prise.

- **art. 65.2[68] de la Loi sur l'accès aux documents;**
- **art. 12.1[69] et 90.1[70] de la Loi sur le secteur privé;**
- **art. 62 et 63(3) du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs**

Pour aller plus loin :

- **Commission d'accès à l'information, Vers la conformité à la Loi sur le privé**
- **Commission d'accès à l'information, Technologie d'identification, de localisation ou de profilage**

3.3.2 Bonnes pratiques pour les SIA

Décision fondée exclusivement sur un traitement automatisé

Dans un objectif de transparence, il est important pour votre organisation de publier des avis informant de façon claire les individus qu'une décision est fondée exclusivement sur un traitement automatisé.

Pour aller plus loin :

- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.2.1., 6.2.2.

66 Entrée en vigueur : 22 sept. 2023
67 Entrée en vigueur : 22 sept. 2023
68 Entrée en vigueur : 22 sept. 2023
69 Entrée en vigueur : 22 sept. 2023
70 Entrée en vigueur : 22 sept. 2023

4 SÉCURITÉ

4.1 Mesures de sécurité adaptées

4.1.1 Obligations légales générales

L'entreprise ou l'organisme doit prendre des **mesures de sécurité adaptées** aux circonstances (sensibilité, quantité, risques, etc.) et besoins de chaque projet afin d'assurer la protection des renseignements personnels.

- **art. 10, 90.171 et 9172 de la Loi sur le secteur privé;**
- **art. 63.1 et 15973 de la Loi sur l'accès aux documents;**
- **art. 7 du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels**
- **Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, chapitre G-1.03.**
- **art. 57 du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs;**

Parmi les mesures qui peuvent être prises pour mitiger les risques, l'entreprise ou l'organisme doit procéder à une **évaluation des facteurs relatifs à la vie privée** lorsqu'il y a une volonté d'acquérir, de développer et de refondre un système d'information ou de prestation électronique de services impliquant, par exemple, la collecte ou la conservation de renseignements personnels.

- **art. 3.3[74] de la Loi sur le secteur privé;**
- **art. 63.5[75] de la Loi sur l'accès aux documents;**

Si un **incident de confidentialité impliquant un renseignement personnel se produit**, il faut prendre des mesures raisonnables pour diminuer les risques de préjudice et pour éviter qu'un incident de la même nature se répète. Si l'incident présente un risque de préjudice sérieux, **toute personne dont un renseignement personnel est concerné par l'incident doit être avisée tout comme la Commission d'accès à l'information**.

- **art. 3.5 à 3.7[76], 90.1[77] et 91[78] de la Loi sur le secteur privé;**
- **art. 63.8 à 63.10[79] et 158[80] de la Loi sur l'accès aux documents;**

71 Entrée en vigueur : 22 sept. 2023
72 Entrée en vigueur : 22 sept. 2023
73 Entrée en vigueur : 22 sept. 2023
74 Entrée en vigueur : 22 sept. 2023
75 Entrée en vigueur : 22 sept. 2023
76 Entrée en vigueur : 22 sept. 2022
77 Entrée en vigueur : 22 sept. 2023
78 Entrée en vigueur : 22 sept. 2023
79 Entrée en vigueur : 22 sept. 2022
80 Entrée en vigueur : 22 sept. 2023

L'entreprise ou l'organisme doit tenir un **registre des incidents de confidentialité**.

- **art. 3.8[81] de la Loi sur le secteur privé;**
- **art. 63.11[82] de la Loi sur l'accès aux documents;**

Pour aller plus loin :

- **Commission d'accès à l'information, Incident de sécurité impliquant des renseignements personnels**
- **Commission d'accès à l'information, Évaluation des facteurs relatifs à la vie privée**
- **Commission d'accès à l'information, Guide d'accompagnement, Réaliser une évaluation des facteurs relatifs à la vie privée**

4.1.2 Bonnes pratiques pour les SIA

Mesures techniques

Votre entreprise ou organisme devrait prendre des mesures de sécurité techniques et managariales afin de réduire des risques à la sécurité des renseignements personnels traités par un SIA. Si cela s'avère approprié, il vous faudrait obtenir une certification de cybersécurité conforme aux standards de l'industrie.

