MODÈLE D'ÉVALUATION DES FACTEURS RELATIFS À LA CIRCULATION DES DONNÉES

Instrument de protection de la vie privée et des droits et libertés dans le développement et l'usage de l'intelligence artificielle.

Mars 2022

Me Vincent Gautrais
Me Nicolas Aubin

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

- 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
- Me Nicolas Aubin est avocat au Cabinet Cain Lamarre, travaillant principalement en protection des renseignements personnels. Il détient une maîtrise en droit des technologies de l'information de l'Université de Montréal. nicolas.aubin@cainlamarre.ca

À propos des partenaires

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 ».

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.

Produit avec le soutien financier des Fonds de recherche du Québec

Québec
Fonds de recherche – Nature et technologies
Fonds de recherche – Santé
Fonds de recherche – Société et culture

ISBN: 978-2-925138-37-2
DOI: 10.61737/RRLB1735

TABLE DES MATIÈRES

LEXIQUE

Algorithme d'apprentissage
Algorithme qui, en se fondant sur des approches mathématiques et statistiques, peut perfectionner leur niveau de précision et de résolution de tâches automatiquement à partir de quantités importantes de données.

Incident de confidentialité
Accès, usage, communication ou perte non autorisée par la Loi d'un renseignement personnel ou toute atteinte à la protection d'un renseignement personnel[1].

Intelligence artificielle (IA)
«Domaine d'étude ayant pour objet la reproduction artificielle des facultés cognitives de l'intelligence humaine dans le but de créer des systèmes ou des machines capables d'exécuter des fonctions relevant normalement de celle-ci.»[2]

Système d'intelligence artificielle (SIA)
«Système conçu pour simuler le fonctionnement de l'intelligence humaine afin d'exécuter des fonctions relevant normalement de celle-ci.»[3] Les systèmes d'apprentissage profond sont un exemple de SIA.

Opération
Tout processus ou ensemble de processus utilisant des renseignements à caractères personnels tels que : la collecte, la communication, l'utilisation, la conservation ou la destruction de renseignements personnels.

Collecte
«Opération par laquelle des renseignements sont placés sous le contrôle d'une entité qui au fait de cette opération acquiert, à l'égard des documents ou renseignements, le droit d'en prendre connaissance. Pour qu'il y ait «collecte» de renseignements ou de documents, il faut que ces documents ou renseignements aient été communiqués à une entité, ou à une personne qui a le droit d'en prendre connaissance.»[4]

Communication
Opération impliquant «de conférer un droit de prendre connaissance de la teneur du document ou du renseignement.»[5]

---

1 *Projet de loi n°64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 22 septembre 2021, en ligne : http://assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html ci-après « PL64 », art 103 (nouvel article 3.6 de la LPRPSP).

2 Office québécois de la Langue française, « Fiche terminologique : "intelligence artificielle" » (2017), en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8385376 (consulté le 20 octobre 2021).

3 Office québécois de la Langue française, « Fiche terminologique : "système d'intelligence artificielle" », en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=23798323 (consulté le 20 octobre 2021).

4 Vincent Gautrais et Pierre Trudel, *Circulation des renseignements personnels et web 2.0.*, Éditions Thémis, Montréal, 2010, p. 226.

5 *Id.*, p. 227.

Utilisation
Cette opération implique avoir connaissance des renseignements personnels et de pouvoir «décider d'agir ou non à la lumière de la connaissance que ces renseignements personnels confèrent.»[6]

Conservation
«Action de maintenir l'intégrité d'un document, que celui-ci contienne - ou non - des renseignements personnels, et ce, durant toute la durée active document afin que ce dernier demeure accessible.»[7]

Hébergement
«Réalisation d'une activité de conservation par un tiers, et ce, relativement à une réalité assez précise à savoir celle pour un prestataire de mettre à disposition des internautes des espaces Web conçus et gérés par ces mêmes tiers.»[8]

Transmission
«Transmettre un document, c'est l'expédier d'un point d'expédition à un point de réception. C'est le faire passer techniquement d'un point à l'autre.»[9]

Renseignement personnel
«Tout renseignement qui concerne une personne physique et permet directement ou indirectement de l'identifier.»[10]

Renseignement dépersonnalisé
Renseignement personnel qui «ne permet plus d'identifier directement la personne concernée»[11].

Renseignement anonymisé
«Un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne»[12].

Renseignement personnel sensible
Renseignement personnel qui «par sa nature ou en raison du contexte de son utilisation ou de sa communication [...] suscite un haut degré d'attente raisonnable en matière de vie privée»[13].

6 *Id.*, p. 231.
7 *Id.*, p. 228.
8 *Id.*, p. 230.
9 *Id.*, p. 106.
10 PL64, préc., note 1. art 2.
11 *Id.* art 102 (nouvel article 12 de la LPRPSP).
12 *Id.* art 111 (nouvel article 23 de la LPRPSP).
13 *Id.* art 102 (nouvel article 12 de la LPRPSP).

INTRODUCTION

MODÈLE D'ÉVALUATION DES FACTEURS RELATIFS À LA CIRCULATION DES DONNÉES

Instrument de protection de la vie privée et des droits et libertés dans le développement et l'usage de l'intelligence artificielle.

1. Mise en contexte de l'élaboration du présent modèle

Intégration dans les lois. Le projet de loi québécois 64 (ci-après «PL64»)[14] a récemment obtenu la sanction royale[15]. Ce dernier impose de réaliser une ***Évaluation des facteurs relatifs à la vie privée*** (ci-après «EFVP») dans certaines circonstances aux personnes et entreprises détentrices ou utilisatrices de renseignements personnels. Ce processus d'analyse n'a rien de nouveau en soi. En Europe, le Règlement Général sur la Protection des Données (ci-après «RGPD»)[16] exige lui aussi de réaliser une procédure similaire intitulée ***Analyse d'impact relative à la protection des données*** (ci-après «AIPD») dans certaines circonstances[17]. Ce type d'analyse est également une démarche déjà bien établie aux États-Unis et en Australie[18].

Définition préalable. Selon PL64, une EFVP est une démarche préventive ayant comme principal objectif d'assurer une meilleure protection des renseignements personnels et, par extension, de la vie privée des personnes concernées. Selon la *Commission d'accès à l'information du Québec* (ci-après «CAI») une EFVP «consiste à considérer tous les facteurs qui auraient des conséquences positives et négatives sur le respect de la vie privée des personnes concernées»[19]. Les facteurs identifiés par la CAI sont :

- «la conformité du projet à la législation applicable à la protection des renseignements personnels et au respect des principes qui l'appuient ;
- la détermination des risques d'atteinte à la vie privée engendrés par le projet et l'évaluation de leurs conséquences;
- la mise en place de stratégies pour éviter ces risques ou les réduire efficacement.»[20]

14 PL64, préc., note 1.
15 *Id.*
16 Union européenne, *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 (Règlement général sur la protection des données) (RGPD)*, Règlement (UE) 2016/679, p. 679, en ligne : https://www.cnil.fr/fr/reglement-europeen-protection-donnees (consulté le 9 novembre 2021).
17 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 35(1).
18 Selon la Commission d'accès à l'information (ci-après "CAI"), le *Privacy Impact Assessment* (ci-après "PIA") ne constitue que l'expression anglaise du EFVP. Voir Commission d'accès à l'information du Québec, *Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée*, mis à jour le 10 mars 2021, en ligne : https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf (consulté le 21 octobre 2021), voir la première note de bas de page du Guide.
19 *Id.* sous la page *Qu'est-ce qu'une évaluation des facteurs relatifs à la vie privée* (EFVP) ?
20 *Id.*

Objectifs et motivations. Les motivations de produire une EFVP ou une AIPD vont bien au-delà des impératifs légaux. En effet, ces instruments remplissent beaucoup d'autres rôles tels que :

- démontrer la diligence de l'entreprise en cas de poursuite ou d'enquête ;
- contrer certaines craintes des usagers puisqu'elle démontre l'importance accordée à la protection de leurs données ;
- identifier les mesures nécessaires au respect des droits et règlements en vigueur et implémenter ces mesures ;
- identifier comment se protéger des fautes, actions ou inactions en provenance des tiers contractants ;
- identifier les besoins en matière d'implémentation de mesures de sécurité ;
- identifier les parties prenantes pouvant procurer un apport bénéfique au projet ;
- identifier s'il est possible ou réaliste de mener le projet à bien tout en respectant la Loi et ;
- identifier la présence des incidents de confidentialité qui pourraient représenter un préjudice grave aux usagers[21].

À ce titre, une entreprise peut être motivée à réaliser une EFVP bien qu'elle ne soit pas imposée par la Loi.

Modèles. Certaines régions, comme l'Europe, bénéficient de plusieurs modèles d'AIPD. On peut notamment penser au modèle européen décrit dans la **Note de Politique No 1/2020 du d.pia.lab** (ci-après «d.pia.lab»)[22] qui est déjà disponible au public. Cependant, la documentation canadienne relative à cette question est bien moins étoffée. Certes, des guides d'accompagnement ont été créés, notamment par la CAI[23]. Toutefois, autant que nous le sachions, ces guides ne proposent pas de modèle d'évaluation similaire au modèle européen susmentionné. De plus, ceux-ci ne prennent pas en considération les toutes dernières modifications législatives apportées par PL64. À ce titre, il convient de proposer un modèle d'analyse d'impact capable de prendre en considération les particularités légales et culturelles canadiennes et québécoises. À cet égard, nous utiliserons des encarts qui identifieront les principales distinctions entre les régimes juridiques québécois et européens.

Limites. Le présent modèle ne prétend pas s'inspirer de tous les règlements et lois québécoises susceptibles d'être appliqués dans toutes les situations impliquant l'utilisation, la conservation, la communication, la collecte et la destruction des renseignements personnels. Les lois et règlements pouvant régir ces opérations sont innombrables et peuvent relever de protections spécifiques, telles que le secret professionnel, qui ne sont pas explorées dans le présent modèle. De plus, ce document ignore certains aspects introduits par PL64, tel que le droit à la désindexation.

De plus, le présent document ne doit pas être considéré à titre de conseil juridique ou comme offrant des conseils juridiques. Il n'engage en aucune façon la responsabilité de ses auteurs.

Importance de PL64. En conséquence, le présent modèle porte un intérêt particulier aux modifications législatives prévues par PL64 puisque ce dernier a récemment reçu une sanction royale. Nous estimons qu'il existe un besoin urgent de promouvoir un modèle capable de guider l'application des normes fixées par le PL64 aux réalités spécifiques des *systèmes d'intelligences artificielles* (ci-après «SIA»).

21 Il est nécessaire de dénoncer certains bris de sécurité susceptibles de porter préjudice aux individus. Voir PL64, préc., note 1 art 103 (nouvel article 3.5. de la LPRPSP).

22 Dariusz Kloza, Alessandra Calvi, Simone Casiraghi, Sergi VAZQUEZ Maymir et Nikolaos Ioannidis, « Analyse d'impact relative à la protection des données dans l'Union européenne : élaboration d'un modèle de rapport du processus d'analyse », *Vrije Universiteit Brussel* 2020.1.57.

23 Commission d'accès à l'information du Québec, préc., note 18.

Lois applicables. Sans prétendre présenter une analyse exhaustive de ceux-ci, le présent modèle explore les instruments suivants :

- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* aussi connue sous le nom de «Projet de loi 64» (ci-après «PL64») ;
- 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* aussi connue sous le nom de «Projet de loi C-11» (ci-après «C-11») ;
- La *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après «LPRPDE») ;
- La *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après «LPRPSP») ;
- La *Loi concernant le cadre juridique des technologies de l'information* (ci-après «LCJTI») et
- La *Charte des droits et libertés de la personne.*

L'obligation future de l'évaluation des facteurs sous PL64. PL64 indique qu'une personne qui exploite une entreprise devra procéder à une EFVP dans certaines circonstances, notamment :

- 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*»[24] *réalisée par une entité publique*[25] *ou privée*[26] ;
- avant de communiquer un renseignement personnel à l'extérieur du Québec[27] ;
- avant de confier «à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte»[28] un renseignement personnel et
- avant de communiquer, sans le consentement des personnes concernées, des renseignements personnels à une personne ou un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques[29].

Signification de l'obligation de créer une EFVP «*lors de l'acquisition, le développement et la refonte de systèmes d'information*». L'obligation de procéder à une EFVP pour «*tout projet d'*acquisition, de développement et de refonte de système d'information ou de prestation électronique de services» est difficile à saisir. Afin d'en comprendre la portée, il faut comprendre, qu'originellement, *PL64 envisageait s'appliquer à* **tous** *les projets de système d'information ou de prestation électronique présents et futurs qui ont recours à des renseignements personnels*[30].

24 PL64, préc., note 1 préambule, art 15 et 103 (nouvel article 63.5 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et nouvel article 3.3. de la LPRPSP).
25 *Id.* art 15 (nouvel article 63.5 la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*).
26 PL64, préc., note 1 art 103. (nouvel article 3.3 de la LPRPSP).
27 *Id.* art 111. (nouvel article 17 de la LPRPSP).
28 *Id.*
29 *Id.* art 118. (nouvel article 21 de la LPRPSP).
30 Assemblée nationale du Québec, « Étude détaillée du projet de loi n 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels - 42e législature, 1re session (27 novembre 2018 au 13 octobre 2021) », Journal des débats de la Commission des institutions 45-20 (17 février 2021), en ligne : http://assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-210217.html (consulté le 1 décembre 2021).

Cependant, considérant les coûts que cela représenterait pour la fonction publique[31], la mention «tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique»[32] a été introduite au projet de loi. Cet amendement avait comme intention de ne pas imposer aux organismes l'obligation de produire une EFVP pour les systèmes d'informations ou de prestations électroniques déjà existants[33].

Toutefois, il faut se garder de conclure que la même logique s'applique nécessairement aux autres situations qui exigent de produire une EFVP. Par exemple, une entreprise qui communique des renseignements personnels à des organisations situées à l'extérieur du Québec devra a priori produire une EFVP même si de telles activités ont été initiées avant la mise en œuvre de PL64.

Dates de mise en œuvre. En date du 22 septembre 2022, il sera obligatoire de produire une EFVP à des fins d'étude, de recherche ou de production de statistiques dans le secteur privé[34].

En date du 22 septembre 2023, il sera obligation de produire une EFVP dans le secteur privé dans les autres circonstances susmentionnées[35].

Démarche volontaire. Ainsi, bien que PL64 ait reçu la sanction royale le 22 septembre 2021, il n'a toujours pas été complètement mis en œuvre pour le secteur privé[36]. À ce titre, la création d'une EFVP constitue, pour le moment, une initiative de nature volontaire pour les organisations privées.

Proportionnalité de l'EFVP. PL64 prévoit également que les EFVP doivent être proportionnées :

- à la sensibilité des renseignements concernée ;
- à la finalité de leur utilisation ;
- à leur quantité ;
- à leur répartition et
- à leur support[37].

31 *Id.*
32 PL64, préc., note 1 art 103. (nouvel article 3.3 de la LPRPSP).
33 *Id.* préambule, art 15 et 103 (nouvel article 63.5. de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et nouvel article 3.3 de la LPRPSP). et voir Assemblée nationale du Québec, préc., note 30.
34 PL64, préc., note 1 art 118 et 175. (nouvel article 21 de la LPRPSP). et Commission d'accès à l'information du Québec, « Évaluation des facteurs relatifs à la vie privée », en ligne : https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/evaluation-facteurs-relatifs-vie-privee (consulté le 23 janvier 2022).
35 PL64, préc., note 1 art 103, 111 et 175. (nouvel article 3.3 et 17 de la LPRPSP). et Commission d'accès à l'information du Québec, préc., note 34.
36 PL64, préc., note 1 art 175.
37 PL64, préc., note 1 préambule, art 15 et 103 (nouvel article 63.5 de la Loi sur l'accès aux documents des organismes publics et sur la protection des *renseignements personnels* et nouvel article 3.3 de la LPRPSP).

2. Spécificités du contenu du présent modèle

Caractéristiques du document. Il convient d'identifier certaines caractéristiques du présent modèle afin d'en guider l'utilisation. Ainsi le présent modèle :

- doit être compris comme une démarche et non un simple document.
- doit être conceptualisé comme étant dynamique. Ainsi, elle est initiée dès la création du projet[38], se modifie tout au long de son développement et lors de son exécution[39]. L'EFVP doit être révisée au regard des nouveaux risques découverts en raison des obstacles et des changements de direction affectant le développement du projet[40].
- est destiné aux acteurs privés. Le présent modèle n'adresse pas les changements législatifs proposés par PL64 auprès des organisations publiques.
- doit être compris comme un ouvrage de doctrine. Cependant, les notes de bas de page et l'Annexe identifient les dispositions législatives et les jurisprudences appropriées.

Circulation. Le présent document propose d'étudier les risques et impacts résultants principalement de la *circulation* des renseignements personnels. Ainsi, c'est en raison de cette circulation que les renseignements personnels trouvent leur valeur et leur utilité. Malgré l'absence d'une terminologie aussi explicite dans PL64 et la LPRPSP, la notion de *circulation* des renseignements personnels reste très influente au sein d'autres régimes de protection des renseignements personnels tels que celui imposé par le RGPD[41]. En particulier, la partie A du présent document réclame à l'évaluateur d'illustrer le cycle de vie prévue des renseignements personnels.

Modèle québécois. Le modèle proposé trouve son inspiration du modèle d.pia.lab. Cependant, contrairement au modèle européen, le modèle en espèce incorpore les particularités légales et culturelles québécoises et canadiennes.

Intelligence artificielle. Finalement, le présent document propose un modèle dédié aux *systèmes d'intelligence artificielle* (ci-après «SIA»). Au-delà de la seule vie privée, les SIA exigent une approche plus globale des vulnérabilités générées incorporant, par exemple, des considérations visant à assurer un usage non discriminatoire des renseignements personnels. À ce titre, le modèle incorpore les éléments d'une *Analyse d'impact algorithmique* (ci-après «AIA») qui demande, entre autres, à :

- «évaluer les risques associés à l'utilisation de décisions fondées exclusivement sur un traitement automatisé de renseignements personnels, comme des erreurs ou encore un effet discriminatoire»[42] et à ;
- «déterminer les mesures à mettre en place pour atténuer de tels risques»[43].

38 Voir notamment Id. art 103 (nouvel article 3.3 de la LPRPDE).

39 Commission d'accès à l'information du Québec, préc., note 18. sous la section «Qu'est-ce qu'une Évaluation des facteurs relatifs à la vie privée (EFVP)?».

40 *Id.*

41 Voir notamment *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 (Règlement général sur la protection des données)(RGPD)*, préc., note 16., préambule 166.

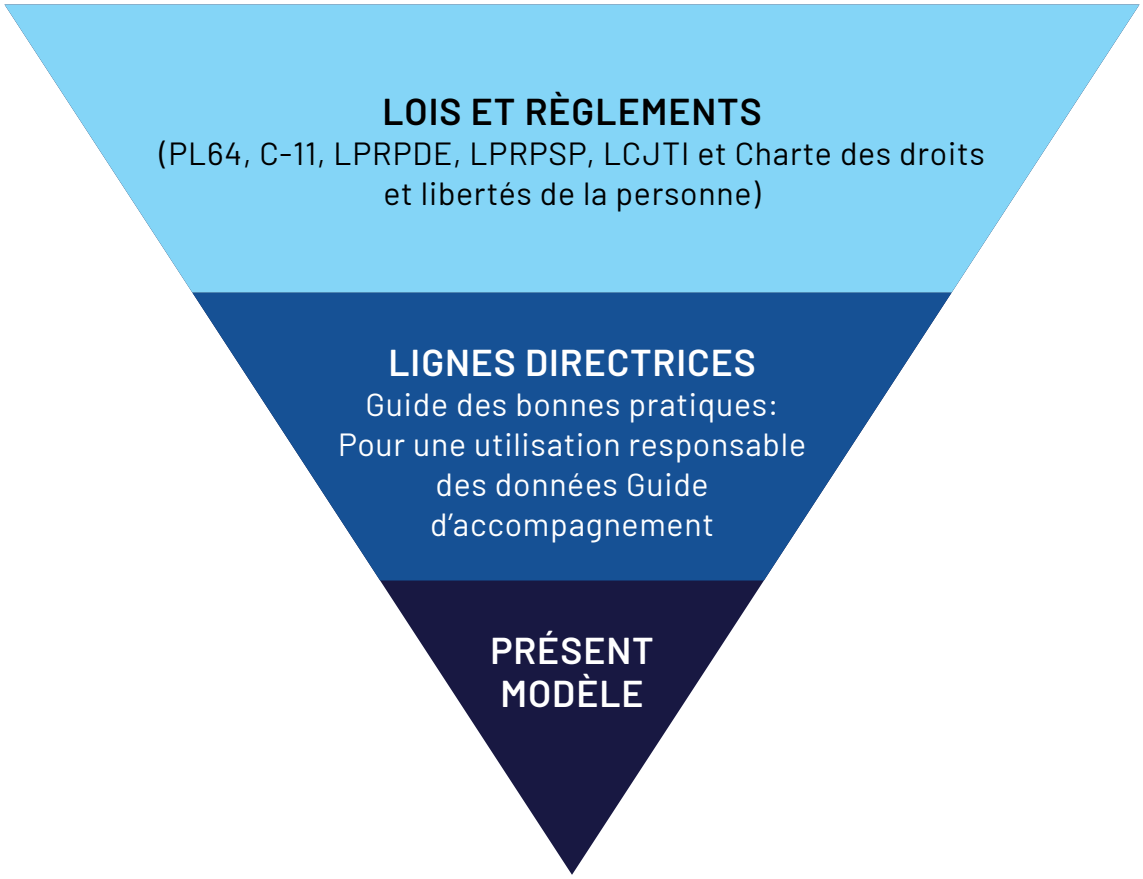
42 Gouvernement du Québec, « Décision fondée exclusivement sur un traitement automatisé », en ligne : https://www.quebec.ca/gouvernement/travailler-gouvernement/services-employes-etat/conformite/protection-des-renseignements-personnels/technologie-et-droit-a-la-protection-des-renseignements-personnels/decision-traitement-automatise (consulté le 20 janvier 2022).

43 *Id.*

Lignes directrices. Le présent document constitue la suite logique du *Guide des bonnes pratiques: Pour une utilisation responsable des données* développé par l'*Observatoire international sur les impacts sociétaux de l'IA et du numérique*[44]. Ce guide propose lui-même des lignes directrices visant à assurer le respect des normes légales dans le développement et le déploiement de SIA. La Figure 1 sous-mentionnée illustre le positionnement du document dans l'architecture normative.

Au-delà de la vie privée. Le présent modèle surpasse les considérations réclamées pour la création d'EFVP[45] ou d'AIDP[46]. En effet, il incorpore des considérations qui dépassent largement la protection de la vie privée et des renseignements personnels telle que la non-discrimination. Afin de refléter convenablement cette réalité, nous qualifierons la démarche proposée en espèce d'***Évaluation des facteurs relatifs à la circulation des données*** (ci-après «EFCD») soit une évaluation incorporant tous les éléments nécessaires pour réaliser une EFVP réclamée par PL64, mais qui évalue, en plus, le respect de principes qui dépassent la simple protection de la vie privée tels que l'explicabilité et la non-discrimination.

Figure 1 : Positionnement du présent modèle dans l'architecture normative



44 OBVIA, « Guide des bonnes pratiques: Pour une utilisation responsable des données développé par l'Observatoire international sur les impacts sociétaux de l'IA et du numérique. », 2022.

45 PL64, préc., note 1 art 103 (nouvel article 3.3 de la LPRPDE).

46 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16. au préambule 84.

3. Structure du document

Trois parties. Le présent document sous-divise l'évaluation en trois parties.

Partie A

Dans la Partie A, l'évaluateur est appelé à présenter les principaux objectifs du projet et à illustrer le cycle de vie des renseignements collectés, utilisés, communiqués et conservés au cours du projet.

Partie B

La Partie B est le cœur du présent modèle. Elle réclame d'évaluer les risques que présente le projet au regard de sept principes fondamentaux. De plus, l'évaluateur devra présenter et évaluer les mesures mises en place pour répondre à ces risques, évaluer les risques résiduels et formuler des recommandations lorsque nécessaire.

Ces principes sont :

I. La responsabilité

II. La justification sociale

III. La transparence

IV. La sécurité

V. L'explicabilité

VI. L'exactitude, le droit de rectification et le droit de révision

VII. La non-discrimination

Partie C

La Partie C comprend l'**évaluation finale** ainsi que les **recommandations** de l'évaluateur. Elle lui permet de présenter succinctement quels sont les manquements qu'il convient de corriger. Elle lui permet également d'identifier quelles mesures sont recommandées afin de mitiger les risques identifiés.

4. Lexique

Importance du lexique dans l'EFCD. L'EFCD devrait contenir un lexique. En effet, les lois ne sont pas uniformes quant aux sens qu'elles accordent à certains termes et concepts. Similairement, elles réfèrent parfois à des concepts similaires par l'usage de différents termes.

Nuances terminologiques

Des sens distincts pour des termes similaires

Les sens accordés à différents termes diffèrent entre régimes législatifs. À titre d'exemple, PL64 et C-11 confèrent un sens différent à la *dépersonnalisation* d'un renseignement.

«RENSEIGNEMENT DÉPERSONNALISÉ» (Article 102 de PL64)	**«DÉPERSONNALISER»** (Article 2 de C-11)
Un renseignement personnel est **dépersonnalisé**: Lorsque ce renseignement ne permet plus d'identifier directement la personne concernée; (soulignement inséré par l'auteur)	**Dépersonnaliser :** Modifier des renseignements personnels — ou créer des renseignements à partir de renseignements personnels — au moyen de procédés techniques afin que ces renseignements ne permettent pas d'identifier un individu ni ne puissent, dans des circonstances raisonnablement prévisibles, être utilisés, seuls ou en combinaison avec d'autres renseignements, pour identifier un individu. (*de-identify*) (soulignements insérés par l'auteur)

Ainsi, au regard du PL64, un renseignement, pour être dépersonnalisé, ne peut pas permettre d'identifier *directement* la personne concernée. Selon C-11 toutefois, un renseignement est dépersonnalisé s'il ne permet pas d'identifier un individu, et ce, même s'il est combiné avec d'autres renseignements dans des circonstances raisonnablement prévisibles. *A priori* donc, PL64 offre donc une définition beaucoup plus large des renseignements *dépersonnalisés* que C-11.

Des termes distincts pour des concepts similaires

Les régimes européen, canadien (sous ce qui était prévu par C-11) et québécois renvoient parfois à des conceptions similaires en utilisant un vocabulaire distinct. Parmi ces distinctions, nous retrouvons les termes utilisés pour référer aux renseignements personnels, à la dépersonnalisation et aux incidents de sécurité.

Renseignements personnels

«RENSEIGNEMENT PERSONNEL» (Article 2 de la LPRPSP)	**«RENSEIGNEMENT PERSONNEL»** (Article 2 de C-11)	**«DONNÉE À CARACTÈRE PERSONNEL»** (Article 4(1) du RGPD)
Tout renseignement qui concerne une personne physique et permet directement ou indirectement de l'identifier.	Tout renseignement concernant un individu identifiable.	«Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale».

Renseignements dépersonnalisés

«RENSEIGNEMENT DÉPERSONNALISÉ» (Article 110 de PL64)	**«PSEUDONYMISATION»** (Article 4(5) du RGPD)
Un renseignement personnel est dépersonnalisé lorsqu'il ne permet plus d'identifier directement la personne concernée.	Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

Incident de confidentialité

«INCIDENT DE CONFIDENTIALITÉ» (Article 103 de PL64)	**«ATTEINTE AUX MESURES DE SÉCURITÉ»** (Article 2 de C-11)	**«VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL»** (Article 4(12) du RGPD)
«Incident de confidentialité» réfère à : 1° l'accès non autorisé par la loi à un renseignement personnel; 2° l'utilisation non autorisée par la loi d'un renseignement personnel; 3° la communication non autorisée par la loi d'un renseignement personnel; 4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.	Communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation prévue à l'article ou du fait que ces mesures n'ont pas été mises en place.	Une violation de la sécurité entrainant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

PARTIE A
RÉSUMÉ DU PROJET

A.1. Considérations générales

Objectifs de la section. Cette partie poursuit trois objectifs principaux soit :

1. faciliter la rédaction des sections subséquentes ;
2. faciliter la compréhension du projet et
3. présenter le cycle de vie des renseignements personnels.

A.2. Décrire le projet

Identifier les personnes responsables. L'évaluateur identifie l'entreprise(s) en charge du projet, la personne responsable du projet et le *Responsable de la protection des renseignements personnels*.

Décrire le projet et identifier ses objectifs. L'évaluateur doit offrir une brève description du projet et identifier ses objectifs. Dans son *Guide sur la rédaction de l'EFVP*, la CAI offre, à titre d'exemples d'objectifs légitimes :

- mieux connaître sa clientèle ;
- déployer sur le Web un service existant ;
- accroître la sécurité d'une installation

ET

- contrer la fraude[47].

Identifier les personnes concernées. L'évaluation devrait également décrire les groupes de personnes concernées par les renseignements personnels collectés, utilisés et/ou communiqués. Il convient d'offrir une approximation de leur nombre et de leur intérêt dans le projet.

A.3. Identifier les renseignements personnels concernés par le projet

Identifier les renseignements personnels. L'évaluateur doit identifier les renseignements personnels qui sont collectés, utilisés, conservés, communiqués et détruits dans le cadre du projet. Il doit également décrire leur support et leur répartition. L'évaluateur peut réunir des renseignements en différents «types» ou catégories de renseignements.

47 Commission d'accès à l'information du Québec, préc., note 18, p. 4.

Types de renseignements personnels. En l'espèce, nous entendons par «type de renseignement» un ensemble regroupant différents renseignements personnels. Il revient à l'évaluateur d'identifier quels regroupements seront pertinents à son évaluation. Nous proposons de regrouper les renseignements en fonction de leur finalité. Par exemple, les «renseignements d'identification» peuvent constituer un «type» de renseignements qui regroupe les informations permettant d'identifier un usager. Cet ensemble peut regrouper, par exemple, son nom, son prénom et son adresse courriel.

Sensibilité. L'évaluateur doit indiquer si les renseignements constituent des renseignements «sensibles». Afin d'évaluer convenablement la sensibilité des renseignements personnels, veuillez vous référer à la section B.2.4.B. du document.

A.4. Décrire le cycle de vie des données

Cycle de vie. L'évaluateur doit décrire le cycle de vie des renseignements personnels concernés par le projet. Dans cette description il convient d'indiquer les opérations qui concernent les renseignements personnels comme :

1. Leur collecte ;
2. Leur utilisation ;
3. Leur communication ;
4. Leur conservation ;
5. Leur destruction et leur anonymisation.

A.4.1. Collecte et utilisation

Sources des renseignements. L'évaluateur doit identifier comment les renseignements sont collectés. À ce titre, les renseignements peuvent être[48] :

recueillis **directement auprès des personnes concernées** par l'entreprise (par le biais d'une page d'inscription sur le site internet de l'entreprise, par exemple ;

- recueillis **auprès un tiers** ;
- **inférés** à partir d'autres renseignements personnels de la personne concernée. (e.g. l'entreprise crée un profil de consommateur).
- **créés** par l'organisation (e.g. l'entreprise assigne un numéro de membre à un usager.)[49] ;

Fins prévues. Il faut indiquer à quelles fins ces renseignements sont recueillis ou utilisés.

Mandat confié à un tiers. Si la personne qui exploite une entreprise mandate un tiers pour recueillir ou utiliser un renseignement, il convient de l'identifier. Il convient également de spécifier l'état ou la province dans laquelle le renseignement est utilisé et / ou communiqué par le tiers.

48 Commission d'accès à l'information du Québec, « Protection des renseignements personnels », en ligne : https://www.cai.gouv.qc.ca/entreprises/protection-des-renseignements-personnels-1/ (consulté le 8 mars 2022).
49 *Id.*

A.4.2. Communication

Destinataires. L'évaluation doit identifier à quels tiers (ou groupes de tiers) les renseignements seront communiqués. Pour nos fins, la communication d'un renseignement à une filiale de l'entreprise en charge du projet constitue une communication et doit être identifiée en conséquence.

Juridiction. La Loi réclame de respecter certaines normes si le renseignement est communiqué à l'extérieur du Québec. À ce titre, il faut indiquer les juridictions dans lesquelles les renseignements sont communiqués.

A.4.3. Conservation, destruction et anonymisation

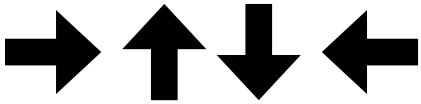
Où. L'évaluateur identifie la province ou l'état dans lequel les renseignements sont conservés. Si l'entreprise mandate un tiers pour héberger ses renseignements, il convient de l'identifier.

Destruction ou anonymisation. L'évaluateur doit indiquer si les renseignements sont détruits ou anonymisés. Si l'entreprise en charge du projet prévoit ne pas détruire ou anonymiser des renseignements personnels, il convient de l'inscrire.

Délai. Identifier *quand* le renseignement est détruit ou anonymisé. Il n'est pas nécessaire d'identifier un délai précis comme un nombre de jours, de mois ou d'années. Le délai peut référer à un évènement spécifique (e.g. la suppression du compte de l'utilisateur)[50].

A.5. Représenter graphiquement le cycle de vie

Représentation graphique. Il peut s'avérer utile de créer une représentation graphique de la circulation des renseignements dans le cadre du projet. Il convient ici de rester succinct dans l'illustration du processus. Pour ce faire, nous recommandons d'utiliser des symboles plutôt que des écrits. Voici des exemples de symboles pouvant être utilisés :

DESTRUCTION	
CONSERVATION (BASES DE DONNÉES)	
CONSERVATION (INFONUAGIQUE)	
TRANSFERT	
UTILISATION	

PARTIE B
ÉVALUATION AU REGARD DES PRINCIPES

B.1. Les sept principes évalués

Principes. Cette partie consiste à évaluer les risques au regard de sept principes distincts soit :

I. La responsabilité ;
II. La justification sociale ;
III. La transparence ;
IV. La sécurité ;
V. L'explicabilité ;
VI. L'exactitude, le droit de rectification et le droit de révision et
VII. La non-discrimination.

Source des principes. Les principes susmentionnés sont inspirés des principes énumérés par le *Guide de bonnes pratiques en intelligence artificielle* de l'*Observatoire international sur les impacts sociétaux de l'IA et du numérique*[51].

B.2. Éléments communs

Structure proposée

Chaque section devrait comprendre:

1. L'identification des normes applicables relatives au principe sous étude ;
2. L'identification des risques ;
3. L'identification des mesures qui ont déjà été mises en place pour diminuer ces risques ;
4. L'évaluation de la probabilité et de l'impact potentiel des risques identifiés ;
5. Des propositions visant à réduire la probabilité et l'impact de ces risques et
6. L'évaluation des risques résiduels.

51 OBVIA, préc., note 44.

B.2.1. Identification des normes applicables

Normes applicables. L'évaluation réclame d'identifier les dispositions législatives qui s'appliquent au projet[52]. En effet, la Loi réclame notamment de se prémunir contre les risques associés aux *incidents de confidentialité*. Or, les *incidents de confidentialité* sont définis comme des comportements non autorisés[53]. Plusieurs normes pertinentes aux principes étudiés sont disponibles en Annexe.

B.2.2. Identification des risques

Identifier les risques. L'évaluateur doit décrire les risques appréhendés. Les risques identifiés peuvent résulter, ou non[54], d'une déviation à une norme légale. Plusieurs exemples de risques sont présentés en Annexe. Par exemple, la CAI propose notamment d'évaluer les risques suivants :

- La conservation de renseignements lorsque leur utilité n'est plus démontrée;
- Le vol de renseignements personnels ;
- La collecte excessive de renseignements ;
- La divulgation non autorisée de renseignements personnels ;
- La réidentification de renseignements préalablement anonymisés ;
- Le manque d'information fournie aux individus lors de la collecte et
- La création excessive ou non justifiée d'informations[55].

B.2.3. Identification des mesures

Mesures. Il convient d'identifier quelles mesures ont déjà été implémentées afin de répondre aux risques identifiés. Une courte description des mesures étudiées doit être présentée.

Types de mesures. Les mesures englobent, notamment :

- les mesures techniques (e.g. crypter ou dépersonnaliser des renseignements) ;
- les mesures organisationnelles (e.g. offrir des formations aux employés de l'entreprise ou limiter l'accès aux renseignements personnels à un nombre limité d'employés) et
- les mesures juridiques (e.g. imposer certains standards de sécurité à ses co-contractants).

Risques créés par les mesures. Il est possible que des mesures mises en place pour réduire certains types de risques créent elles-mêmes de nouveaux types de risques. Ces risques ne doivent pas être ignorés et doivent être identifiés.