Pour aller plus loin :

- University College London (Royaume-Uni) 2019;
- European Commission (EU) 2020, p.9-10;
- Information Commissioner's Office (Royaume-Uni) 2020;
- International Technology Law Association (International) 2019, p.298-299

Évaluation de facteurs relatifs à la circulation des données

Il serait pertinent pour vous d'effectuer une évaluation de facteurs relatifs à l'usage des données afin que vous soyez en mesure d'établir le niveau de mesures de sécurité nécessaires en proportion aux risques posés par l'utilisation du SIA. Pour cela, prenez en compte la sensibilité, la finalité, la quantité, la répartition et le support des renseignements personnels. Vous pouvez également évaluer les risques associés aux codes source internes et externes. Les évaluations sont un bon moyen de rendre compte des mesures de sécurités établies.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- European Commission (EU) 2020, p.12-13;
- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.3.7

81 Entrée en vigueur : 22 sept. 2022
82 Entrée en vigueur : 22 sept. 2022

Facteurs en lien avec les dommages

Vous pouvez identifier les préjudices potentiels causés par un défaut ou une attaque à un modèle d'IA. Par exemple, il pourrait s'agir d'évaluer l'impact d'un mauvais résultat émis par le SIA ou de l'indisponibilité soudaine du service.

Pour aller plus loin :

- University College London (Royaume-Uni) 2019

Facteurs de risques

Idéalement, vous devez réévaluer régulièrement le risque que des renseignements personnels soient inférés d'un modèle selon les derniers développements en informatique. De plus, il vous est conseillé d'évaluer la sécurité et la résilience d'un SIA en cas de cyberattaques. Cela vous permettra de savoir comment il performe dans le pire scénario.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- University College London (Royaume-Uni) 2019;
- European Commission (EU) 2020, p.9-10

Catégorisation des risques

Vous pouvez identifier les types de vulnérabilités auxquelles un SIA est exposé. Par exemple, la pollution de données, l'infrastructure physique du système ou les cyberattaques.

Pour aller plus loin :

- University College London (Royaume-Uni) 2019;
- European Commission (EU) 2020, p.9-10

Validation

Vous pouvez déterminer une manière de valider la performance d'un modèle lorsque de nouvelles données sont ajoutées. De cette façon, vous pourrez surveiller et vérifier si un SIA rencontre ses objectifs.

Pour aller plus loin :

- Gov. UK (Royaume-Uni) 2020;
- European Commission (EU) 2020, p.11;
- University College London (Royaume-Uni) 2019

Reproductibilité

Un modèle de SIA est reproductible lorsqu'il agit de la même façon quand il est reproduit dans les mêmes conditions. Établissez des méthodes d'évaluation pour vérifier si un modèle est fiable et reproductible. Documentez ces méthodes afin de démontrer que le modèle a été conçu de manière à assumer la reproductibilité.

Pour aller plus loin :

- Gov. UK (Royaume-Uni) 2020;
- European Commission (EU) 2020, p.11;
- University College London (Royaume-Uni) 2019

Fournisseurs externes

Prévoyez une politique d'approvisionnement d'IA ayant un niveau suffisant de partage d'information afin de permettre des évaluations complètes. Vous pouvez possiblement la joindre au fournisseur du modèle de SIA afin de vous permettre d'effectuer une évaluation ensemble.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Mises à jour

Il serait pertinent pour votre organisation de déterminer la durée entre les mises à jour des paramètres de sécurité selon les limites et besoins de votre SIA. Vous pourrez ensuite offrir cette information aux utilisateurs.

Pour aller plus loin :

- European Commission (EU) 2020, p.9

Mesures organisationnelles

Vos mesures de sécurité organisationnelles devraient inclure, notamment, des formations de qualité sur les risques d'incidents de sécurité aux renseignements personnels traités par un SIA.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Documentation

Vous avez tout intérêt à documenter les mesures de sécurité que vous avez établies.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- University College London (Royaume-Uni) 2019

4.2 Données d'entraînement

4.2.1 Bonnes pratiques pour les SIA

Registre

Tenez un registre et documentez les mouvements et le stockage des données. Un registre bien organisé peut vous aider à déterminer quelles mesures de sécurité sont appropriées, et faciliter le déroulement de vos audits et autres vérifications. Vous devrez détruire la documentation contenant des données à caractère personnel dès que les fins auxquelles les renseignements ont été utilisés sont accomplies.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Dépersonnalisation

Dépendamment du niveau de risque et de sévérité de préjudice potentiel, appliquez des techniques de dépersonnalisation aux données d'entraînement avant qu'elles ne soient incorporées au modèle ou partagées autrement.