B.2.4. Évaluation des risques

Évaluer le risque. Ensuite, l'évaluateur doit analyser adéquatement l'importance des risques. Il s'agit ici d'évaluer les risques qui subsistent malgré la présence des mesures susmentionnées. Pour ce faire, l'évaluateur est appelé à étudier deux composantes du risque soit (A) sa *probabilité* et (B) son *impact* appréhendé[56].

52 Commission d'accès à l'information du Québec, préc., note 18, p. 12-13.
53 PL64, préc., note 1, art 103 (nouvel article 3.6. de la LPRPSP).
54 Commission d'accès à l'information du Québec, préc., note 18, p. 15.
55 *Id.*, p. 16.
56 *Id.*, p. 19-20.

DISTINCTIONS AVEC LE RÉGIME EUROPÉEN

Quels sont les risques devant être évalués ?

L'EFVP réclamée par PL64 réclame d'évaluer les risques liés à la *vie privée*[57]. En effet, le projet de loi réclame d'évaluer les risques liés aux incidents de confidentialité et de produire une «*Évaluation des facteurs relatifs à la vie privée*».

Sur ce plan, le projet de loi se distingue du RGPD qui réclame plutôt d'évaluer les risques liés aux droits et libertés des personnes physiques[58]. À ce titre, une AIPD européenne ne se limite pas qu'aux risques liés à la vie privée et réclame donc d'évaluer un nombre de risques beaucoup plus importants qu'une EFVP québécoise.

Impact des risques «importants»

Le régime européen, le régime qui était prévu par C-11 et le régime québécois prévoient tous des obligations qui ne s'appliquent qu'en présence de risques importants.

À titre d'exemple, ces trois régimes prévoient une obligation d'informer la personne concernée en cas d'incidents présentant des risques élevés. En effet, le RGPD prévoit que «lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne»[59], cette dernière doit en être informée dans les meilleurs délais[60]. Similairement, C-11 prévoit que la personne concernée doit être avisée en cas d'atteintes aux mesures de sécurité qui présentent un «risque réel de préjudice grave»[61]. PL64, quant à lui, prévoit qu'en cas d'incident présentant un «risque de préjudice sérieux», la personne qui exploite une entreprise doit aviser «toute personne dont un renseignement personnel est concerné par l'incident»[62].

Cependant, ces régimes ne prévoient pas toujours les mêmes obligations en présence de risques importants. Ainsi, le RGPD prévoit qu'une analyse d'impact doit être réalisée pour un projet présentant des risques élevés aux droits et libertés des personnes concernées[63]. En revanche, la présence de «risques importants» n'est pas une considération pertinente à l'obligation de produire une EFVP sous PL64[64].

De plus, contrairement au Canada et au Québec, l'Europe désire se doter de règles s'adressant à certains risques importants créés spécifiquement par les SIA. Ainsi, la *Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union* impose certaines obligations spécifiques aux entreprises désireuses de créer ou d'utiliser les SIA qu'elle qualifie «à haut risque»[65].

Dans tous les cas, tous ces régimes réclament une réactivité des acteurs qui diffèrent en fonction de l'importance des risques ou des préjudices appréhendés.

57 *Id.*, p. 15.

58 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 35(1).

59 *Id.* art 34.

60 *Id.*

61 Ministre de l'innovation, des sciences et de l'industrie, *Projet de loi C-11 : 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*, (2020), Deuxième session, (Quarante-troisième législature, 69 Elizabeth II, 2020). art 58(1) et 58(3).

62 PL64, préc., note 1 art 103 (nouvel article 3.5. de la LPRPSP).

63 *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 (Règlement général sur la protection* des données) (RGPD), préc., note 16., art 35.

64 Voir notamment, PL64, préc., note 1 art 103 (nouvel article 3.3. de la LPRPSP).

65 Commission Européenne, Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, (2021) 206 final. art 6.

B.2.4.A. Probabilité

Évaluation de la probabilité. L'évaluation de la probabilité du risque réclame d'évaluer les *chances que le risque se manifeste*[66]. Cette évaluation sera très souvent une appréciation approximative puisque l'évaluateur ne p eut pas espérer connaître toutes les variables pouvant influencer cette probabilité.

Système de notation. L'évaluateur devrait assigner une note décrivant à la probabilité du risque. Nous proposons un système de notation basé sur trois notes :

Basse (1) : Il est impossible ou improbable que le risque se concrétise.

Modérée (2) : Il est possible voir probable que le risque se concrétise.

Élevée (3) : Il est très probable que le risque se concrétise.

À noter que l'évaluateur peut, s'il le désire, utiliser ou emprunter un autre système de notation. Le *Guide d'accompagnement* de la Commission d'accès à l'information par exemple, propose un système d'évaluation distinct[67].

B.2.4.B. Impact

Évaluation de l'impact. PL64 propose une liste non exhaustive de caractéristiques à prendre en considération lors de l'évaluation du risque soit :

1. la *sensibilité* des renseignements concernés ;
2. la *probabilité que les renseignements concernés soient utilisés à des fins préjudiciables* et
3. les *conséquences appréhendées* de leur utilisation[68].

Nous proposons de qualifier l'évaluation de ces caractéristiques sous l'appellation : **évaluation de *l'impact du risque***[69].

1) Sensibilité des renseignements

Sensibilité : première composante de l'analyse de l'impact. PL64 indique que le caractère «sensible» du renseignement influence l'évaluation du risque de préjudice[70]. PL64 définit un renseignement *sensible* comme un renseignement suscitant un «haut degré d'attente raisonnable en matière de vie privée»[71]. L'évaluation de la sensibilité du renseignement doit se faire au regard (i) de la *nature* du renseignement et (ii) du *contexte* de sa collecte, de sa communication ou de son utilisation[72].

i. La nature

La nature du renseignent. PL64 et C-11 n'énumèrent pas toutes les catégories de renseignements qui sont, par leur nature, sensibles ou délicates. Il est néanmoins possible de mobiliser d'autres instruments juridiques tels que la LPRPDE ainsi que les décisions de la *CAI*, du *Commissariat à la protection de la vie privée du Canada* et des tribunaux afin d'identifier les renseignements disposant d'une nature sensible.

66 Commission d'accès à l'information du Québec, préc., note 18, p. 20.
67 *Id.*
68 Voir PL64, préc., note 1, art 103 (nouvel article 3.7 de la LPRPSP).
69 Nous empruntons la même appellation que la CAI. Voir Commission d'accès à l'information du Québec, préc., note 18, p. 19.
70 C-11 utilise le terme "délicat" plutôt que "sensible". Voir, par e.g., *Projet de loi C-11 : 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*, préc., note 61. art 9, 12, 15 .
71 Voir PL64, préc., note 1, art 110 (nouvel article 12 de la LPRPSP).
72 *Id.*

Exemples de renseignements par nature sensibles. Ainsi, les sources susmentionnées considèrent (ou ont considéré) que les renseignements suivants sont, par leur nature, sensibles :

- les informations médicales[73] ;
- les renseignements financiers[74] ;
- les identifiants gouvernementaux uniques comme le numéro d'assurance sociale[75] ;
- les données biométriques[76] ;
- les données de géolocalisation[77] ;
- les origines ethniques et raciales[78] ;
- les opinions politiques[79] ;
- la vie sexuelle ou l'orientation sexuelle[80] et
- les croyances religieuses ou philosophiques[81].

73 Voir par exemple : *Id.* ; *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, en ligne : https://www.canlii.org/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html?resultIndex=1 (consulté le 4 octobre 2021), art. 4.3.4. de l'Annexe 1., Commissaire à la protection de la vie privée, 7 février 2018, 2018-006, *Rapport de conclusions d'enquête en vertu de la LPRPDE no 2018-006*, par. 55 (consulté le 4 octobre 2021), *Compagnie des chemins de fer nationaux du Canada*, 2012 Tribunal de santé et sécurité au travail Canada, par. 24, en ligne : https://canlii.ca/t/gh3z4 (consulté le 4 octobre 2021)., *Dossier : 1011656-S (Ministère de la Santé et des Services sociaux et Régie de l'assurance maladie du Québec)*, 2018 Commission d'accès à l'information du Québec aux paras 27, 54 et 55.

74 *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 73. art. 4.3.4. de l'Annexe 1., *Enquête sur la conformité d'Equifax Inc. et d'Equifax Canada à la LPRPDE à la suite de l'atteinte à la sécurité des renseignements personnels en 2017*, 2019 Commissaire à la protection de la vie privée, par. 19, en ligne : https://canlii.ca/t/hzzpj (consulté le 4 octobre 2021)., *Un homme s'oppose à ce que des travailleurs assignés temporairement traitent les renseignements liés à la paye*, 2003 Commissaire à la protection de la vie privée, 2, en ligne : https://canlii.ca/t/1ngzz (consulté le 4 octobre 2021)., *Une institution financière prend de vigoureuses mesures correctives après que des mesures de sécurité insuffisantes et un stockage inutile ont rendu vulnérables aux atteintes à la vie privée des données sensibles*, 2015 Commissaire à la protection de la vie privée, par. 30, en ligne : https://canlii.ca/t/gnmbx (consulté le 4 octobre 2021)., *Banque Royale du Canada c. Trang*, [2016] 2 RCS 412, par. 36 (Cour suprême du Canada), en ligne : https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/16242/index.do (consulté le 4 octobre 2021). et *M'Boutchou c. Banque de Montréal*, 2008 Cour supérieure, par. 51, en ligne : https://canlii.ca/t/21pbr (consulté le 4 octobre 2021).

75 *Lévy c. Nissan Canada inc.*, 2019 Cour supérieure, par. 72, en ligne : https://canlii.ca/t/j2klc (consulté le 4 octobre 2021). et *Rapport de conclusions d'enquête en vertu de la LPRPDE no 2007-389 : TJX Companies Inc./Winners Merchant International L.P.*, 2007 Commissariat à la protection de la vie privée du Canada, par. 41, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2007/tjx_rep_070925 (consulté le 4 octobre 2021).

76 PL64, préc., note 1, art 110 (nouvel article 12 de la LPRPSP); Commission d'accès à l'information du Québec, « Biométrie » (24 mars 2021), en ligne : https://www.cai.gouv.qc.ca/biometrie/ (consulté le 4 octobre 2021). ; *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1, en ligne : http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/C-1.1 (consulté le 4 octobre 2021). aux art 43, 44 et 45., Commission d'accès à l'information du Québec, Borris Perron et Éric Singh, *Rapport d'inspection concernant le système de carte OPUS de la société de transport de Montréal*, Dossier 11 04 88, 2012. et *Un manufacturier de jouets connectés améliore les mesures de sécurité pour protéger adéquatement les renseignements d'enfants*, 2018 Commissaire à la protection de la vie privée, par. 21, en ligne : https://canlii.ca/t/hrvj9 (consulté le 4 octobre 2021).

77 *Loi concernant le cadre juridique des technologies de l'information*, préc., note 76. art 43 al 2., Commission d'accès à l'information du Québec, Borris Perron et Éric Singh, *Rapport d'inspection concernant le système de carte OPUS de la société de transport de Montréal*, Dossier 11 04 88, 2012. et *Un manufacturier de jouets connectés améliore les mesures de sécurité pour protéger adéquatement les renseignements d'enfants*, préc., note 76, par. 21.

78 Commissariat à la protection de la vie privée du Canada, « Position de principe sur la publicité comportementale en ligne » (4 décembre 2015), en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/ (consulté le 4 novembre 2021).

79 *Id.*

80 *Id.*

81 *Id.*

Exemples de renseignements peu sensibles. En revanche, les renseignements suivants ont été identifiés comme étant de nature «peu sensibles»:

- les adresses électroniques d'usagers (sauf elles permettent à elles seules d'identifier la personne concernée ou certains de ses renseignements personnels)[82];
- les noms et prénoms d'usagers[83].

ii. Le contexte

Le contexte : composante de la sensibilité. Le contexte de la communication ou de l'utilisation d'un renseignement[84] peut également renforcer ou diminuer sa sensibilité[85].

Le tout est supérieur à la somme de ses parties. Ainsi, bien que la Loi spécifie que l'on doit évaluer la sensibilité du renseignement[86], il convient plutôt d'évaluer la sensibilité du renseignement au regard de l'ensemble de données qui l'accompagne. En effet, un ensemble de renseignements peut être sensible même si individuellement les renseignements qui le composent ne le sont pas.

Exemple de contextes pertinents. La *Loi sur la protection des renseignements personnels et les documents électroniques* indique que les renseignements d'identification comme le nom et le prénom ne sont pas, en soi, sensibles dans un contexte où ils permettraient d'identifier un abonné à une revue générale d'information[87]. En revanche, dans son enquête sur Ashley Madison (un site de rencontre entre personnes infidèles) le commissaire à la protection de la vie privée du Canada a identifié que les noms et prénoms des abonnés de ce site devaient être considérés sensibles en raison du contexte[88]. Cela s'expliquait, d'une part, par la nature du site et des activités de ses usagers[89], mais également par le fait que l'entreprise «faisait valoir la discrétion et la sécurité offertes à ses utilisateurs en tant qu'aspect clé de ses services»[90].

---

82 *Une enquête révèle que Facebook n'a pas obtenu le consentement des non-membres en vue de l'utilisation de leurs adresses électroniques pour leur proposer des amis*, 2012 Commissaire à la protection de la vie privée, par. 45, en ligne : https://canlii.ca/t/fr2gg (consulté le 4 octobre 2021). *Enquête conjointe sur Ashley Madison menée par le commissaire à la protection de la vie privée du Canada et le commissaire à la protection de la vie privée/commissaire à l'information par intérim de l'Australie*, 2016 Commissaire à la protection de la vie privée, par. 57 et 75, en ligne : https://canlii.ca/t/h3p5k (consulté le 4 octobre 2021).

83 *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 73. art 4.3.4. (Annexe 1). ET *Enquête conjointe sur Ashley Madison menée par le commissaire à la protection de la vie privée du Canada et le commissaire à la protection de la vie privée/commissaire à l'information par intérim de l'Australie*, préc., note 82, par. 57. et *Wajam Internet Technologies Inc.*, 2017 Commissaire à la protection de la vie privée, en ligne : https://canlii.ca/t/hrvhw (consulté le 4 octobre 2021).

84 PL64, préc., note 1, art 110 (nouvel article 12 de la LPRPSP).

85 Par exemple, si les renseignements concernent des enfants. Voir par e.g. *Un manufacturier de jouets connectés améliore les mesures de sécurité pour protéger adéquatement les renseignements d'enfants*, préc., note 76, par. 21. et *Banque Royale du Canada c. Trang*, préc., note 74, par. 45-50.

86 Voir par exemple PL64, préc., note 1, art 111 (nouvel article 17 de la LPRPSP).

87 *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 73. à l'art 4.3.4. (Annexe 1).

88 *Enquête conjointe sur Ashley Madison menée par le commissaire à la protection de la vie privée du Canada et le commissaire à la protection de la vie privée/commissaire à l'information par intérim de l'Australie*, préc., note 82, par. 47.

89 *Id.*

90 *Id.*, par. 50.

DISTINCTIONS AVEC LE RÉGIME EUROPÉEN

L'évaluation de la «sensibilité» du renseignement

Comme les régimes québécois et canadien, le régime européen prend en considération la «sensibilité» des renseignements[91]. Le RGPD identifie très clairement quels sont les renseignements qu'il considère «sensibles». Ainsi, le RGPD prévoit des «catégories particulières de données à caractère personnel»[92] qu'elle qualifie de «données sensibles»[93]. Ces dernières sont :

- l'origine «raciale» ;
- les opinions politiques ;
- les convictions religieuses ou philosophiques ;
- l'appartenance syndicale ;
- les données génétiques ;
- les données biométriques aux fins d'identifier une personne physique de manière unique ;
- les données concernant la santé ;
- les données concernant la vie sexuelle

ET

- les données concernant l'orientation sexuelle d'une personne physique[94].

Le RGPD prévoit également des normes spécifiques aux données relatives aux condamnations pénales et aux infractions[95]. Le RGPD prohibe l'usage de ces données sauf si l'une des exceptions prévues par la Loi s'applique[96].

La clarté du RGPD contraste très fortement avec le traitement de la sensibilité par les régimes canadien et québécois. En effet, PL64 et C-11 n'énumèrent pas les renseignements qu'ils considèrent «sensibles», ce qui impose à ceux qui utilisent ou recueillent des renseignements personnels la charge d'évaluer eux-mêmes la sensibilité des renseignements. Or, les critères fixés par les projets de loi pour guider cette évaluation sont, eux-mêmes, assez vagues.

Ainsi, PL64 propose d'évaluer la sensibilité individuelle d'un renseignement au regard d'un critère polymorphique et évolutif soit le «haut degré d'attente raisonnable en matière de vie privée»[97]. À noter toutefois, qu'un amendement au projet de loi a précisé que ce «haut degré d'attente raisonnable en matière de vie privée» pouvait résulter de la «nature notamment médicale, biométrique ou autrement intime» d'un renseignement[98].

Similairement, C-11 ne définit pas ce qu'il considère être un renseignement «délicat». Plus encore, ce projet de loi identifie que certaines règles s'appliquent au regard de «renseignements médicaux de nature délicate»[99], ce qui sous-entend logiquement qu'il existe des renseignements médicaux de nature non délicate[100].

À ce titre, l'approche européenne est beaucoup plus claire et exhaustive que les approches canadienne et québécoise. En fait, le Commissariat à la vie privée du Canada reconnaissait lui-même en 2018 qu'en droit canadien: «il n'y a pas de ligne de démarcation nette pour déterminer si un renseignement est sensible ou non.»[101]

---

91 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16. au préambule 51.

92 *Id.* art. 9 et 10.

93 *Id.* au préambule 10.

94 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16. art 9(1).

95 PL64, préc., note 1, art 110 (nouvel article 12 de la LPRPSP).

96 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16. art 9 et 10.

97 PL64, préc., note 1, art 110 (nouvel article 12 de la LPRPSP).

98 *Id.*

99 *Projet de loi C-11 : 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*, préc., note 61, p. 11. art 66 (3).

100 *Id.*

101 Commissariat à la protection de la vie privée du Canada, «Lignes directrices pour l'obtention d'un consentement valable» (24 mai 2018), en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/ (consulté le 4 novembre 2021).