Pour aller plus loin :

- **art. 2 e) / 20 du projet de loi fédéral C-27;**
- Information Commissioner's Office (Royaume-Uni) 2020

Codes *open source*

L'utilisation de codes standards d'apprentissage automatiques *open source* provenant de parties tierces peut créer des risques additionnels. Il pourrait être nécessaire d'adapter les logiciels et le matériel informatique à ces risques additionnels.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Infrastructure informatique

Afin d'atténuer les risques, vous pouvez prévoir une ligne de conduite sécuritaire dès la conception qui sépare l'environnement du développement du modèle d'IA du reste de l'infrastructure informatique. Des « machines virtuelles » ou « conteneurs », émulations du système informatique isolées du reste du système, peuvent être configurés spécifiquement pour les tâches d'apprentissage automatique.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Déploiement

Les données de sortie du modèle peuvent révéler certains éléments des renseignements personnels ayant été utilisés pour l'entraînement du modèle. Il vous est possible d'entraîner un modèle en utilisant un langage de programmation et des cadres informatiques adaptés au développement, puis de convertir le modèle dans un format plus sécuritaire pour la phase de déploiement.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

4.3 Cyberattaques

4.3.1 Bonnes pratiques pour les SIA

Cyberattaques

Identifiez les types de cyberattaque possibles, et celles auxquelles le SIA est le plus vulnérable. Certaines méthodes utilisées pour augmenter l'explicabilité d'un modèle peuvent le rendre plus sujet à des risques d'attaques.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- European Commission (EU) 2020, p.9

Attaque de boîte noire

Dans une attaque de boîte noire, l'attaquant n'a pas accès aux paramètres du modèle. (Adversarial Attacks and Defences for Convolutional Neural Networks, 2018)

Surveiller les requêtes des utilisateurs de l'interface de programmation afin de détecter toute utilisation suspecte. Prévoir une procédure d'enquête et de suspension immédiate du compte d'utilisateur si une attaque est suspectée.

Attaque de boîte blanche

Dans une attaque de boîte blanche, l'attaquant a accès aux paramètres du modèle. (Adversarial Attacks and Defences for Convolutional Neural Networks, 2018)

Une interface de programmation peut réduire les risques d'attaques de boîte blanche puisqu'elle permet de ne pas donner d'accès direct au modèle.

Il y a plus de risques d'attaques lorsque qu'un modèle est fourni par un tiers dans sa totalité, car le fournisseur aura plus de difficulté à surveiller le modèle, et donc à prévenir les attaques.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Surapprentissage

Il y a du surapprentissage lorsqu'un modèle se concentre trop sur des détails des données d'entraînement et mémorise plus les exemples particuliers que le motif général. Le surapprentissage rend un modèle d'apprentissage automatique plus vulnérable aux attaques par inversion de modèle et par inférence d'appartenance. Évitez le surapprentissage afin d'atténuer le risque d'attaques aux renseignements personnels. Ceci vous permettra d'assurer la qualité des inférences si de nouveaux exemples sont ajoutés au modèle.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Plan de contingence

Vous pouvez prévoir une procédure d'urgence et une solution de repli en cas de cyberattaque. Prévoyez également des procédures de gouvernance en cas d'urgence ou d'échec du système.

Pour aller plus loin :

- University College London (Royaume-Uni) 2019;
- European Commission (EU) 2020, p.9;
- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.3.6

5 EXPLICABILITÉ

5.1 Obligations légales générales

Lorsqu'une entreprise ou un organisme met en place un **système de décisions automatisées**, des explications suffisantes sont offertesafin de vérifier l'absence de discrimination ou toute autre vulnérabilité dans le processus décisionnel.

Un projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels doit permettre que ces derniers, lorsqu'ils sont informatisés, soient **communiqués à la personne concernée dans un format technologique structuré et couramment utilisé**.

- **art. 12.1[83], 90.1[84] de la Loi sur le secteur privé;**
- **art. 65.2[85] de la Loi sur l'accès aux documents;**
- **art. 62 et 63 du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs**

Toute communication doit s'effectuer en des **termes simples et clairs**. C'est le cas notamment du contenu des politiques, lorsqu'un consentement est demandé ou bien encore lorsqu'un organisme public ou une entreprise recueille un renseignement personnel par un moyen technologique.

Également, lorsqu'une personne fait une demande d'accès, le renseignement personnel informatisé la concernant doit être communiqué sous la forme d'une **transcription écrite et intelligible**. Il doit aussi être communiqué dans un **format technologique structuré et couramment utilisé**, à moins que cela ne soulève de difficultés pratiques sérieuses. Les raisons et principaux facteurs ayant menés à la décision doivent être transmis à la personne concernée.

- **art. 10 al. 3, 53.1[86], 63.4[87], 65.2 et 84[88] de la Loi sur l'accès des documents;**
- **art. 3.2[89], 8[90], 8.2[91], 12.1, 14[92] et 27[93] de la Loi sur le secteur privé;**

art. 66 du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs

Pour aller plus loin :

- **Commission d'accès à l'information, Services et formulaires**
- **Commission d'accès à l'information, Politique de confidentialité**
- **Commission d'accès à l'information, Transparence**
- **Commission d'accès à l'information, Consentement**

83 Entrée en vigueur : 22 sept. 2023
84 Entrée en vigueur : 22 sept. 2023
85 Entrée en vigueur : 22 sept. 2023
86 Entrée en vigueur : 22 sept. 2023
87 Entrée en vigueur : 22 sept. 2023
88 Entrée en vigueur : 22 sept. 2024
89 Entrée en vigueur : 22 sept. 2023
90 Entrée en vigueur : 22 sept. 2023
91 Entrée en vigueur : 22 sept. 2023
92 Entrée en vigueur : 22 sept. 2023
93 Entrée en vigueur : 22 sept. 2023 et 22 sept. 2024

5.2 Bonnes pratiques pour les SIA

Explicabilité

Vos raisons, paramètres et facteurs communiqués à la personne concernée devraient inclure des informations permettant de comprendre la logique sous-jacente aux raisons derrière la décision d'un SIA, et d'avoir l'information nécessaire afin d'avoir la capacité de décider si elle souhaite contester une décision.

> *« L'explicabilité est une obligation pour les organisations qui utilisent l'IA dans les processus de prise de décision visant à fournir des informations précises dans des termes compréhensibles par l'homme, expliquant comment une décision ou un résultat a été atteint par un système d'IA. » (International Technology Law Association (International) 2019)*

En ce sens, il vous faudrait inclure les catégories de données utilisées et le raisonnement derrière leur utilisation, afin de comprendre comment un profil est établi et utilisé, et pourquoi le profil est pertinent pour le processus décisionnel. Vous devez communiquer les paramètres et facteurs de manière significative, simple et claire.

Pour aller plus loin :

- **art. 11 du projet de loi fédéral C-27 – Partie 3 Loi sur l'intelligence artificielle et les données;**
- Information Commissioner's Office (Royaume-Uni) 2020;
- Monetary Authority of Singapore (Singapour) 2019, p.12;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.15, 44-45;
- European Commission (EU) 2020, p.14-15;
- Commission européenne (UE) 2018, p.35;
- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.2.3.

Communication

Vous devez communiquer les capacités et les objectifs d'un SIA en termes simples et clairs. Vous pouvez expliquer la conception des fonctionnalités, des attributs et des modèles du SIA dans les descriptions des produits ou services offerts aux personnes concernées. Expliquez aussi l'utilisation des renseignements personnels au sein du SIA.

Si la description explicite de la logique d'un SIA est hautement complexe, vous pouvez considérer une approche d'explication implicite sur le fonctionnement général du SIA. Utilisez des techniques interactives et de visualisation afin d'expliquer les concepts le plus simplement et clairement possible.

Pour aller plus loin :

- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.53-54;
- Commission européenne (UE) 2018, p.28

Politique interne

Vous avez avantage à développer une politique interne sur l'explicabilité indiquant à quels moments une explication des procédures techniques est nécessaire afin d'assurer la compréhension par la personne concernée. Vous pouvez aussi inclure une définition d'explicabilité dans les politiques internes.

Pour aller plus loin :

- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.53

Conception

Analysez et veillez à inclure le principe d'explicabilité dans la conception dès le début du projet et à chacune des phases de développement du SIA. Il est essentiel que vous cherchiez continuellement à utiliser le modèle le plus simple et interprétable possible.

Pour aller plus loin :

- University College London (Royaume-Uni) 2019;
- International Technology Law Association (International) 2019, p.294-295

Évaluation

Évaluez à quel point un SIA peut être compris par les personnes concernées. Si le SIA a été fourni par une partie tierce, consultez cette dernière lors de l'évaluation du niveau d'explicabilité.

Pour aller plus loin :

- University College London (Royaume-Uni) 2019;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.57

Code source et données ouvertes

Publiez et partagez ou offrez une licence sur les données, lorsque possible, le code source ou le modèle du SIA si cela s'avère approprié compte tenue de certaines limitations, tel que la propriété intellectuelle, la protection des renseignements personnels ou encore la cybersécurité. Vous pourrez voir des moyens permettant de d'atténuer ces limitations. Par exemple, il est possible de partager des données en utilisant une fiducie de données.

Si la publication n'est pas possible, vous pourrez prévoir des moyens de mitiger. Par exemple, vous pourriez publier les métadonnées du modèle, tel que la performance de ce dernier sur certaines bases de données.

Pour aller plus loin :

- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.2.6.;
- International Technology Law Association (International) 2019, p.300-301;
- Gov. UK (Royaume-Uni) 2020

6 EXACTITUDE, DROIT DE RECTIFICATION ET DROIT DE RÉVISION

6.1 Exactitude

6.1.1 Obligations légales générales

Les renseignements personnels détenus doivent être **exacts, complets et à jour** pour l'utilisation aux fins déterminées.