Les problématiques visées par la sensibilité

Le concept de «sensibilité» identifiée en Europe n'adresse pas les mêmes problématiques qu'au Québec et au Canada. En effet, en Europe, les catégories de données sensibles réfèrent principalement à des motifs de discriminations généralement reconnus par les instruments juridiques nationaux et internationaux[102]. À ce titre, le concept de sensibilité, et les obligations prévues par le RGPD à l'égard des données sensibles visent principalement à protéger des personnes appartenant à des groupes vulnérables des risques de discriminations illégitimes ou arbitraires[103].

Au Québec et au Canada, les renseignements présentant des risques de discriminations tels que l'origine ethnique et les affiliations politiques ont également été considérés comme étant sensibles[104]. Cependant, le fait que certains renseignements tels que les informations financières, les données de géolocalisation et le numéro d'assurance sociale soient considérés comme étant par nature «sensibles» implique que les droits québécois et canadien conceptualisent différemment la sensibilité des renseignements et incorporent des considérations qui dépassent largement les risques de traitements discriminatoires.

Le régime québécois diffère dans la mesure où le concept de sensibilité est principalement affaire de sécurité des renseignements personnels puisque les lois en cause ne traitent que de la seule protection des renseignements. Ceci nous ramène à la difficile question de la portée limitée des lois québécoises et canadiennes qui traitent principalement du respect de la vie privée alors que le RGPD envisage une protection plus large fondée sur les droits et libertés fondamentales.

102 Voir par exemple : Union Européenne, *Charte des droits fondamentaux de l'Union Européenne*, Journal officielle de l'Union Européenne, C 326/391, Doc ID: 12012P/TXTDoc Sector: 1Doc Title: Charte des droits fondamentaux de l'Union européenne, en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A12012P%2FTXT (consulté le 4 octobre 2021). art 21; Conseil de l'Europe, *Convention européenne des droits de l'homme*, en ligne : https://www.echr.coe.int/documents/convention_fra.pdf (consulté le 4 octobre 2021). art 14 et Nations Unies, *Pacte international relatif aux droits civils et politiques*, 16 décembre 1966, en ligne : https://www.ohchr.org/fr/professionalinterest/pages/ccpr.aspx (consulté le 4 octobre 2021). art 4. Québec, *Charte des droits et libertés de la personne*, (1975), C-12. art 10 et Canada, *Annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11 | Loi constitutionnelle de 1982*, (1982) c 11, en ligne : https://www.canlii.org/fr/ca/legis/lois/annexe-b-de-la-loi-de-1982-sur-le-canada-r-u-1982-c-11/derniere/annexe-b-de-la-loi-de-1982-sur-le-canada-r-u-1982-c-11.html (consulté le 4 octobre 2021) art 15.

103 Jean-Marc Van Gyseghem, « Les catégories particulières de données à caractère personnel », dans *Le règlement général sur la protection des données (RGPD/GDPR)*, coll. Cahiers du CRIDS, Bruxelles, Larcier, 2018, p. 255-284 à la p. 255.

104 Par exemple : *Enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet d'AggregateIQ Data Services Ltd.*, 2019 Commissaire à la protection de la vie privée, par. 70, 75, en ligne : https://canlii.ca/t/j3lsr (consulté le 4 octobre 2021).

2) Probabilité que le renseignement soit utilisé à des fins préjudiciables

Probabilité de fins préjudiciables. Le second élément à étudier lors de l'évaluation de l'impact est la *probabilité que le renseignement soit utilisé à des fins préjudiciables*. Celle-ci réfère à la probabilité que le renseignement, une fois le risque concrétisé, puisse causer un préjudice pour l'individu concerné. À ce titre, il importe de distinguer l'étude de la *probabilité que le renseignement soit utilisé à des fins préjudiciables* de l'étude de la *probabilité du risque* susmentionnée. Cette dernière réfère plutôt aux chances que le risque se manifeste.

Exemple de la distinction. Prenons, à titre d'exemple, un serveur informatique hébergeant des données financières très sensibles, mais qui dispose de très bonnes sécurités visant à contrer les intrusions. En pareilles circonstances, la *probabilité du risque* d'intrusions sera probablement *basse*, mais l'impact du risque peut être important parce que la *probabilité que le renseignement soit utilisé à des fins préjudiciables* comme un vol d'identité peut se révéler élevée.

3) Conséquences appréhendées

Conséquences appréhendées. Finalement, l'évaluation de *l'impact* implique d'évaluer les *conséquences appréhendées* de l'incident de confidentialité.

Exemples. La fraude, le vol d'identité, la création d'un sentiment d'intrusion chez la personne concernée, l'impact sur le dossier de crédit et les sollicitations non désirées sont tous des conséquences possibles de la concrétisation d'un risque[105].

4) Autres considérations

Liste de considérations non exhaustive. PL64 identifie que la liste des trois considérations susmentionnées (soit la *sensibilité,* la *probabilité que le renseignement soit utilisé à des fins préjudiciables* et les *conséquences appréhendées*) n'est pas exhaustive[106]. À ce titre, d'autres éléments peuvent affecter l'*impact* appréhendé d'un risque. PL64 n'identifie pas quels sont ces autres éléments. Cependant, nous sommes d'avis que le *nombre de personnes pouvant être affectées* constitue une autre considération pouvant influencer l'*impact* du risque. En effet, le *Guide d'accompagnement* de la CAI identifie que le nombre de personnes affectées doit être pris en considération lors de l'évaluation de l'impact du risque[107]. De plus, l'article 150 de PL64 identifie que le «nombre de personnes affectées concernées par le manquement»[108] doit être pris en considération lors de l'imposition de sanctions contre une personne ayant contrevenu à ses obligations sous PL64.

5) Catégorisation de l'impact

Catégorisation de l'impact. Nous proposons plutôt d'identifier si l'impact du risque est :

Bas (1) : Le risque concrétisé n'affectera ou ne préjudiciera pas les personnes concernées de façon importante ou ne les affectera pas du tout.

Modéré (2) : Le risque concrétisé affectera ou préjudiciera modérément les personnes concernées.

Élevé (3) : Le risque concrétisé affectera ou préjudiciera les personnes concernées de façon importante.

---

105 Commission d'accès à l'information du Québec, préc., note 18, p. 17. quoique la CAI identifie certains de ces exemples comme des "impacts potentiels."

106 PL64, préc., note 1, art 103 (nouvel article 3.7. de la LPRPSP).

107 Commission d'accès à l'information du Québec, préc., note 18, p. 19.

108 La *quantité* des renseignements affectés par un potentiel incident de confidentialité doit également être prise en considération lors de la détermination des mesures de sécurité appropriées (PL64, préc., note 1, art 159 (nouvel article 90.2. de la LPRPSP). et *Loi sur la protection des renseignements personnels dans le secteur privé*, chapitre P-39.1. art 10.

B.2.4.C. Catégorisation des risques

Catégorisation des risques. À l'instar du d.pia.lab, nous recommandons d'assigner une cote intégrant l'évaluation de la probabilité et de l'impact du risque. Ainsi, nous proposons d'identifier si le risque est :

Bas (1)

Modéré (2)

Élevé (3)

B.2.5. Identification de recommandations

Recommandations de mesures. L'évaluateur peut émettre des recommandations visant à réduire le risque évalué et les décrire, s'il y a lieu.

B.2.6. Évaluation du risque résiduel

Risque résiduel. Après l'évaluation des risques et l'établissement des mesures visant à éliminer ou amoindrir ces risques, l'évaluateur doit analyser la présence de risques résiduels, c'est-à-dire les risques qui existent malgré l'application des recommandations. L'évaluateur doit inscrire l'échelle du risque résiduel et sous-diviser ce dernier au regard de sa probabilité et de son impact.

B.3. Présentation des sections

B.3.1. Représentation par tableau

Utilité des tableaux. Nous proposons d'utiliser des tableaux afin de représenter les différents éléments susmentionnés. Cette pratique, inspirée du d.pia.lab[109] permet de présenter succinctement et efficacement les éléments désirés.

B.3.2. Recenser les normes applicables

Normes applicables. Tel qu'identifié, avant de procéder à l'évaluation des risques, l'évaluateur doit recenser les normes s'appliquant au projet. L'Annexe attachée au présent document identifie plusieurs normes pertinentes à l'évaluation.

109 D. Kloza, A. Calvi, S. Casiraghi, S. V. Maymir et N. Ioannidis, préc., note 22, 40.

B.3.3. Tableau de gestion des risques

Gestion des risques et recommandations. Nous proposons le tableau suivant à des fins de présentation de l'évaluation du risque et des recommandations.

ÉVALUATION DU RISQUE				
Risque	**Mesures implémentées**	**Probabilité**	**Impact**	**Échelle du risque**
[Appellation du risque identifié]: [Description du risque identifié et de ses causes.]	[Mesures imposées]	[Basse / Modérée / Élevée] [Justification]	[Bas / Modéré / Élevé] [Justification au regard de: A. La sensibilité des renseignements B. Les probabilités d'utilisations préjudiciables C. Les conséquences appréhendées]	[Bas / Modéré / Élevé]

RECOMMANDATIONS			
Mesures recommandées	**Probabilité résiduelle**	**Impact résiduel**	**Échelle du risque résiduel**
[Mesures à imposer]	[Basse / Modérée / Élevée] [Justification]	[Bas / Modéré / Élevé] [Explication]	[Bas / Modéré / Élevé]

I. La responsabilité

1. Objectifs de la section

Identifier les responsables et leurs responsabilités. Dans cette section, l'évaluateur doit identifier les organisations et les individus responsables de la protection des renseignements personnels. À ce titre, il est nécessaire d'assigner clairement les responsabilités des différentes personnes et acteurs œuvrant au sein du projet : tant à l'interne de l'organisation, qu'à l'externe (e.g. la responsabilité des partenaires).

2. Considérations générales

a) Responsable de la protection des renseignements personnels

Identité du responsable. PL64 prévoit que le *Responsable de la protection des renseignements personnels* est la «personne ayant la plus haute autorité»[110] dans l'entreprise.

Responsable de la protection des renseignements personnels. Il convient d'identifier le ou la *Responsable de la protection des renseignements personnels,* et d'identifier s'il / elle dispose des pouvoirs nécessaires pour remplir son rôle et qu'il / elle comprend son rôle. Ce dernier(e) a, notamment, comme mandat de veiller au respect de la Loi et d'approuver des politiques et les pratiques de gouvernance sous-mentionnées.

Possible délégation. Cependant, le *Responsable de la protection des renseignements personnels* peut déléguer sa fonction par écrit. Ses responsabilités peuvent être déléguées à un membre de son personnel ou à une personne externe[111].

b) Gouvernance des renseignements personnels

Politiques et pratiques de gouvernance. L'organisation doit adopter et mettre en œuvre des politiques et pratiques encadrant la gouvernance à l'égard des renseignements personnels. Celles-ci doivent être «proportionnées à la nature et à l'importance des activités de l'entreprise»[112]. Elles doivent être «approuvées par le responsable de la protection des renseignements personnels.»[113]

Contenu des politiques et pratiques de gouvernance. Les politiques et pratiques de gouvernance doivent prévoir, entre autres[114] :

- l'encadrement applicable à la conservation et à la destruction de ces renseignements ;
- les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie des renseignements et
- un processus de traitement des plaintes relatives à la protection de ceux-ci[115].

110 PL64, préc., note 1. art 103 (nouvel article 3.1. de la LPRPSP).
111 *Id.* Voir les commentaires à l'amendement 55 dans Assemblée Nationale du Québec (Commission des institutions), *Étude détaillée du projet de loi n°64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Texte adopté avec des amendements),* Dépôt à l'Assemblée nationale : n°2702-20210914 (2021), 1 (42e Législature).
112 PL64, préc., note 1. art 103 (nouvel article 3.2. de la LPRPSP).
113 *Id.*
114 *Id.*
115 *Id.*

Limiter l'accès aux renseignements. L'organisation devrait prévoir limiter l'accès de ses préposés et agents aux renseignements personnels. À moins de consentement des personnes concernées ou d'exceptions prévues par la Loi, les préposés et agents de l'entreprise ne peuvent accéder qu'aux renseignements nécessaires à l'exercice de leurs fonctions[116].

c) Considérations externes

Évaluer les responsabilités des partenaires. Si le projet recourt à des partenaires, il convient d'évaluer si les responsabilités de chacun sont clairement identifiées dans les contrats. Si les partenaires exercent des responsabilités, il convient de les identifier.

Garde d'un document technologique. Si l'entreprise en charge du projet confie la garde d'un document technologique à un prestataire de service, celle-ci doit l'informer au préalable :

- de la «protection que requiert le document en ce qui a trait à la confidentialité de l'information»[117] et
- des «personnes habilitées à en prendre connaissance»[118] ;

3. Considérations propres aux SIA

Assigner un Responsable en IA. Tel qu'il sera démontré dans les sections subséquentes, l'usage d'une SIA présente des risques et des considérations qui leur sont propres. Pour cette raison, il est recommandé de nommer un(e) *Responsable en IA* qui aura la responsabilité d'identifier et de répondre aux risques s'y rapportant[119]. Il ou elle devrait :

- Détenir les connaissances et les compétences nécessaires pour comprendre le fonctionnement du SIA ;
- Détenir les connaissances et les compétences nécessaires pour détecter les incidents de confidentialité ;
- Détenir les connaissances, l'autorité et les compétences nécessaires pour identifier, comprendre et appliquer les mesures de sécurité appropriée et
- Détenir les connaissances, l'autorité et les compétences nécessaires pour altérer les résultats ou le fonctionnement du SIA si nécessaire.

Par défaut. Si l'organisation n'assigne pas de *Responsable de l'IA* alors ce poste est, par défaut, occupé par le *Responsable de la protection des renseignements personnels*[120].

116 *Id.* art 117 (nouvel article 20 de la LPRPSP).
117 *Loi concernant le cadre juridique des technologies de l'information*, préc., note 76. art 26
118 *Id.*
119 OBVIA, préc., note 44, 8.
120 *Id.*

II. La justification sociale

1. Objectifs de la section

Structure de la section. Cette section se sous-divise en deux parties. La première partie concerne l'évaluation de la justification sociale du projet dans son ensemble. La seconde se préoccupe de l'évaluation des opérations de collecte, d'utilisation, de communication, de conservation et de destruction affectant les renseignements personnels.

Objectifs de l'évaluation du projet. L'évaluation de la justification sociale du projet implique d'analyser les objectifs du projet. Elle réclame également d'identifier si ce que propose le projet est rationnellement lié aux objectifs précités. Finalement, il convient d'évaluer si le projet constitue une atteinte minimale à la vie privée des personnes concernées.

Objectifs de l'évaluation des opérations. L'évaluation des opérations implique, quant à elle, d'évaluer les fins des opérations affectant les renseignements personnels et d'évaluer la légalité des opérations de collecte, d'utilisation, de communication et de conservation.

Il convient également de souligner certaines considérations relatives au *consentement* et certaines obligations liées à la circulation des renseignements personnels à l'extérieur du Québec.

2. Considérations propres au projet

Établir l'existence d'objectifs. Le projet doit être motivé par un ou plusieurs objectifs. Ceux-ci ont déjà dû être identifiés dans la Partie A de l'évaluation.

Établir la légitimité des objectifs. Il convient d'évaluer si les objectifs du projet sont légitimes et se rapportent à des «préoccupations réelles et justifiables»[121]. Si l'objectif du projet est de répondre à une problématique particulière, il peut s'avérer utile de présenter des données probantes, des références à la littérature scientifique ou toute autre forme de documentation capable d'illustrer l'existence de la problématique.

Établir la proportionnalité du projet. Le projet doit privilégier une «solution proportionnée»[122] à ses objectifs. Similairement à la CAI, nous proposons d'évaluer le projet au regard de questionnements inspirés du test de la proportionnalité énoncé par la Cour suprême du Canada dans l'arrêt *R v Oakes* (1986)[123]. Ces questionnements sont :

- Existe-t-il un lien rationnel entre les objectifs du projet et les moyens prévus par ce dernier ? Ces moyens doivent être «ni arbitraires, ni inéquitables, ni fondés sur des considérations irrationnelles.»[124]
- Le projet est-il celui «de nature à porter le moins possible atteinte»[125] aux droits des personnes concernées ?
- Les effets des mesures restreignant le droit sont-ils proportionnels aux objectifs ?[126] Il s'agit ici de déterminer si les «avantages concrets surpassent les conséquences ou les préjudices pour les personnes concernées»[127].

121 Commission d'accès à l'information du Québec, préc., note 18, p. 4.
122 *Id.*
123 *R. c. Oakes*, [1986] 1 RCS 103 (Cour suprême du Canada), en ligne : https://canlii.ca/t/1ftv5 (consulté le 7 décembre 2021). para 70. et Commission d'accès à l'information du Québec, préc., note 18, p. 4.
124 *R. c. Oakes*, préc., note 123. para 70.
125 *Id.*
126 *Id.*
127 Commission d'accès à l'information du Québec, préc., note 18, p. 4.

Limites. Il n'appartient pas, à ce stade-ci de l'évaluation, de se prononcer extensivement sur les opérations prévues par le projet. L'évaluation devrait, si possible, se limiter à adresser le projet dans son ensemble.

Parties prenantes. Il peut également s'avérer utile d'identifier si l'entreprise en charge du projet a consulté des organismes ou des groupes de la société civile afin qu'ils puissent faire part de leurs inquiétudes face aux risques présentés par le projet. Une telle démarche peut faciliter l'identification des risques et des bénéfices présentés par le projet.

a) Existence d'un lien rationnel

Lien avec les objectifs. Analyser l'existence d'un lien rationnel consiste à identifier que les moyens utilisés peuvent réellement répondre aux objectifs précités. Par exemple, si l'objectif est de mieux connaitre sa clientèle, alors utiliser certains types de renseignements personnels en provenance de celle-ci est une démarche rationnelle. De plus, il convient d'évaluer si les fins déterminées des renseignements personnels (tel qu'identifié à la Partie A) sont rationnellement liées aux objectifs du projet dans son ensemble. Si le projet utilise des SIA, il peut être utile d'évaluer la solution au regard de la littérature scientifique ou de données probantes.

b) Atteinte minimale

Risque minimal. En l'espèce, il s'agit de déterminer si les objectifs du projet pourraient être accomplis par d'autres moyens qui seraient moins invasifs et moins risqués pour les personnes concernées. Si une alternative présente moins de risques pour les usagers que le projet étudié, il convient de proposer cette dernière, d'identifier pourquoi celle-ci n'est pas privilégiée et d'évaluer la justesse de cette justification.

c) Proportionnalité

Renvoie à la section C de l'évaluation. Nous proposons d'évaluer le troisième critère à la Partie C de la présente évaluation. En effet, l'objectif de l'EFCD est justement d'identifier les conséquences ou les préjudices potentiels qui pourraient affecter les personnes concernées. En d'autres termes, évaluer si le projet est *proportionnel* réclame d'effectuer, en grande partie, l'EFCD elle-même. À ce titre, il convient d'évaluer ce critère à la Partie C du document soit l'*Évaluation finale*.

3. Considérations propres aux opérations

Objectifs de la sous-section. L'évaluateur doit s'assurer que la collecte, l'utilisation, la communication, la conservation, la destruction et l'anonymisation des renseignements personnels répondent aux normes établies. Pour ce faire il convient, d'une part, d'évaluer les risques associés à chacune de ces opérations et, d'autre part, d'évaluer les risques liés aux opérations concernant des personnes ou des organismes situés à l'extérieur du Québec.

a) Collecte

Déterminer l'intérêt sérieux et légitime. L'évaluateur doit identifier si la collecte de renseignements personnels poursuit «un intérêt sérieux et légitime.»[128]

Identifier les fins. Les fins des renseignements personnels doivent être clairement identifiées et communiquées aux personnes concernées avant leurs collectes[129]. L'évaluateur a été appelé à identifier les fins des renseignements personnels à la Partie A.

128 *Code Civil du Québec*, CCQ-1991 516 (1991)., art 37. et PL64, préc., note 1, art 100 et 104 (nouveaux art. 1.1. et 4 de la LPRPSP).
129 PL64, préc., note 1. art 105 (nouvel article 5 de la LPRPSP).

Pertinence. Une fois ces fins identifiées, il convient d'évaluer si la collecte ne vise *que* des renseignements personnels *pertinents* aux fins désignées[130].

Nécessité. Seuls les renseignements personnels *nécessaires* à la réalisation des fins susmentionnées peuvent être recueillis[131]. Selon la CAI, il n'est pas possible de déroger au critère de nécessité, même si la personne concernée y consent[132]. La CAI identifie que, pour faire preuve de la nécessité, il convient de démontrer :

1. le caractère légitime, important, urgent et réel de la collecte[133] ;
2. la proportionnalité de l'atteinte à la vie privée[134] et les fins poursuivies soit :
    - que la collecte est rationnellement liée aux fins visées[135] ;
    - qu'il «n'existe pas d'autre solution raisonnable portant moins atteinte à la vie privée»[136] ;
    - «l'effet utile est plus grand que le préjudice susceptible d'être causé»[137]

Moyens licites. Les renseignements doivent être recueillis par des moyens licites[138].

Origine des renseignements. Les renseignements personnels doivent normalement être recueillis auprès de la personne concernée[139]. Cependant, les renseignements personnels peuvent être recueillis auprès de tiers si :

- la personne concernée **consent** à la collecte de ses renseignements auprès de tiers[140]. À noter que «le consentement à la communication par un tiers de renseignements personnels peut être donné par la personne concernée à la personne qui les recueille auprès de ce tiers»[141].

OU

130 Plus précisément le Code civil réclame de ne recueillir "que les renseignements pertinents à l'objet déclaré du dossier". *Code Civil du Québec*, préc., note 128., art 37.

131 PL64, préc., note 1. art 105 (nouvel article 5 de la LPRPSP).

132 Commission d'accès à l'information du Québec, « La collecte de renseignements personnels », en ligne : https://www.cai.gouv.qc.ca/la-collecte-de-renseignements-personnels/ (consulté le 10 mars 2022). et Commission d'accès à l'information du Québec, *Enquête à l'égard de 9055-4635 Québec inc. (Alimentation Larouche)*, par. 16-17, en ligne : https://decisions.cai.gouv.qc.ca/cai/ss/fr/item/500003/index.do (consulté le 19 janvier 2022).

133 Commission d'accès à l'information du Québec, *Enquête à l'égard de 9055-4635 Québec inc. (Alimentation Larouche)*, préc., note 132, par. 16-17.

134 *Id.*, par. 17.

135 Commission d'accès à l'information du Québec, « Fiche d'information sur les pièces d'identité : entreprises », p. 1, en ligne : https://www.cai.gouv.qc.ca/documents/CAI_FI_pieces_identite_entreprises.pdf (consulté le 20 janvier 2022).

136 *Id.* La CAI formule également le questionnement ainsi : «l'atteinte au droit à la vie privée est-elle minimisée?» Voir Commission d'accès à l'information du Québec, préc., note 132. Voir aussi : Commission d'accès à l'information du Québec, *Enquête à l'égard de 9055-4635 Québec inc. (Alimentation Larouche)*, préc., note 132. au para 33.

137 Commission d'accès à l'information du Québec, préc., note 135. Aussi formulée ainsi par la CAI :"la divulgation du renseignement requis est-elle nettement plus utile à l'entreprise que préjudiciable à la personne concernée». Voir Commission d'accès à l'information du Québec, préc., note 132. À noter que ces informations en provenance de la CAI datent d'avant la réforme apportée par PL64. Cependant, la modification de l'article 5 de la LPRPSP par PL64 ne semble pas, a priori, modifier substantiellement le critère de nécessité. Ces informations ont cependant été altérées par les auteurs afin de refléter la principale modification apportée à l'article soit que la nécessité doit dorénavant s'interpréter au regard des fins déterminées avant la collecte plutôt qu'au regard de l'objet du dossier.

138 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 5.

139 *Id.* art 6.

140 *Id.*

141 *Id.* art 15.

- la personne qui recueille le renseignement auprès d'un tiers dispose d'un **intérêt sérieux et légitime**[142] et :
  - «les renseignements sont recueillis **dans l'intérêt de la personne concernée** et ne peuvent être recueillis directement auprès de celle-ci dans un temps opportun»[143]

  ou

  - «la cueillette auprès d'un tiers est nécessaire pour s'assurer de **l'exactitude** des renseignements»[144].

OU

- la Loi autorise autrement la collecte auprès d'un tiers sans le consentement de la personne concernée.

Refus de service. Il n'est pas permis de refuser d'acquiescer à une demande de bien, de service ou d'emploi en raison du refus de fournir un renseignement personnel sauf si :

- «la collecte est nécessaire à la conclusion ou à l'exécution du contrat»[145] ;
- «la collecte est autorisée par la loi»[146]

OU

- «il y a des motifs raisonnables de croire qu'une telle demande n'est pas licite»[147].

Paramètres par défaut. Si le service ou le produit technologique offert au public dispose de paramètres de confidentialité, ceux-ci doivent, par défaut, assurer le plus haut niveau de confidentialité sans qu'une intervention de la personne concernée soit nécessaire[148]. Cette norme n'affecte toutefois pas les paramètres de confidentialité d'un témoin de connexion[149].

142 *Id.* art 6; *Code Civil du Québec*, préc., note 128. art 37. et PL64, préc., note 1, art 100 et 104 (nouveaux art. 1.1. et 4 de la LPRPSP).
143 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 6.
144 *Id.*
145 *Id.* art 9.
146 *Id.*
147 *Id.*
148 PL64, préc., note 1. art 108 (nouvel article 9.1. de la LPRPSP).
149 *Id.*

b) Utilisation

Limité aux fins déterminées avant la collecte. Il convient d'évaluer si le renseignement *n'est utilisé qu'*aux fins pour lesquelles il a été recueilli[150].

Exceptions. Si l'utilisation n'est pas réalisée aux fins pour lesquelles il a été recueilli alors il convient d'identifier si l'une des exceptions prévues par la Loi s'applique. Ainsi, PL64 prévoit que l'utilisation du renseignement personnel est permise dans l'une ou l'autre des circonstances suivantes :

- elle est à des «fins compatibles»[151] avec celles pour lesquelles il a été recueilli[152] ;
- elle est manifestement au bénéfice de la personne concernée[153] ;
- elle est nécessaire à des fins d'étude, de recherche ou de production de statistiques et le renseignement est dépersonnalisé[154] ;
- elle est nécessaire aux fins des pratiques administratives courantes de l'entreprise[155]
- elle poursuit des fins sérieuses et légitimes et que le renseignement est *anonymisé*[156]

OU

- la personne concernée y consent. Ce consentement «doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible»[157].

Anonymisation. Tel qu'identifié, la Loi permet l'utilisation du renseignement personnel sans le consentement de la personne concernée s'il est *anonymisé*. PL64 prévoit que le renseignement est *anonymisé* lorsqu'il «est, en tout temps, raisonnable de prévoir dans les circonstances [que le renseignement] ne permet plus, de façon irréversible, d'identifier directement ou indirectement [la personne concernée]»[158]. La Loi impose que les renseignements doivent être *anonymisés* selon les «meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement»[159].

Risques associés à l'anonymisation. Cependant, prétendre qu'un renseignement est *anonymisé* comporte des risques. Les critères fixés par la Loi pour pouvoir bénéficier de cette exception peuvent s'avérer difficiles à atteindre. En effet, lors des consultations portant sur l'adoption de PL64[160] certains intervenants, dont la CAI, ont identifié que l'anonymisation était «pratiquement impossible à atteindre»[161].

150 PL64, préc., note 1, art 110 (nouvel article 12 de la LPRPSP).
151 La Loi prévoit que «pour qu'une fin soit compatible [...], il doit y avoir un lien pertinent et direct avec les fins auxquelles le renseignement a été recueilli. Toutefois, ne peut être considérée comme une fin compatible la prospection commerciale ou philanthropique.»
152 PL64, préc., note 1, art 110 (nouvel article 12 de la LPRPSP). et *Code Civil du Québec*, préc., note 128., art 37.
153 PL64, préc., note 1. art 110 (nouvel article12 de la LPRPSP).
154 *Id.*
155 *Id.*
156 *Id.* art 119 (nouvel article 23 de la LPRPSP).
157 *Id.* art. 110 (nouveaux art. 12 de la LPRPSP). et *Code Civil du Québec*, préc., note 128. art. 37.
158 PL64, préc., note 1, art 119 (nouvel article 23 de la LPRPSP).
159 *Id.*
160 À noter que ces commentaires ne visaient pas la version finale de PL64. Des amendements seront apportés à l'article 111. Ces amendements viendront, par exemple, ajouter les critères de *raisonnabilité* («raisonnable de prévoir dans les circonstances») et de *permanence* («en tout temps») susmentionnés.
161 Voir, par exemple, Assemblée nationale du Québec, « Étude détaillée du projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels - 42e législature, 1re session (27 novembre 2018 au 13 octobre 2021) », *Journal des débats de la Commission des institutions* 45-96 (29 septembre 2020), en ligne : http://assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-200929.html (consulté le 3 décembre 2021).

C'est d'ailleurs en raison de ces interventions qu'un amendement a été apporté au projet de loi[162]. C'est cet amendement qui est à l'origine de l'étrange mention selon laquelle l'impossibilité d'identifier (de façon irréversible) la personne concernée devrait être «en tout temps, raisonnable de prévoir dans les circonstances»[163].

Afin de préciser l'intention derrière cet amendement, il convient de partager un commentaire émis par le *Ministre québécois responsable de l'Accès à l'information et la Protection des renseignements personnels* au cours d'échanges à l'Assemblée nationale. En effet, ce dernier a identifié : «qu'indépendamment du contexte, dans la mesure où je fais les *efforts raisonnables* pour anonymiser de façon irréversible, je serai dans le respect de la loi.»[164]

Critères d'anonymisation. Un processus *d'anonymisation* robuste devrait, au moins, respecter les trois critères suivants :

- **L'individualisation,** c'est-à-dire qu'il ne devrait pas être possible d'isoler ou d'identifier une personne directement ou indirectement à partir des renseignements[165].
- **La corrélation,** c'est-à-dire qu'il ne devrait pas être possible de «relier les ensembles de données distincts qui concernent une même personne.»[166]
- **L'inférence,** c'est-à-dire qu'il ne devrait pas être possible de «déduire de nouvelles informations sur une personne.»[167]

162 Assemblée nationale du Québec, « Étude détaillée du projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels », *Journal des débats de la Commission des institutions* 45-132 (31 mars 2021), en ligne : http://assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-210331.html (consulté le 21 janvier 2022).

163 PL64, préc., note 1, art 119 (nouvel article 23 de la LPRPSP).

164 Assemblée nationale du Québec, préc., note 162.

165 Gouvernement du Québec, « Destruction ou anonymisation » (23 novembre 2021), en ligne : https://www.quebec.ca/gouvernement/travailler-gouvernement/services-employes-etat/conformite/protection-des-renseignements-personnels/anonymisation/destruction-ou-anonymisation (consulté le 21 janvier 2022); ARTICLE 23 DATA PROTECTION WORKING PARTY, *Opinion 05/2014 on Anonymisation Techniques*, WP216, 0829/14/EN, Bruxelles, Commission européenne, 2014, en ligne : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

166 *Id.*

167 *Id.*

DISTINCTIONS AVEC LE RÉGIME EUROPÉEN

Un renseignement anonymisé est-il un renseignement personnel ?

Il est très clair sous le régime européen qu'un renseignement personnel anonymisé ne peut pas être considéré comme une donnée à caractère personnel[168]. En conséquence, le RGPD n'impose pas le respect des principes relatifs à la protection des données aux données anonymisées[169].

Cette conclusion est logique puisque les données à caractère personnel sont définies par le RGPD comme des informations se «rapportant à une personne physique identifiée ou identifiable»[170]. Or, pour qu'il y ait anonymisation d'une donnée, celle-ci ne doit plus permettre d'identifier la personne concernée[171]. En conséquence, une donnée anonymisée ne peut être, par définition, une donnée à caractère personnel.

En contrepartie, au Québec, l'article 119 de PL64[172] indique que même anonymisé, un renseignement n'échappe pas complètement aux obligations imposées par la LPRPSP. En effet, comme pour les renseignements personnels, un renseignement anonymisé ne peut être utilisé qu'à des «fins sérieuses et légitimes»[173]. Pourtant l'article 1 de la LPRPSP indique clairement que la Loi s'applique aux renseignements *personnels*. Or, les renseignements anonymisés, qui se définissent par leur incapacité à identifier la personne concernée, ne peuvent, logiquement, répondre à la définition de *renseignements personnels*. En effet, les *renseignements personnels* se définissent par leur capacité à identifier la personne physique concernée par le renseignement[174]. À ce titre, les renseignements anonymisés qui concernent une personne physique semblent bénéficier d'un statut particulier sous PL64. D'une part, ils ne peuvent répondre, logiquement, à la définition de *renseignement personnel,* mais, d'autre part, ils n'échappent pas totalement à certaines obligations imposées par LPRPSP.

168 ARTICLE 23 DATA PROTECTION WORKING PARTY, préc., note 165. ; Athena BOURKA, Prokopios DROGKARIS et Ioannis AGRAFIOTIS, *Pseudonymisation techniques and best practices: recommendations on shaping technology according to data protection and privacy provisions.*, Agence de l'Union européenne pour la cyber-Sécurité (ENISA), 2019, p. 13, en ligne : https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119810ENN (consulté le 28 octobre 2021). ; *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, (24 octobre 1995), 281 (OJ L), en ligne : http://data.europa.eu/eli/dir/1995/46/oj/fra (consulté le 12 mars 2022).

169 *Id* ; *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16. préambule 26.

170 *Id.* art 4(1).

171 A. Bourka, P. Drogkaris et I. Agrafiotis, préc., note 168, p. 13.

172 Voir Assemblée Nationale du Québec, « Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels - Amendements », voir p. 82 du document «Amendements adoptés - PL 64», en ligne : http://assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html (consulté le 19 janvier 2022).

173 PL64, préc., note 1, art 119 (nouvel article 23 de la LPRPSP).

174 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 2.

c) Communication

Communications. Ensuite, il convient d'évaluer si les renseignements sont *communiqués* à des tiers et si ces communications sont permises[175].

Consentement. Sauf exception, la personne concernée doit consentir aux communications de ses renseignements personnels[176].

Exemple d'exception : la transaction commerciale. Cependant, il est permis de communiquer des renseignements personnels sans le consentement de la personne concernée dans le cadre d'une transaction commerciale lorsque :

- Ce renseignement est **nécessaire** aux «fins de la conclusion d'une transaction commerciale à laquelle [la personne qui exploite une entreprise] entend être partie»[177] ;
- Une **entente** est conclue avec l'autre partie. Cette entente doit stipuler que la partie s'engage à :

  a. n'utiliser le renseignement **qu'aux seules fins de la conclusion** de la transaction commerciale»[178] ;

  b. à «**ne pas communiquer le renseignement** sans le consentement de la personne concernée»[179] ou l'autorisation de la LPRPSP ;

  c. à prendre «les **mesures** nécessaires pour assurer la protection du **caractère confidentiel** du renseignement»[180] ;

  d. à **détruire** le renseignement si :

  - la transaction commerciale n'est pas conclue ou si
  - l'utilisation du renseignement «n'est plus nécessaire aux fins de la transaction commerciale»[181].

Si, une fois la transaction commerciale conclue, la partie qui s'est vue communiquer un renseignement personnel désire continuer d'utiliser le renseignement ou le communiquer, celle-ci doit :

- dans un délai raisonnable après la conclusion de la transaction commerciale, «aviser la personne concernée qu'elle détient un renseignement personnel la concernant en raison de la transaction»[182]

ET

- n'utiliser ou ne communiquer le renseignement que «conformément à la LPRPSP»[183] ;

175 *Code Civil du Québec*, préc., note 128., art 37. et PL64, préc., note 1, aux art 110-118 (Art 13 à 21.0.2 LPRPSP).
176 *Id.*
177 PL64, préc., note 1, art 115 (nouvel article 18.4 de la LPRPSP).
178 *Id.*
179 *Id.*
180 *Id.*
181 *Id.*
182 *Id.*
183 *Id.*

Exemple d'exception : le mandat, le contrat de service ou d'entreprise. Il est également permis de communiquer des renseignements personnels sans le consentement de la personne concernée lorsque :

- Ce renseignement est **nécessaire** «à l'exercice d'un **mandat** ou à **l'exécution d'un contrat de service** ou **d'entreprise**»[184] que la personne qui exploite une entreprise confie à la personne ou l'organisme à qui le renseignement est communiqué ;
- Le mandat ou le contrat est confié par **écrit**[185] ;
- Le mandat ou le contrat inscrit les **mesures** que le mandataire ou l'exécutant du contrat doit prendre :
    a. «pour assurer la **protection** du caractère **confidentiel** du renseignement personnel communiqué»[186] ;
    b. «pour que ce renseignement ne soit **utilisé** que dans l'exercice de son mandat ou l'exécution de son contrat»[187] ;
    c. pour que le mandataire ou exécutant ne **conserve** pas le renseignement après son expiration[188] ;

Ces mesures n'ont pas à être inscrites si le mandataire ou l'exécutant est un organisme public[189] ou un membre d'un ordre professionnel.