- **art. 11[94], 71[95] de la Loi sur le secteur privé;**
- **art. 72 la Loi sur l'accès aux documents;**
- **art. 56 du projet de loi fédéral C-27 – Partie 1 Loi sur la protection de la vie privée des consommateurs**

Pour aller plus loin :

- **Commission d'accès à l'information, Protection des renseignements personnels**
- **Commission d'accès à l'information, Concernant l'accès à vos renseignements**

6.1.2. Bonnes pratiques pour les SIA

Exactitude des données

Vous devez mettre en place des mesures pour que les renseignements personnels utilisés pour produire des inférences, prédictions et évaluations soient exacts, mis à jour, complets et non-équivoques. Vous devez documenter et enregistrer ces mesures.

Pour aller plus loin :

- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.38, 67;
- European Commission (EU) 2020, p.10;
- Secrétariat du Conseil du Trésor du Canada (Canada) 2019, §6.3.3

94 Entrée en vigueur : 22 sept. 2023
95 Entrée en vigueur : 22 sept. 2023

Traçabilité des données

Vous devez établir des mesures de traçabilité des données permettant d'identifier le renseignement personnel qui a été utilisé afin de rendre une décision et d'évaluer son niveau d'exactitude. Ces mesures devraient être mises en place tout au long du cycle de vie du SIA.

Il est essentiel pour vous d'enregistrer la source d'origine, le type de collecte, les mouvements et interactions, et la transformation des données. Vous pouvez enregistrer comment l'exactitude des données est maintenue à travers ces traitements. Si l'origine d'une donnée n'est pas retraçable, vous pouvez évaluer les risques d'utiliser une telle donnée.

Pour aller plus loin :

- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.37, 48-49;
- European Commission (EU) 2020, p.14

Possibilité de correction et mise à jour

Vous devez mettre des outils de gestion de préférences en matière de vie privée à la disposition des personnes concernées. Ces outils pourraient permettre aux utilisateurs de vérifier l'exactitude des renseignements personnels, de les mettre à jour, de les supprimer ou d'en ajouter, et de corriger les inexactitudes.

Pour aller plus loin :

- Commission européenne (UE) 2018, p.17-20, 36

Mise à jour

Vous devez régulièrement réviser et mettre à jour les données. Si cela est approprié, vous pouvez effectuer les mises à jour avec des nouvelles données d'entrée obtenues par le SIA déployé.

Pour aller plus loin :

- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.40

Facteurs nuisant à l'exactitude

Vous devez comprendre et adresser les facteurs pouvant nuire à la qualité, et donc l'exactitude des données. Ces facteurs incluent notamment

- la fiabilité des sources d'origine des données;
- le temps écoulé depuis la collecte ou la dernière mise à jour;
- à quel point les valeurs dans les groupes de données correspondent aux véritables caractéristiques des entités décrites dans ces groupes;
- l'exhaustivité de l'ensemble de données d'attributs et d'éléments;
- l'intégrité de l'ensemble des données qui a été joint à partir des groupes de données, par la façon dont l'extraction et la transformation ont été effectués;
- l'intervention humaine (i.e. : filtrage, application d'étiquettes, modification des données...);
- la facilité d'utilisation des groupes de données.

Pour aller plus loin :

- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.38

Registre de décisions erronées

Vous devez tenir un registre des décisions rendues sur la base d'inférences, prédictions ou évaluations erronées à cause de renseignements personnels inexacts, incomplets ou équivoques.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

6.2 Droit de rectification

6.2.1 Obligations légales générales

Si un renseignement personnel concernant une personne est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, **cette personne peut exiger qu'il soit rectifié**. Une personne peut **aussi faire supprimer** un renseignement périmé ou non justifié.

- **art. 8, 12.1, 16, 19, 28, 28.1, 29, 30, 32 à 36, 78, 79 de la Loi sur le secteur privé;**
- **art. 65.296, 89 à 93, 9497 et 9898 de la Loi sur l'accès aux documents;**
- **art. 38 à 40 du C.c.Q.;**

Pour aller plus loin :

- **Commission d'accès à l'information, Rectifier vos renseignements**

6.2.2 Bonnes pratiques pour les SIA

Canal de rétroaction

Vous devez mettre en place des canaux de communication permettant aux personnes concernées de donner des commentaires ou de poser des questions en lien avec leurs renseignements personnels. Ces canaux pourraient être gérés par le ou la responsable en IA si cela est approprié.

Pour aller plus loin :

- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.56,57

Retrait des renseignements

La rectification ou suppression d'un renseignement personnel contenu dans un modèle de SIA peut engendrer la nécessité de réentraîner ou de supprimer un modèle.