- En retour, le mandataire ou l'exécutant doit :
    a. «**aviser** sans délai le responsable de la protection des renseignements personnels de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué»[190] ;
    b. «permettre au responsable de la protection des renseignements personnels d'effectuer toute **vérification** relative à cette confidentialité»[191].

d) Conservation, destruction et anonymisation

Conservation limitée. Finalement, l'évaluateur doit identifier si les renseignements sont bel et bien *détruits* ou *anonymisés* après l'accomplissement de leurs fins tel que le requiert la Loi[192]. Si tel n'est pas le cas, l'évaluateur doit an analyser si les délais prévus bénéficient d'un délai de conservation prévu par une loi.

Durée. Selon la CAI, le délai de conservation d'un renseignement n'a pas nécessairement besoin de préciser un nombre précis de jours, de mois ou d'années. Le délai peut référer «à un événement déterminé ou [à] une situation précise.»[193]

Obligation de conservation. Il convient également d'identifier si la Loi impose un délai de conservation spécifique à un renseignement personnel et si ce délai est respecté. Par exemple, lorsqu'un renseignement personnel est utilisé dans le cadre d'une décision exclusivement automatisée alors ce dernier doit être conservé pendant au moins un an suivant la décision[194].

184 *Id.* art 115 (nouvel article 18.3 de la LPRPSP).
185 *Id.*
186 *Id.*
187 *Id.*
188 *Id.*
189 Plus précisément un organisme public "au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*". Voir *Id.*
190 *Id.*
191 *Id.*
192 *Id.* art 119 (nouvel article 23 de la LPRPSP).
193 Commission d'accès à l'information du Québec, préc., note 50.
194 PL64, préc., note 1. art 109 (nouvel article 11 de la LPRPSP).

DISTINCTIONS AVEC LE RÉGIME EUROPÉEN

Normes applicables au «traitement» ou à des opérations spécifiques

La notion de «traitement» est centrale au RGPD. Le RGPD entend comme «traitement» : «toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel»[195]. La notion regroupe donc, entre autres[196] :

- la collecte ;
- l'enregistrement ;
- l'organisation ;
- la conservation ;
- la consultation ;
- l'utilisation ;
- la communication par transmission ;
- l'effacement ;
- la destruction.

Les normes prévues par le RGPD s'appliquent généralement aux «traitements» des données et, donc, à l'ensemble des opérations susmentionnées[197].

La notion de «traitement» est absente de PL64[198]. En conséquence, les normes imposées par PL64 s'appliquent à des opérations spécifiques. Ainsi, le projet de loi prévoit des normes, parfois distinctes, pour la communication[199], la collecte[200], la conservation[201], la destruction[202] et l'utilisation[203] des renseignements personnels.

C-11 prévoyait lui-aussi appliquer des normes spécifiques à la collecte[204], à l'utilisation[205] ou à la communication[206] des renseignements personnels.

195 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 4.

196 *Id.*

197 Voir par exemple, *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 6 et 9 À noter que ce n'est pas toujours le cas. Par exemple, des obligations sont prévues spécifiquement pour la collecte et la conservation des données. Voir par exemple, *Id.*, art 5(1)(b) et 5(1)(e).

198 À noter toutefois que PL64 utilise le terme "traitement" dans les normes prévue aux décisions fondées exclusivement sur un *traitement* automatisé. Voir par e.g. PL64, préc., note 1, art 102 (nouvel article 12 de la LPRPSP).

199 Voir par exemple, *Id.* art 111 (nouvel article 17 de la LPRPSP).

200 Voir par exemple, *Id.* art 107 et 111 (nouvel article 8 et 17 de la LPRPSP).

201 Voir par exemple, *Id.* art 103, 110 et 111 (nouveaux art. 3.2., 21.02. et 23 de la LPRPSP).

202 Voir par exemple, *Id.* art 103 et 118 (nouvel article 3.2. et 21.0.2. de la LPRPSP).

203 Voir par exemple, *Id.* art 119 (nouvel article 22 de la LPRPSP).

204 Voir par exemple, *Projet de loi C-11 : 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*, préc., note 61. art 13.

205 Voir par exemple, *Id.*, art 21, 30 et 38.

206 Voir par exemple, *Id.*, art 31 à 37 et 39.

e) Consentement

De l'importance du consentement. Tel qu'identifié, les opérations concernant les renseignements personnels réclament souvent d'obtenir le consentement de la personne concernée[207]. L'évaluateur doit donc comprendre ce qu'est un consentement valide au regard de la LPRPS afin d'évaluer convenablement la légalité et les risques liés aux opérations qui réclament le consentement de la personne concernée.

Caractéristiques des consentements. Un consentement doit être :

1. **Manifeste** : «c'est-à-dire évident, certain et indiscutable»[208] ;
2. **Libre** : «c'est-à-dire être donné sans contrainte»[209] ;
3. **Éclairé** : «c'est-à-dire qu'il doit être précis, rigoureux et spécifique»[210] . La personne concernée doit donc être en mesure de porter jugement éclairé sur la portée du consentement. Cela impose donc d'indiquer :
    - quels renseignements seront communiqués et/ou utilisés ;
    - à qui ces renseignements seront communiqués et/ou pour qui ceux-ci seront utilisés ;
    - les raisons pour lesquelles le renseignement est communiqué et/ou utilisé ;
    - comment le renseignement est communiqué et/ou utilisé ;
    - quelles seront les conséquences de ces communications et/ou de ces utilisations[211] ;
4. Donné **à des fins spécifiques**. Le consentement doit être demandé à des fins spécifiques et pour chacune de ces fins[212].

ET

5. **Limité dans le temps**. En effet, «le consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé»[213].

207 Voir, par exemple : Code Civil du Québec, préc., note 128., art 37 ; PL64, préc., note 1, art. 110 (nouvel article 14 LPRPS). et COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, préc., note 50.
208 PL64, préc., note 1, art. 110 (nouvel article 14). et COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, préc., note 50.
209 PL64, préc., note 1, art 110 (nouvel article 14 de la LPRPSP).
210 PL64, préc., note 1, art. 110 (nouvel article 14). et COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, préc., note 50.
211 *Id.*
212 PL64, préc., note 1, art 110 (nouvel article 12 et 14 de la LPRPSP).
213 *Id.* et COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, préc., note 50.

Clairement et distinctement. Le consentement doit être formulé en termes simples et clairs[214]. Lorsque la demande de consentement est faite par écrit, elle doit être demandée distinctement de toute autre information communiquée à la personne concernée[215].

Consentement exprès pour les renseignements sensibles. L'utilisation et la communication des renseignements «sensibles» pour d'autres fins que celles pour lesquelles il a été recueilli réclament un consentement «manifesté de façon expresse»[216]. Selon la CAI, un consentement exprès doit être «explicite et sans équivoque, donné par un geste positif manifestant clairement l'accord.»[217]

Interaction avec le principe de Transparence. Finalement, PL64 prévoit que si la personne concernée fournie ses renseignements après avoir été informée des droits et informations mentionnés aux points 2.2. et 2.3. de la prochaine section portant sur la *Transparence*, alors elle consent à leur utilisation et à leur communication pour les fins auxquelles ces renseignements ont été recueillis[218].

Obligation d'assistance. L'organisation doit prêter assistance à la personne concernée qui le requiert afin de l'aider à comprendre la portée du consentement demandé[219].

Conséquences d'un consentement invalide. Un consentement qui n'est pas donné conformément aux normes édictées par la LPRPSP est sans effet[220].

Droit de retirer son consentement. Une personne concernée peut retirer son consentement à la communication ou à l'utilisation des renseignements recueillis[221].

214 PL64, préc., note 1, art. 110 (nouvel article 14 de la LPRPSP).
215 *Id.*
216 PL64, préc., note 1, art. 110 (nouvel article 12 et 13 de la LPRPSP).
217 Commission d'accès à l'information du Québec, « Le consentement à l'utilisation de la biométrie », en ligne : https://www.cai.gouv.qc.ca/biometrie/le-consentement-a-lutilisation-de-la-biometrie/ (consulté le 4 novembre 2021).
218 PL64, préc., note 1, art 107 (nouvel article 8.3.).
219 *Id.* art. 110 (nouvel article 12 de la LPRPSP).
220 *Id.* art. 110 (nouvel article 14 de la LPRPSP).
221 *Id.* art. 107 (nouvel article 8 de la LPRPSP).

DISTINCTIONS AVEC LE RÉGIME EUROPÉEN

Ce qu'est le consentement

La forme que doit prendre le consentement diffère grandement entre les régimes québécois et européen. En effet, le RGPD prévoit que tout consentement doit être donné «par un acte positif clair»[222]. Ainsi, en Europe, il ne pourrait y avoir de consentement en cas de «silence, de cases cochées par défaut ou d'inactivité»[223].

Au Québec, le consentement ne se fait pas toujours au terme d'un acte positif. En effet, le consentement *positif* est caractéristique des consentements dits *exprès*[224]. Ainsi, la CAI définit le consentement exprès comme un consentement «explicite et sans équivoque, donné par un geste positif manifestant clairement l'accord.»[225] Similairement, le Gouvernement du Québec soutient que le consentement exprès «exige un acte positif de la personne, soit une action volontaire, comme le fait de remplir un formulaire, de répondre par l'affirmative à une question ou de cocher une case»[226].

En fait, le consentement au Québec ne réfère pas tout à fait à la même notion qu'en Europe. En effet, non seulement le consentement ne se fait pas toujours au terme d'un acte positif, mais en plus, dans plusieurs circonstances, le «consentement» requis par la Loi renvoie davantage à une obligation d'information que d'une véritable nécessité d'obtenir une manifestation de la volonté de la personne concernée.

Ainsi, la Loi québécoise impose d'aviser la personne concernée de certaines informations suivant le nouvel article 8 de la LPRPSP (identifiées aux points 2.2. et 2.3. de la prochaine section portant sur la *Transparence*)[227]. Si la personne concernée est validement informée de ces informations, alors la Loi prévoit qu'elle «consent» à l'utilisation et à la communication des renseignements personnels aux fins qui leur sont prévues[228].

Une intervention de la présidente de la CAI, Me Diane Poitras, lors des auditions publiques sur PL64, résume très bien la place réservée au consentement sous le régime québécois :

- [...] même si le consentement conserve une place importante, la loi prévoit déjà d'autres bases juridiques autorisant la collecte, l'utilisation ou la communication de renseignements personnels. Les modifications proposées par le projet de loi vont dans le même sens.
- Par exemple, le consentement n'est pas requis pour recueillir un renseignement auprès de la personne concernée. Une entreprise doit avoir un intérêt sérieux et légitime pour recueillir des renseignements personnels. Elle doit déterminer, avant leur collecte, à quelles fins elles serviront et ne recueillir que les renseignements nécessaires à ces finalités. Elle en informe la personne concernée. Ce n'est donc que si une entreprise souhaite utiliser les renseignements personnels qu'elle détient à de nouvelles fins ou les communiquer à des tiers qu'elle doit obtenir le consentement de la personne concernée[229]. (soulignements ajoutés par les auteurs)

222 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., au préambule 32.

223 *Id.*, au préambule 32. PL64, préc., note 1, art 102 (nouvel article 12 et 13 de la LPRPSP).

224 Commission d'accès à l'information du Québec, préc., note 217.

225 *Id.*

226 Gouvernement du Québec, « Renseignements personnels sensibles », en ligne : https://www.quebec.ca/gouvernement/travailler-gouvernement/services-employes-etat/conformite/protection-des-renseignements-personnels/consentement/renseignements-personnels-sensibles (consulté le 4 novembre 2021).

227 PL64, préc., note 1, art 107 (nouveaux articles 8 à 8.3. de la LPRPSP).

228 *Id.* art 107 (nouvel article 8.3. de la LPRPSP).

229 « Consultations particulières et auditions publiques sur le projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels », (2020) 45-96 *Journal des débats de la Commission des institutions*, en ligne : http://assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-200929.html (consulté le 19 janvier 2022).

Ce qu'est un consentement exprès

Il est clair, à la vue de ce qui précède, que l'Europe et le Québec n'accordent pas le même sens au caractère «exprès» d'un consentement. Tel qu'identifié, la notion de consentement «exprès» est, au Québec, intrinsèquement lié à la manifestation du consentement par un «geste positif clair»[230]. Or, tel qu'indiqué dans les *Lignes directrices sur le consentement au sens du règlement 2016/679* rédigées par le Groupe de travail «Article 29», «le RGPD stipule qu'une «déclaration ou un acte positif clair» est une condition *sine qua non* d'un consentement «standard»»[231]. Recueillir le consentement dit «explicite» ou «exprès» d'une personne concernée réclame donc davantage que la manifestation d'un geste positif clair. Selon le Groupe de travail, Il convient, par exemple, de réclamer une déclaration écrite signée par la personne concernée[232]. À ce titre, il faut se garder de conclure qu'un consentement considéré «exprès» au Québec serait nécessairement considéré comme tel en Europe.

Droit de retirer son consentement

PL64 et le RGPD reconnaissent tous les deux un droit de retirer son consentement dans certaines circonstances[233]. Or, contrairement à PL64, le RGPD identifie très clairement qu'il doit être «aussi simple de retirer que de donner son consentement»[234].

f) Personnes et organismes hors Québec

Communications et opérations confiées à une personne à l'extérieur du Québec. Communiquer des renseignements personnels à une personne ou à un organisme à l'extérieur du Québec ou confier à ceux-ci la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte des renseignements personnels réclame de procéder à une EFVP et d'être lié à ce tiers par une entente écrite[235]. L'EFVP doit considérer :

- la sensibilité du renseignement ;
- la finalité du renseignement ;
- les mesures de protection qui seront imposées au renseignement

ET

- le régime juridique de l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables.

La communication ou l'attribution de tâche peut procéder si[236]. :

- «l'évaluation démontre que le renseignement bénéficierait d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus»[237] ;

ET

- la tâche fait l'objet d'une entente écrite qui tient compte notamment :
  - des résultats de l'évaluation et
  - «le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation»[238].

230 Gouvernement du Québec, préc., note 226.
231 Groupe de travail « Article 29 », *Lignes directrices sur le consentement au sens du règlement 2016/679*, 17/FR, p. 21, en ligne : https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf (consulté le 4 novembre 2021).
232 *Id.*
233 PL64, préc., note 1, art 107 et 119 (nouvel article 8 et 22 de la LPRPSP). et *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 7.
234 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 7.
235 PL64, préc., note 1, art 111 (nouvel article 17 de la LPRPSP).
236 *Id.*
237 *Id.*
238 *Id.*

III. La transparence

1. Objectifs de la section

Évaluer la transparence. La présente section vise à évaluer les problématiques liées à la diffusion des informations auprès du public et des personnes concernées. Dans cette section, l'évaluateur sera également appelé à évaluer du respect des droits d'accès des personnes concernées.

2. Transparence auprès des personnes concernées

Principaux objectifs de la transparence. L'évaluation des obligations relevant de la transparence auprès des usagers s'intéresse principalement à :

1. Informer convenablement les personnes concernées des fins du projet et des opérations prévues ;
2. Informer les personnes concernées de leurs droits à l'égard des renseignements personnels et à l'égard du processus auquel ils sont soumis ;
3. Informer les personnes concernées de l'usage de certaines technologies ;
4. Assurer le respect du droit d'accès des personnes concernées

ET

5. Diffuser une politique de confidentialité en termes simples et clairs[239].

2.1. Informer les personnes concernées de la politique de confidentialité

Informations sur le site Internet. Toute personne qui recueille par un moyen technologique des renseignements personnels doit publier sur le site Web de son entreprise et diffuser par «tout moyen propre à atteindre les personnes concernées»[240] les informations suivantes :

1. la politique de confidentialité écrite

ET

2. les avis identifiant toutes modifications apportées à la politique de confidentialité.

Ces informations doivent être rédigées en termes simples et clairs.

239 *Id.* art 107 (nouvel article 8.2.).
240 *Id.*

2.2. Informer les personnes concernées des fins et des moyens

Informations communiquées lors de la collecte et sur demande. Lors de la collecte des renseignements et sur demande, l'organisation doit informer les personnes concernées :

1. des fins auxquelles ces renseignements sont recueillis ;
2. des moyens par lesquels les renseignements sont recueillis ;
3. du nom des tiers ou des catégories de tiers pour qui la collecte est faite (si applicable) ;
4. du nom des tiers à qui il est nécessaire de communiquer les renseignements pour la réalisation des fins des renseignements (si applicable)[241]

ET

5. de la possibilité que les renseignements soient communiqués à l'extérieur du Québec (si applicable)[242].

Informations communiquées sur demande. L'organisation doit également communiquer certaines informations si la personne concernée en fait la demande. L'organisation doit donc indiquer à la personne concernée :

1. quels sont les renseignements personnels recueillis auprès d'elle ;
2. quelles sont les catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise ;
3. qu'elle est la durée de conservation de ces renseignements ;
4. quelles sont les coordonnées du *Responsable de la protection des renseignements personnels* ;

ET

5. quelle est la source des renseignements recueillis, si ceux-ci ont été recueillis auprès d'une autre personne qui exploite une entreprise[243].

Termes simples et clairs. Ces informations doivent être transmises à la personne concernée en termes simples et clairs, et ce, «quel que soit le moyen utilisé pour recueillir les renseignements»[244].

2.3. Informer les personnes concernées de leurs droits

Informer des droits. L'évaluateur doit également s'assurer que l'organisation informe les personnes concernées de certains droits. Ainsi, les personnes concernées doivent être informées lors de la collecte et sur demande :

1. de leur droit d'accès ;
2. de leur droit de rectification ;

ET

3. de leur droit de retirer leur consentement à la communication et à l'utilisation des renseignements recueillis[245].

241 Commission d'accès à l'information du Québec, « Transparence », en ligne : https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/transparence/ (consulté le 4 novembre 2021). et PL64, préc., note 1, art 107 (nouvel article 8 de la LPRPSP).
242 PL64, préc., note 1, art 107 (nouvel article 8 de la LPRPSP).
243 *Id.* art 106-107 (nouveaux art. 7 et 8 de la LPRPSP).
244 *Id.* art 107 (nouvel article 8 de la LPRPSP).
245 *Id.*

Termes simples et clairs. Comme les renseignements susmentionnés, PL64 prévoit que ces informations doivent être communiquées à la personne concernée en termes simples et clairs, et ce, «quel que soit le moyen utilisé pour recueillir les renseignements»[246].