Vous devez incorporer des fonctions permettant un retrait simple et sans altérations majeures au modèle. En ce sens, mettez en place un système de gestion et une ligne de déploiement efficace afin de réduire les coûts et les conséquences découlant d'un retrait de renseignement personnel.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

96 Entrée en vigueur : 22 sept. 2023
97 Entrée en vigueur : 22 sept. 2022 et 22 sept. 2023
98 Entrée en vigueur : 22 sept. 2023

La suppression d'une **donnée d'entraînement** ne mène pas nécessairement à la suppression de tous les modèles entraînés sur cette donnée, à moins que le modèle lui-même inclut cette donnée, ou qu'un modèle puisse être utilisé pour inférer une telle donnée. L'effet d'une suppression d'un renseignement personnel des données d'entraînement sur la capacité du SIA à atteindre ses objectifs d'entraînement est donc négligeable.

Il est plus probable que les personnes concernées fassent des demandes de rectification concernant les **données de sortie** plutôt que des données d'entraînement. Il est important de noter que des prédictions et inférences produites par un SIA ne peuvent être inexactes si elles ne prétendent pas être des faits. Si le renseignement personnel utilisé pour atteindre un résultat n'est pas inexact, incomplet ou équivoque, alors le droit à la rectification ne s'applique pas.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

6.3 Révision de décision exclusivement automatisée et intervention humaine

6.3.1. Obligations légales générales

Lorsqu'une décision fondée **exclusivement sur un traitement automatisé** est prise, ou **avant qu'une telle décision soit prise**, la personne concernée doit en **être informée**.

Sur demande, elle doit être informée **du renseignement personnel utilisé, des raisons, ainsi que des facteurs et paramètres utilisés** pour rendre la décision. Elle doit aussi être informée de son droit de rectification.

La personne doit avoir **l'occasion de présenter ses observations** à un membre du personnel en mesure de réviser la décision.

- **art. 12.1[99] et 90.1[100] de la Loi sur le secteur privé;**
- **art. 65.2[101] de la Loi sur l'accès aux documents**

Pour aller plus loin :

- **Commission d'accès à l'information, Vers la conformité à la Loi sur le privé**
- **Commission d'accès à l'information, Traitement automatisé**
- **Commission d'accès à l'information, Espace évolutif – Modernisation des lois**

99 Entrée en vigueur : 22 sept. 2023
100 Entrée en vigueur : 22 sept. 2023
101 Entrée en vigueur : 22 sept. 2023

6.3.2. Bonnes pratiques pour les SIA

Équité

Veillez à ce que les décisions fondées exclusivement sur un traitement automatisé et les révisions de ces décisions soient équitables, justes et non-discriminatoires.

Pour aller plus loin :

- International Technology Law Association (International) 2019, p.296-297;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.64

Procédure de contestation

Vous devez faciliter le processus de révision de décision en offrant une manière simple de contester la décision et de présenter ses observations. Vous pouvez prévoir la capacité d'un SIA à supporter une intervention humaine dès le début de sa conception.

Il vous serait utile de considérer les exigences d'interprétabilité et de conception d'une interface efficace pour les utilisateurs. Par exemple, vous pouvez fournir un lien vers une procédure de révision au moment où la décision est transmise à la personne concernée, avec les délais pour l'examen du dossier et un point de contact désigné pour toute question.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Monetary Authority of Singapore (Singapour) 2019, p.11;
- Commission européenne (UE) 2018, p.30-31, 37;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.55;
- International Technology Law Association (International) 2019, p.293;
- University College London (Royaume-Uni) 2019

Analyse de décision

Dans leur analyse concernant une décision automatisée, vos membres devraient considérer les renseignements personnels utilisés par le SIA afin de produire la décision, les observations additionnelles de la personne concernée, ainsi que des facteurs externes additionnels. Vous devez identifier les facteurs externes à considérer dès la conception du SIA.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Monetary Authority of Singapore (Singapour) 2019, p.6, 12

Évaluation

Vous devez régulièrement surveiller et analyser les données recueillis sur les révisions effectuées. Si les décisions fondées exclusivement sur un traitement automatisé sont régulièrement modifiées en réponse des demandes de révision, il se peut que le SIA ait besoin de mise à jour ou de modification. Vous pouvez inclure les décisions corrigées dans les nouvelles données d'entraînement pourrait réduire le taux d'erreur.

Vous pouvez identifier les besoins selon les résultats de la surveillance et analyse. Par exemple, il peut s'agir du besoin de recueillir plus de données, du besoin d'améliorer la qualité des données, ou du besoin de modifier la procédure de développement du modèle.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Registre

Vous devez tenir un registre des demandes de révision de décisions fondée exclusivement sur un traitement automatisé, et d'informations supplémentaires concernant les révisions. C'est le cas, par exemple, si la personne concernée a présenté des observations, et si la décision a été renversée en conséquent.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

6.4 Membres du personnel chargés des révisions

6.4.1. Bonnes pratiques pour les SIA

Responsabilité

Vous avez la responsabilité de vous assurer que les membres du personnel aient l'autorité et les compétences nécessaires afin de faire des révisions significatives et de pouvoir renverser des décisions automatisées. Vos membres devraient être responsables de leurs décisions.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Formation

Les membres de votre personnel devraient recevoir une orientation, formation et du support adéquats. Vos membres devraient comprendre qu'ils ont un rôle complémentaire au SIA, et ils devraient connaître les facteurs à considérer lors d'une décision.