Droit de retirer son consentement. Les personnes concernées doivent pouvoir retirer leur consentement à la «communication ou à l'utilisation des renseignements recueillis»[247].

Fins commerciales et philanthropiques. La personne qui exploite une entreprise et qui utilise des renseignements personnels à des fins de prospection commerciale ou philanthropique doit «s'identifier auprès de la personne à qui elle s'adresse et l'informer de son droit de retirer son consentement à ce que les renseignements personnels la concernant soient utilisés à ces fins».[248] Si la personne concernée retire son consentement, alors les renseignements personnels ne peuvent plus être utilisés à de telles fins[249].

2.4. Informer de l'usage de certaines technologies

Technologies d'identification, de localisation et de profilage. PL64 réclame à la personne «qui recueille des renseignements personnels auprès de la personne concernée en ayant recours à des technologies qui permette de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci»[250] de l'informer du recours à cette technologie ainsi que des «moyens offerts, le cas échéant, pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage»[251]. Ces informations doivent parvenir à la personne concernée *avant* la collecte ou l'utilisation des renseignements[252].

Décision fondée exclusivement sur un traitement automatisé. Si l'entreprise utilise des renseignements personnels afin de rendre des décisions fondées exclusivement sur un traitement automatisé alors la personne concernée doit en être informer «au plus tard au moment où elle l'informe de cette décision»[253].

2.5. Droit d'accès

Contenu du droit d'accès. Le droit d'accès consiste, d'une part, à confirmer auprès de la personne concernée que l'organisation détient des renseignements personnels la concernant[254] et, d'autre part, de lui donner accès à ces renseignements en lui fournissant une copie s'il en fait la demande[255].

Délais. Le *Responsable de la protection des renseignements personnels* doit répondre à la demande d'accès, par écrit, «au plus tard dans les 30 jours de la date de réception de la demande»[256].

Gratuit. Une personne désireuse de consulter les renseignements personnels la concernant «soit pour prendre une décision à son égard, soit pour informer un tiers» doit pouvoir le faire gratuitement[257]. Elle peut également faire reproduire un dossier qu'une autre personne détient sur elle «moyennant des frais raisonnables.»[258]

246 *Id.*
247 *Id.*
248 *Id.* art 119 (nouvel article 22 de la LPRPSP).
249 *Id.*
250 *Id.* art 107 (nouvel article 8.1. de la LPRPSP).
251 *Id.*
252 *Id.*
253 *Id.* art 110 (nouvel article 12.1. de la LPRPSP).
254 *Code Civil du Québec*, préc., note 128. art. 38 et PL64, préc., note 1, art 120 (nouvel article 27 de la LPRPSP).
255 PL64, préc., note 1, art 120 (nouvel article 27 de la LPRPSP). À noter que la Loi habilite d'autres personnes que la personne concernée à bénéficier d'un droit d'accès à certains renseignements sous certaines circonstances. Voir notamment *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 27 et PL64, préc., note 1, art 120 (nouvel article 27 de la LPRPSP).
256 PL64, préc., note 1, art 124 (nouvel article 32 de la LPRPSP).
257 *Code Civil du Québec*, préc., note 128. art. 38.
258 *Id.*

Accessible et intelligible. Les renseignements personnels communiqués à la personne concernée doivent être écrits de façon accessible «dans une transcription intelligible»[259]. Si le demandeur le réclame, les renseignements personnels doivent être communiqués dans un format technologique structuré et couramment utilisé à moins que cela ne crée des difficultés pratiques sérieuses[260].

Exceptions. La Loi prévoit qu'il est possible de refuser l'accès sous certaines circonstances telles que :

- la présence d'un intérêt sérieux et légitime à refuser l'accès

ou

- ces renseignements sont susceptibles de nuire sérieusement à un tiers[261].

3. Transparence auprès du public

Transparence auprès du public. Cette section réfère aux informations qui visent à informer le public ou le public des politiques, des mesures et des incidents affectant les renseignements personnels.

Normes impératives. Les informations suivantes doivent être publiées, par écrit, sur le site Internet de l'entreprise :

1. Les informations détaillées au sujet des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels[262] et
2. Le titre et les coordonnées du *Responsable de la protection des renseignements personnels*[263].

En l'absence de site Internet, ces informations doivent être diffusées par tout autre moyen approprié[264].

Politiques et pratique encadrant la gouvernance. Les politiques et pratiques encadrant la gouvernance à l'égard des renseignements personnels publiés doivent prévoir les éléments susmentionnés dans la section portant sur la Responsabilité.

Traitement des plaintes. Un processus de traitement des plaintes relatives à la protection des renseignements personnels doit être disponible. Les politiques et pratiques encadrant la gouvernance à l'égard des renseignements personnels doivent prévoir ce processus[265].

Incidents présentant des risques de préjudice sérieux. Finalement, la Loi prévoit qu'en cas d'incident de confidentialité présentant un risque de préjudice sérieux, la personne qui exploite une entreprise doit aviser, avec diligence, la CAI et toute «personne dont un renseignement personnel est concerné par l'incident»[266]. Elle doit également communiquer à toutes personnes ou tous organismes susceptibles de diminuer le risque, en ne leur communiquant que les renseignements nécessaires à la diminution du risque sans consentement de la personne concernée[267]. Le *Responsable de la protection des renseignements personnels* doit enregistrer cette communication[268].

259 *Id.*
260 PL64, préc., note 1, art 103 et 112 (nouvel article 3.3 et 27 de la LPRPSP).
261 *Code Civil du Québec*, préc., note 128. art. 38.
262 PL64, préc. note 1, art. 103 (nouvel article 3.2).
263 *Id.* art. 103 (nouvel article 3.1).
264 *Id.* art. 103 (nouvel article 3.1. et 3.2).
265 *Id.* art. 103 (nouvel article 3.2).
266 *Id.* art. 103 (nouvel article 3.5 de la LPRPSP).
267 *Id.*
268 *Id.*

IV. La sécurité

1. Objectifs de la section

Évaluer la sécurité. La Loi prévoit l'obligation de prendre des mesures de sécurité «propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits»[269].

2. Considérations générales

Raisonnabilité des mesures. Les mesures de sécurité doivent être raisonnables compte tenu :

- de la sensibilité des renseignements ;
- de la finalité de l'utilisation des renseignements ;
- de la quantité de renseignements ;
- de la répartition des renseignements

ET

- de leur support[270].

Évaluer la sécurité tout au long du cycle de vie. L'évaluateur doit s'assurer de la sécurité du renseignement à toutes les étapes de son cycle de vie.

Types de risques. La sécurité englobe donc plusieurs types de risques incluant ceux associés aux cyberattaques visant à *accéder* aux renseignements personnels, aux cyberattaques ou problèmes techniques pouvant *empêcher l'accès* aux renseignements personnels (e.g. *ransomware* ; destruction physique d'un serveur), aux cyberattaques visant à *altérer* les renseignements personnels, etc. Les risques identifiés peuvent être de nature physique, telle qu'une interruption du service en raison d'une perte d'électricité ou d'une destruction des serveurs, ou informatique tels qu'une cyberattaque.

Évaluer les risques liés aux incidents de confidentialité. L'évaluateur devra analyser les risques liés aux incidents de confidentialité, ce qui implique nécessairement d'évaluer les risques liés:

- aux *accès* non autorisés par la loi ;
- aux *utilisations* non autorisées par la loi ;
- aux *communications* non autorisées par la loi

ET

- aux *pertes* imprévues ou non autorisées d'un renseignement personnel.

269 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 10.
270 *Id.*

Types de mesures. Des mesures doivent être prévues afin, notamment :

1. de détecter les incidents de confidentialité ;
2. de répondre de façon appropriée aux incidents de confidentialité ;
3. d'enregistrer les incidents de confidentialité[271] ;
4. de contrôler et limiter l'accès aux renseignements confidentiels[272] ;
5. de diminuer les probabilités des risques ;

ET

6. de limiter leurs impacts.

Actions requises en cas d'incidents de confidentialité. Une personne qui exploite une entreprise et qui a des motifs de croire que s'est produit un incident de confidentialité doit :

- «prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé»[273] ;
- «éviter que de nouveaux incidents de même nature ne se produisent»[274]

ET

- inscrire l'incident dans un *Registre des incidents de confidentialités*[275] ;

Actions requises en cas de risques de préjudices sérieux. Cependant, si un incident présente des risques de préjudices sérieux aux personnes concernées, alors la personne qui exploite une entreprise doit :

- aviser la Commission d'accès à l'information avec diligence[276] ;

ET

- «aviser toute personne dont un renseignement personnel est concerné par l'incident»[277].

Origines des risques. Les risques évalués visent :

- les risques *externes* tels que l'accès non autorisé aux renseignements personnels par un tiers ;
- les risques *internes* créés par un manquement ou une action de *l'entreprise* en soi ou par des actions des membres du personnel ;

ET

- les risques créés par les *partenaires* de l'entreprise (tels que les sous-traitants).

Dépersonnalisation des renseignements personnels. Une méthode simple et efficace visant à limiter les risques liés à un renseignement personnel est de *dépersonnaliser* ce dernier. La dépersonnalisation implique de s'assurer que le renseignement ne permet plus d'identifier *directement* la personne concernée[278].

271 PL64, préc., note 1, art 103 (nouvel article 3.5. de la LPRPSP).
272 *Loi concernant le cadre juridique des technologies de l'information*, préc., note 76. art 25.
273 PL64, préc., note 1, art 103 (nouvel article 3.5. de la LPRPSP).
274 *Id.*
275 *Id.* art 103 (nouvel article 3.8. de la LPRPSP).
276 *Id.* art 103 (nouvel article 3.5. de la LPRPSP).
277 *Id.*
278 *Id.* art 110 (nouvel article 12 de la LPRPSP).

Remplacer des données d'identification comme le nom et prénom d'un usager par un identifiant alphanumérique permet de dépersonnaliser le renseignement. Il importe toutefois que l'identifiant ne soit pas produit à partir des renseignements personnels de la personne concernée. Évitez, par exemple, d'assigner un identifiant composé des initiales et de la date de naissance de la personne concernée. Il conviendrait plutôt de choisir l'identifiant grâce à une fonction de compteur, un générateur de nombres pseudo aléatoire ou une fonction de hachage cryptographique[279].

Empêcher la réidentification. Toute utilisation de renseignements dépersonnalisés doit s'accompagner de «mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés»[280].

Anonymisation des renseignements personnels. Il est également possible *d'anonymiser* des renseignements personnels pour leur assurer une plus grande sécurité. Cependant, tel qu'identifié, il convient de faire preuve de prudence avant d'indiquer qu'un renseignement est *anonymisé* au regard de PL64.

3. Considérations propres aux SIA

Risques spécifiques aux SIA. Des mesures de sécurité propres aux SIA doivent être prévues. En effet, ces dernières présentent des risques de sécurité qui leur sont spécifiques tels que :

- *Les risques liés aux membership inference attacks qui permettent d'identifier la présence de renseignements personnels d'une personne spécifique dans les données d'entrainement d'une SIA*[281] *;*
- *Les risques liés aux* attaques par inversion de modèle qui permet d'inférer des données d'entrainement d'une SIA[282] ;
- *Les risques liés à* l'empoisonnement des données d'entrainement *d'une SIA* en y injectant des échantillons trompeurs[283] («*Data poisoning*») ;
- Les attaques d'évasion qui consistent à modifier légèrement les données que les SIA cherchent à catégoriser dans l'objectif de la tromper («*Evasion attacks*»)[284]…

Assistance du responsable de l'IA. Le *responsable de l'IA* identifié dans la section *La responsabilité* doit assister les démarches de l'évaluateur visant à identifier les risques qui y sont liés à l'usage des SIA et les mesures pouvant les adresser.

279 A. BOURKA, P. DROGKARIS et I. AGRAFIOTIS, préc., note 168, p. 24 et s.
Techniquement, ENISA identifie ces mesures dans le cadre de la pseudonymisation des renseignements personnels. Cependant, tel que susmentionné, la *pseudonymisation* tel que comprise par le RGPD est très similaire au concept de *dépersonnalisation* en droit québécois.

280 PL64, préc., note 1, art 110 (nouvel article 12 de la LPRPSP).

281 Michael VEALE, Reuben BINNS et Lilian EDWARDS, « Algorithms that remember: model inversion attacks and data protection law », (2018) 376-2133 Philos Trans A Math Phys Eng Sci 20180083, 5, DOI : 10.1098/rsta.2018.0083.
Voir également : Hongsheng HU, Zoran SALCIC, Gillian DOBBIE et Xuyun ZHANG, «Membership Inference Attacks on Machine Learning: A Survey», arXiv:2103.07853 [cs] 2021, 1, en ligne : http://arxiv.org/abs/2103.07853 (consulté le 1 octobre 2021).

282 M. Veale, R. Binns et L. Edwards, préc., note 281.
Voir aussi: Matt Fredrikson, Somesh Jha et Thomas Ristenpart, « Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures », 2015.12. et Ximeng Liu, Lehui Xie, Yaopeng Wang, Jian Zou, Jinbo Xiong, Zuobin Ying et Athanasios V. Vasilakos, « Privacy and Security Issues in Deep Learning: A Survey », (2021) 9 *IEEE Access*, 4567, doi : 10.1109/ACCESS.2020.3045078.

283 X. Liu et al., préc., note 282, 4568.

284 *Id.*

V. L'explicabilité

1. Objectifs de la section

Définir le principe d'explicabilité. L'organisation doit être en mesure de fournir des explications suffisantes et compréhensibles à ses usagers. Le principe d'explicabilité se distingue de la transparence en ce qu'il se préoccupe plutôt à s'assurer que la personne concernée comprenne les informations qui lui sont fournies dans un contexte particulier, soit celui des décisions fondées exclusivement sur un traitement automatisé.

Définir «décision fondée exclusivement sur un traitement automatisé». PL64 n'identifie pas ce qu'est une «décision fondée exclusivement sur un traitement automatisé»[285]. Cependant, le gouvernement du Québec a publié un billet sur l'impact d'amendements à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* qui concerne les décisions fondées exclusivement sur un traitement automatisé[286]. Ainsi, une décision fondée exclusivement sur un traitement automatisé est une décision prise sans «qu'aucune personne physique n'a exercé un contrôle important dans la décision»[287] (soulignement ajouté par les auteurs). À ce titre, prévoir une intervention humaine mineure qui ne pourrait avoir de répercussion réelle sur la décision ne permet pas de se soutirer des obligations liées aux traitements exclusivement automatisés[288]. Cependant, le billet indique également qu'un «outil d'aide à la décision»[289] ne saurait être considéré comme une «décision fondée exclusivement sur un traitement automatisé» puisqu'il «ne rend aucune décision»[290].

Au regard de ce qui précède, il convient d'identifier que les SIA ne peuvent pas toutes être reconnues comme des décisions fondées exclusivement sur un traitement automatisé. Concurremment, les décisions fondées exclusivement sur un traitement automatisé ne sont pas toutes produites par des SIA.

Selon nous, pour produire une «décision» au sens de la Loi, la détermination prise par la SIA doit pouvoir préjudicier la personne concernée ou, minimalement, produire un effet qui pourrait justifier sa révision par un individu. Nous ne pensons pas qu'une SIA ayant comme objectif de hausser la résolution d'images, aussi sensibles soient-elles, pourrait être considérée comme productrice de «décisions» au sens de la Loi. Cette conclusion est cohérente au regard des droits et devoirs conférés par PL64 à l'égard des décisions fondées exclusivement sur un traitement automatisé. Les obligations liées à l'explicabilité ne peuvent, selon nous, s'interpréter isolément des autres droits conférés à l'égard des décisions fondées exclusivement sur un traitement automatisé tel que le droit de pouvoir «présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision»[291].

285 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 12.1.
286 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, chapitre A-2.1. art. 65.2.
287 Gouvernement du Québec, préc., note 42.
288 *Id.*
289 *Id.*
290 *Id.*
291 PL64, préc., note 1. art. 110 (nouvel article 12.1. de la LPRPDE).

2. Processus décisionnels exclusivement automatisés

Contenu du principe. PL64 réclame de l'exploitant d'une entreprise qui utilise des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé[292] de fournir, entre autres, à la demande de la personne concernée les informations suivantes :

- d'indiquer, avant ou au moment de la décision, à la personne concernée que ses renseignements sont soumis à un processus décisionnel exclusivement automatisé[293] ;
- les renseignements utilisés pour rendre la décision[294] ;
- les raisons, les principaux facteurs et les principaux paramètres ayant mené à la décision[295]

ET

- dans les cas où un profilage de la personne concernée est effectué, l'entreprise doit l'informer du recours à cette technologie et l'informer des moyens offerts pour désactiver cette fonction, le cas échéant[296].

Éléments à évaluer. Nous recommandons donc à l'évaluateur d'analyser :

- si la personne concernée est convenablement informée que ses renseignements sont soumis à un processus décisionnel exclusivement automatisé ;
- si une explication à la fois compréhensible et exacte du fonctionnement du processus automatisé utilisé est fournie à la personne concernée ;
- si cette explication décrit convenablement les capacités et des limites de la technologie utilisée ;
- si cette explication identifie les renseignements ou catégories de données utilisées par le processus exclusivement automatisé ;
- si cette explication justifie l'utilisation de ces mêmes catégories de données dans la prise de décision ;
- s'il existe, dans les cas où un profil est établi et utilisé, une explication quant au à la pertinence de ce profil dans le processus décisionnel[297]. En pareilles circonstances, l'évaluateur doit également s'assurer que l'entreprise respecte ses obligations liées à l'utilisation de technologies de profilage (voir section Transparence)

ET

- si les principaux paramètres et principaux facteurs de la technologie ont été communiqués «de manière significative, simple et claire»[298].

La précision absolue n'est pas réclamée. Il ne s'agit pas ici de fournir une explication capable de vulgariser parfaitement et scientifiquement le processus décisionnel automatisé. En effet, si la prise de décision automatisée est faite par un SIA, la description explicite du processus d'une SIA peut s'avérer incompréhensible pour certaines personnes. Il suffit de produire des explications suffisantes permettant de comprendre la «logique» derrière la décision automatisée[299]. L'explication devrait, entre autres, permettre aux personnes concernées de prendre des décisions éclairées quant à l'exercice de leurs autres droits, notamment leur droit de demander une révision de la décision.