Vos membres devraient apprendre à avoir un niveau sain de scepticisme dans les résultats produits par les SIA et de ne pas tenir pour acquis que les résultats sont toujours bons. Vous devez leur offrir une formation sur le fonctionnement et les limites du SIA, et sur la façon d'anticiper les erreurs produites par un SIA et la raison de ces erreurs. Vous pouvez fournir des approximations de taux d'erreur.

Il devrait aussi y avoir une formation sur la façon de motiver et d'expliquer pourquoi une décision fondée exclusivement sur un traitement automatisé est confirmée ou renversée.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.8;
- European Commission (EU) 2020, p.8, 15, 20, 22

Biais d'automatisation

Vous pouvez effectuer des tests préalables avec les membres pour observer leur réflexions et comportements, et ainsi prévoir des techniques de prévention et d'intervention en cas de biais d'automatisation. Vous pouvez prévoir ces mécanismes dès le début de conception du SIA et à chacune des phases de son cycle de vie.

Biais d'automatisation :
« Lorsque les utilisateurs humains s'appuient régulièrement sur la sortie générée par un système d'aide à la décision et cessent d'utiliser leur propre jugement ou cessent de se demander si la sortie pourrait être erronée. « [traduction libre] (Information Commissioner's Office (UK) 2020)

Vous devez surveiller les décisions des membres du personnel, plus précisément pourquoi et combien de fois un membre a confirmé ou renversé une décision automatisée. Vous pouvez prévoir un plan de redressement si un membre confirme trop régulièrement les décisions sans être capable de démontrer une analyse authentique.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.38-40

Établir un comité d'évaluation

Dans la mesure où le contrôle par la personne concernée, du fait de la complexité de l'évaluation, risque d'être illusoire, il est diligent que vous mettiez en place un comité d'évaluation indépendant représentant une variété de parties prenantes.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Monetary Authority of Singapore (Singapour) 2019, p.9;
- University College London (Royaume-Uni) 2019;
- Gov. UK (Royaume-Uni) 2020;
- International Technology Law Association (International) 2019, p.296

7 NON-DISCRIMINATION

7.1 Équité et non-discrimination

7.1.1. Obligations légales générales

Toute personne a droit à la reconnaissance et à l'exercice, en pleine égalité, des droits et libertés de la personne, sans distinction, exclusion ou préférence fondée sur la race, la couleur, le sexe, l'identité ou l'expression de genre, la grossesse, l'orientation sexuelle, l'état civil, l'âge sauf dans la mesure prévue par la loi, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, la condition sociale, le handicap ou l'utilisation d'un moyen pour pallier ce handicap.

- **art. 10 de Charte des droits et libertés de la personne**

Pour aller plus loin :

- **Commission d'accès à l'information, Rétablir l'équilibre, p.87, 88, 98, 156**
- **Commission d'accès à l'information, Intelligence artificielle et protection des renseignements personnels, p.7, 11**
- **Commission des droits de la personne et des droits de la jeunesse, Mémoire à la Commission d'accès à l'information sur le document de consultation « intelligence artificielle », p.7-11, 14, 15, 18, 25**

7.1.2. Bonnes pratiques pour les SIA

Équité algorithmique

Vous devez clairement définir le terme « discrimination » dans le contexte spécifique du SIA. Pour cela, vous pouvez consulter les groupes affectés afin d'avoir une définition significative.

Les résultats du SIA doivent être justes et équitables. Il est de votre responsabilité de prévenir les résultats discriminatoires injustifiés résultant de données déséquilibrées, de conception ou fonctionnement défectueux, ou toute autre raison.

Pour aller plus loin :

- Monetary Authority of Singapore (Singapour) 2019, p.6, 7;
- European Commission (EU) 2020, p.16-17;
- University College London (Royaume-Uni) 2019;
- Gov. UK (Royaume-Uni) 2020

Responsabilité et gouvernance

Votre responsable en IA devrait être responsable de la stratégie d'atténuation des risques de discrimination, et de mettre en place des mesures et politiques conformes à l'état de l'art.

Vous pouvez offrir des formations éducatives sur les risques de discrimination d'un SIA à vos membres du personnel responsables de la création et du bon fonctionnement du SIA. Vous devez vous assurer d'avoir des équipes diversifiées.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Monetary Authority of Singapore (Singapour) 2019, p.7;
- University College London (Royaume-Uni) 2019;
- Gov. UK (Royaume-Uni) 2020;
- International Technology Law Association (International) 2019, p.290, 296

Évaluation

Tout au long de son cycle de vie, un SIA devrait être surveillé et régulièrement évalué afin de prévenir des résultats discriminatoires. À ce titre, il est de votre devoir d'identifier les risques que le SIA produise des résultats discriminatoires, les groupes de population affectés, et les préjudices potentiels.

Il pourrait être utile de faire une évaluation d'impact relative aux droits de l'homme. À ce titre, vous pouvez évaluer quel sera l'impact social et environnemental du projet de SIA.

Vous pouvez utiliser des techniques mathématiques permettant de mesurer le niveau de discrimination d'un SIA. Au besoin, vous pouvez faire un audit algorithmique afin de vous assurer qu'un SIA ne produit pas de résultats discriminatoires, erronés ou injustifiés, et afin de vérifier le bon fonctionnement du SIA. Vous pouvez documenter ces pratiques.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- **Commission d'accès à l'information, Évaluation des facteurs relatifs à la vie privée**
- Commission européenne (UE) 2018, p.31;
- Monetary Authority of Singapore (Singapour) 2019;
- European Commission (EU) 2020, p.5, 16;
- Gov. UK (Royaume-Uni) 2020;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.64

Utilisation et fin compatible

Lorsque l'évaluation du risque de discrimination d'un SIA nécessite le traitement de données personnelles, et que cette évaluation n'est pas une fin qui a été déterminée lors de la collecte, il faut vous assurer qu'un nouveau consentement soit obtenu, que cette utilisation soit à des fins compatibles avec celles pour lesquelles il a été recueilli, ou que son utilisation soit manifestement au bénéfice de la personne concernée.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020

Solutions IA

Vous devez prendre en compte le potentiel de discrimination dès le début de la conception du SIA, et des mesures doivent être prises en conséquence. Il existe certaines techniques d'ajustement afin de corriger des déséquilibres dans les données d'entraînement.

Par exemple, des données peuvent être ajoutées ou soustraites afin de corriger les déséquilibres causés par la sous-représentation ou surreprésentation de certains groupes de population. Si un modèle reflète une ancienne discrimination, il est possible de modifier les données, changer la procédure d'apprentissage du modèle ou de modifier un modèle à la suite de l'entraînement. Vous devez déterminer les techniques appropriées selon le projet et l'état de l'art.

Pour aller plus loin :

- Information Commissioner's Office (Royaume-Uni) 2020;
- Info-communications Media Development Authority and Personal Data Protection Commission (Singapour) 2020, p.64

Signalement

Vous pouvez mettre en place un système de signalement de problèmes liés à la discrimination ou à la mauvaise performance du SIA.

Pour aller plus loin :

- European Commission (EU) 2020, p.21-22;
- University College London (Royaume-Uni) 2019

QUELQUES EXEMPLES DE CIRCONSTANCES POUVANT CAUSER DES RÉSULTATS INÉQUITABLES OU DISCRIMINATOIRES EN IA

Exemples corrompus

Lorsque le SIA conserve le biais existant dans les anciennes données.

Échantillon biaisé

Les observations confirment les prédictions, ainsi créant une boucle de rétroaction perverse.

Fonctionnalités limitées

Les fonctionnalités peuvent être moins informatives ou recueillies de manière moins fiable lorsqu'il est question de groupe minoritaire.

Disparité de la taille de l'échantillon

Lorsqu'il y a moins de données d'entraînement sur les groupes minoritaires que les groupes majoritaires.

Serveur mandataire

Même si les attributs protégés ne sont pas utilisés pour entraîner un SIA, il peut toujours y avoir d'autres serveurs mandataires des attributs protégés.

- University College London (Royaume-Uni) 2019

RÉFÉRENCES

Guidance on AI and data protection, **Information Commissioner's Office (UK) 2020**

Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, **Commission européenne (UE) 2018**

Data Ethics Framework, **Gov. UK (UK) 2020**

Principles to Promote Fairness, Ethics, Accountability and Transparence in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, **Monetary Authority of Singapore (Singapore) 2019**

Responsible AI Policy Framework, **International Technology Law Association (International) 2019**

Assessment List for Trustworthy Artificial Intelligence, **European Commission (EU) 2020**

Directive sur la prise de décision automatisée, **Secrétariat du Conseil du Trésor du Canada (Canada) 2019**

Algorithmic Impact Assessment : Fairness, Robustness and Explainability in Automated Decision-Making, **University College London (UK) 2019**

Model Artificial Intelligence Governance Framework, **Info-communications Media Development Authority and Personal Data Protection Commission (Singapore) 2020**

CENTRE
DE RECHERCHE
EN DROIT
PUBLIC

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