---

292 *Id.*
293 *Id.*
294 *Id.*
295 *Id.*
296 *Id.* art 107 (nouvel article 8.1. de la LPRPDE).
297 OBVIA, préc., note 44, 26.
298 *Id.*
299 *Id.*, 26-27.

Utiliser des outils pédagogiques. Il peut s'avérer opportun, dans certaines circonstances, d'utiliser des techniques interactives et des visualisations telles que des schémas, des tableaux ou des graphiques, afin de faciliter la compréhension de la technologie utilisée.

Politique interne. Il peut être approprié de prévoir dans les politiques internes de l'organisation une définition de ce que l'entreprise entend par «explicabilité». Il peut également s'avérer utile d'identifier dans ces mêmes politiques à «quels moments une explication des procédures techniques [devient] nécessaire afin d'assurer la compréhension par la personne concernée.»[300]

Processus fournis par des tiers. Le fait que l'organisation utilise un SIA ou un traitement automatisé fourni par un tiers ne libère pas celle-ci de ses obligations d'explicabilité auprès des personnes concernées. En effet, PL64 prévoit que ces informations doivent être fournies par l'*utilisateur* des renseignements personnels[301]. *À ce titre*, il peut s'avérer utile de recevoir de ce même tiers une explication suffisante du fonctionnement du traitement automatisé afin de pouvoir transmettre l'information aux personnes concernées[302].

300 *Id.*, 27.
301 PL64, préc., note 1. art 110 (nouvel article 12.1. de la LPRPDE).
302 OBVIA, préc., note 44, 27.

VI. L'exactitude, le droit de rectification et le droit de révision

1. Objectifs de la section

Interconnexion de l'exactitude, du droit de rectification et du droit de révision. Nous proposons d'étudier la conformité au principe d'exactitude, au droit de rectification et au droit de réviser une décision fondée exclusivement sur un traitement automatisé dans une même section. En effet, le droit de rectification et le droit de révision s'inscrivent en grande partie dans le principe d'exactitude puisqu'ils visent en partie à s'assurer qu'une personne ne soit pas assujettie à des décisions basées sur de fausses informations ou de fausses prémisses. À ce titre, assurer le respect de ces droits renforce le respect du principe d'exactitude.

Deux types d'exactitudes. Le principe d'exactitude consiste donc à s'assurer de :

1. l'exactitude des renseignements personnels utilisés ;

et

2. l'exactitude des décisions fondées exclusivement sur un traitement automatisé.

2. L'exactitude des renseignements personnels

2.1. L'exactitude des renseignements

Exactitudes des renseignements personnels. Les renseignements personnels détenus doivent être[303] :

1. exacts ;
2. complets

ET

3. à jour.

Propositions de mesures. À ce titre, il importe de mettre en place des mesures afin de s'assurer que les renseignements personnels utilisés répondent à ces critères. Cela peut se faire, par exemple, par des mises à jour régulières des données ou par la correction de facteurs pouvant nuire à l'exactitude des renseignements (e.g. l'intégrité des renseignements n'est pas assurée, réduire le temps écoulé entre les collectes, s'assurer de la fiabilité des sources d'origines des renseignements…).

Outils de gestion de préférences. Il importe donc de mettre des outils de gestion de préférences en matière de vie privée à la disposition des personnes concernées. Ces outils pourraient permettre de vérifier l'exactitude des renseignements personnels, de les mettre à jour, de corriger les inexactitudes, de les supprimer et/ou d'en ajouter[304].

303 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108.art 11, PL64 préc., note 1. art 101 (nouvel article 11 de la LPRPSP) et *Projet de loi C-11 : 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*, préc., note 61. art 56.

304 OBVIA, préc., note 44, 27.

2.2. Droit de rectification

2.2.1. Considérations générales

Droit de rectification. Les demandes de rectification doivent permettre de modifier (ou de supprimer) ses renseignements. Les personnes concernées par les renseignements doivent pouvoir être en mesure de rectifier ou supprimer un renseignement :

- inexact ;
- incomplet ;
- équivoque ;

OU

- un renseignement dont la collecte, sa communication ou sa conservation n'était pas autorisée[305].

La demande de rectification doit être faite par écrit et doit être adressée au responsable de la protection des renseignements personnels[306]. Elle doit être faite par l'une des personnes habilitées par la Loi à agir ainsi, parmi lesquelles la «personne justifiant son identité à titre de personne concernée»[307].

Ajout de commentaires. La personne concernée peut également formuler des commentaires par écrit se rapportant à ses renseignements personnels[308]. À ce titre, il convient de 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.»[309]

Suppression. Une personne peut également exiger la suppression :

- d'un renseignement personnel périmé ;
- d'un renseignement non justifié au regard des fins prévues ;

OU

- d'un renseignement personnel dont la collecte, sa communication ou sa conservation n'était pas autorisée[310].

Limites au droit de rectification. En contrepartie, la demande de rectification n'a pas à être accordée, notamment, dans les circonstances suivantes :

1. si le renseignement personnel est exact, complet et non-équivoque et
2. si le renseignement a été collecté, utilisé et communiqué légalement[311].

OU :

1. si le renseignement personnel inféré (ou prédit) par l'application ou le système sous étude ne prétend pas être un fait et
2. si le renseignement a été collecté, utilisé et communiqué légalement[312].

---

305 *Code Civil du Québec*, préc., note 128. art. 40. et PL64, préc., note 1, art 121 (nouvel article 28 de la LPRPSP).
306 PL64, préc., note 1, art 123 et 129 (nouveaux articles 30 et 40.1 de la LPRPSP) ; *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 30.
307 *Id.*
308 PL64, préc., note 1, art 101 (nouvel article 1.1. de la LPRPSP).
309 OBVIA, préc., note 44, 26.
310 *Code Civil du Québec*, préc., note 128. art 40. ; PL64, préc., note 1, art 121 (nouvel article 28 de la LPRPSP).
311 *Code Civil du Québec*, préc., note 128.
312 *Id.*

Responsabilités du *Responsable de la protection des renseignements personnels.* C'est le *Responsable de la protection des renseignements personnels* qui doit répondre aux demandes de rectification. Il doit également assister les personnes concernées dans leurs demandes de rectification si ces dernières ne sont pas suffisamment précises ou que la personne le requiert[313].

Délais. Le *Responsable de la protection des renseignements personnels* doit répondre à la demande avec diligence au plus tard 30 jours de sa date de réception[314].

Responsabilités en cas d'acceptation. S'il accorde la rectification, alors le responsable doit notamment :

1. notifier, sans délai, la rectification à toute personne qui a reçu les renseignements dans les 6 mois précédents[315] ;
2. notifier, sans délai, la rectification à la personne de qui elle tient les renseignements[316] et
3. délivrer sans frais au requérant une copie «de tout renseignement personnel modifié ou ajouté»[317] ou une «attestation de la suppression»[318] du renseignement.

Responsabilités en cas de refus. S'il refuse d'accorder la rectification, le responsable doit notamment :

1. motiver son refus ;
2. préciser les recours qui s'offrent au requérant pour contester son refus et
3. si réclamés par le requérant, prêter assistance à ce dernier afin de l'aider à comprendre le refus[319].

2.2.2. Considérations propres aux SIA

Retour sur l'explicabilité. Il est possible qu'une personne concernée demande de rectifier les résultats ou données de sorties des SIA. En pareilles circonstances, il convient d'identifier si le droit de rectification s'applique. Ainsi, il convient de se rappeler que le droit de rectification ne s'applique pas dans les circonstances suivantes :

1. les renseignements utilisés pour atteindre le résultat sont exacts, complets et non équivoques[320] et que
2. les renseignements sont collectés, utilisés et communiqués légalement[321].

OU si:

1. les résultats n'ont pas la prétention d'être des faits[322] et que
2. les renseignements sont collectés, utilisés et communiqués légalement[323].

313 PL64, préc., note 1, art 124 (nouvel article 32 de la LPRPSP).
314 *Id.* et *Code Civil du Québec*, préc., note 128.
315 *Id.* art 40.
316 *Id.*
317 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 35.
318 *Id.* et PL64, préc., note 1, art 127 (nouvel article 35 LPRPSP).
319 PL64, préc., note 1, art 126 (nouvel article 34 de la LPRPSP).
320 Commission d'accès à l'information du Québec, préc., note 18, p. 24. citant *Guidance on AI and data protection*, Information Commissioner's Office (UK) 2020.
321 *Id.*
322 OBVIA, préc., note 44, 26. citant *Guidance on AI and data protection*, Information Commissioner's Office (UK) 2020.
323 Commission d'accès à l'information du Québec, préc., note 18, p. 24.

Destruction des modèles. La suppression d'un renseignement personnel par un usager n'implique pas de devoir supprimer tous les modèles entrainés à partir de ce renseignement. Cependant, le modèle peut devoir être supprimé s'il permet d'inférer un renseignement personnel[324].

Traçabilité des données. Il peut s'avérer opportun d'établir, tout au long du cycle de vie du SIA, 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.»[325]

Il convient également de documenter les déplacements des renseignements, leur origine, comment ils sont collectés, comment ils sont transformés ainsi que les mesures mises en place pour s'assurer que «l'exactitude des données [soit] maintenue»[326] à travers ces opérations[327].

DISTINCTIONS AVEC LE RÉGIME EUROPÉEN

Suppression des renseignements

Le régime québécois traite la suppression d'un renseignement comme une extension au droit de rectification[328]. Ce droit de rectification, tel qu'identifié, permet non seulement de rectifier l'inexactitude et l'incomplétude de ses renseignements personnels, mais également de réclamer la suppression de tous renseignements collectés, communiqués ou utilisés illégalement[329].

Le RGPD rattache plutôt la suppression des renseignements comme une extension du *droit à l'effacement*. Conséquemment, le RGPD prévoit que le droit d'effacer ses données à caractère personnel doit être justifié par l'un des multiples motifs qui permettent d'appliquer le droit à l'effacement[330]. Ces motifs sont toutefois étrangers au droit de rectification tel que conçu sous le RGPD[331].

Or, certains motifs justifiant l'usage du droit à l'effacement en Europe permettraient, au Québec, de justifier l'usage d'un droit de rectification. Par exemple, il est possible d'obtenir sous le RGPD, l'effacement de données à caractère personnel qui «ont fait l'objet d'un traitement illicite»[332]. À ce titre, bien que les assises juridiques de la suppression des renseignements personnels diffèrent entre l'Europe et le Québec, il n'est pas clair si cette différence provoque des distinctions importantes en pratique.

---

324 OBVIA, préc., note 44, 28. citant *Guidance on AI and data protection, Information Commissioner's Office* (UK) 2020
325 *Id.*, 31.
326 *Id.*, 26.
327 *Id.*
328 PL64, préc., note 1, art 127 (nouvel article 35 de la LPRPSP).
329 *Code Civil du Québec*, préc., note 128. art 40.
330 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 16-17.
331 *Id.*
332 *Id.* art 17.

3. L'exactitude des décisions fondées exclusivement sur des traitements automatisés

3.1. L'exactitude des décisions

Mesures. L'entreprise doit adopter des mesures visant à s'assurer qu'un usager n'est pas préjudicié par une décision se basant sur des inférences, prédictions ou évaluations erronées. Il faut donc s'assurer de l'exactitude du traitement des renseignements et des résultats découlant de ce traitement. Pour assurer cela, l'organisation peut mettre en place différentes mesures telles que :

1. assurer la traçabilité des données qui permettraient d'identifier le renseignement personnel utilisé dans une prise de décision exclusivement automatisée ;
2. enregistrer les mouvements des renseignements utilisés ;
3. évaluer l'exhaustivité de l'ensemble des données d'attributs et d'éléments ;
4. identifier les risques d'inexactitudes et de biais liés au traitement des renseignements par des humains (voir la section portant sur la Non-discrimination)

ET

5. tenir un registre de décisions erronées[333].

3.2. Droit de révision

Intervention humaine. Une personne concernée par une *décision fondée exclusivement sur un traitement automatisé* devrait pouvoir «présenter ses observations à un membre du personnel en mesure de réviser la décision»[334]. Cette révision doit bénéficier d'une intervention humaine dans le processus décisionnel.

Implications pratiques. L'organisation doit s'assurer que l'intervention humaine ne représente pas purement une formalité cosmétique. Les personnes concernées par la décision doivent pouvoir bénéficier d'un réel jugement humain. Cela signifie, entre autres :

1. qu'il doit être possible de réviser la décision ;
2. que les personnes chargées de réviser les décisions doivent détenir l'autorité et les compétences nécessaires pour faire des révisions significatives et infirmer les décisions[335] ;
3. que les réviseurs sont tenus responsables de leurs décisions[336];
4. de prévoir des mesures visant à assurer que les réviseurs adoptent une posture raisonnablement sceptique à l'égard des résultats produits par le processus automatisé ;

ET

5. de pouvoir mot irconstances dans lesquelles une décision est confirmée ou infirmée par le réviseur[337].

Obligation de conservation. Si un renseignement a été utilisé dans le cadre d'une décision fondée exclusivement sur un traitement automatisé alors il convient de conserver ce renseignement pendant au moins un an suivant la décision[338].

333 Voir OBVIA, préc., note 44, 27.
334 PL64, préc., note 1, art. 110 (nouvel article 12.1. LPRPSP).
335 OBVIA, préc., note 44, 30.
336 *Id.*
337 *Id.*, 31.
338 PL64, préc., note 1. art 109 (nouvel article 11 de la LPRPSP).

DISTINCTIONS AVEC L'EUROPE

Illégalité de la prise de décision exclusivement automatisée

Le RGPD prévoit qu'en principe la prise de décision exclusivement automatisée est interdite si elle produit des effets juridiques à l'égard de la personne concernée ou qui l'affecte significativement de façon similaire[339]. Le règlement prévoit des exceptions à cette règle soit[340] :

- lorsque la prise de décision exclusivement automatisée est nécessaire à l'exécution d'un contrat ;
- lorsque la prise de décision exclusivement automatisée est autorisée en vertu de la législation européenne ou nationale (sous certaines conditions)

OU

- lorsque la décision est «fondée sur le consentement explicite de la personne concernée»[341] .

Même si ces exceptions s'appliquent, le RGPD prévoit plusieurs garanties devant être offertes à la personne concernée parmi lesquelles :

1. le droit d'obtenir une intervention humaine ;
2. le droit d'exprimer son point de vue ;

ET

3. le droit de contester la décision[342].

Au Québec, toutefois, PL64 est beaucoup plus permissif à l'égard des prises de décisions exclusivement automatisées. Ce projet de loi ne prévoit pas formellement de circonstances dans lesquelles la prise de décision exclusivement automatisée serait prohibée.

339 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 22(1). et Groupe de travail « Article 29 » sur la Protection des données, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, 17/FR, coll. WP251rev.01, Bruxelles, 2018, p. 21, en ligne : https://www.cnil.fr/sites/default/files/atoms/files/wp251_profilage-fr.pdf (consulté le 27 janvier 2022).

340 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 22(2).

341 *Id.*

342 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 22(3).

VII. La non-discrimination

1. Objectif de la section

Assurer un traitement non discriminatoire. Le principal objectif de la présente section est d'évaluer les risques liés aux comportements discriminatoires des SIA.

2. Considérations propres aux SIA

Définir la discrimination. Avant de procéder à évaluer les risques de discriminations, l'organisation doit définir ce qu'elle entend comme «discrimination» dans le contexte de l'utilisation d'un SIA. Le responsable de la stratégie doit lutter contre les formes de discriminations *directes* et *indirectes*[343].

Identifier les groupes affectés. Afin de lutter convenablement contre les risques de discriminations, il convient d'identifier les groupes pouvant être affectés par celles-ci. L'article 10 de la *Charte des droits et libertés de la personne* prohibe la discrimination fondée sur :

- la race ;
- la couleur ;
- la langue ;
- l'origine ethnique ou nationale ;
- l'identité ou l'expression de genre ;
- l'orientation sexuelle ;
- le sexe ;
- la grossesse ;
- l'état civil ;
- l'âge (sauf dans la mesure prévue par la loi) ;
- la religion ;
- les convictions politiques ;
- la condition sociale ;
- le handicap

ET

- l'utilisation d'un moyen pour pallier ce handicap[344].

343 Yordanka IVANOVA, *The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI*, Luís ANTUNES, Maurizio NALDI, Giuseppe F. ITALIANO, Kai RANNENBERG et Prokopios DROGKARIS (dir.), *Privacy Technologies and Policy*, coll. Lecture Notes in Computer Science, Cham, Springer International Publishing, 2020, p. 3-24, p. 8, doi : 10.1007/978-3-030-55196-4_1.

344 *Charte des droits et libertés de la personne*, préc., note 102. art 10.

Risques de discriminations directes. Il y a discrimination *directe* lorsque le SIA établit une distinction injustifiable à partir d'un motif prohibé par la *Charte des droits et libertés de la personne*[345]. Tel serait le cas, par exemple, d'une SIA qui défavoriserait des candidats s'identifiant comme autochtones.

Risques de discriminations indirectes. Il y a discrimination *indirecte* lorsque la discrimination ne résulte pas de l'analyse directe de motifs prohibés. Tel serait le cas, par exemple, d'une SIA qui fonde ses décisions sur des caractéristiques individuelles fortement corrélées aux motifs de discriminations prohibés[346]. Par exemple, le salaire et le code postal sont des renseignements qui peuvent être fortement corrélés à la couleur de peau d'un individu[347]. À ce titre, il convient d'être prudent lorsque l'on réclame à une SIA de fonder ses décisions à partir de ces données. Agir ainsi risque de discriminer contre les membres de minorités visibles.

Discriminations intersectionnelles. Les formes de discriminations intersectionnelles doivent également être prises en considération. Une discrimination intersectionnelle existe lorsque la discrimination se fonde sur l'imbrication de plusieurs motifs discriminatoires[348]. Tel qu'indiqué par la Cour suprême :

«Il peut arriver qu'il soit impossible de reconnaître un traitement discriminatoire à l'égard d'une personne ou d'un groupe en l'examinant au regard d'un seul motif de discrimination interdit et qu'il soit nécessaire d'appliquer plusieurs facteurs convergents qui, isolément, ne permettraient peutêtre pas de mesurer l'ampleur des conséquences du déni de l'avantage ou de l'imposition du fardeau en cause»[349].

3. Les causes et les risques de traitements discriminatoires

Différentes sources de risques. Des risques de discriminations peuvent résulter notamment (1) du développement du SIA, (2) de son entrainement ou (3) de l'usage qui en est fait.

3.1. Les causes de discriminations liées au développement du SIA

Risques créés lors du développement du SIA. Il importe de rester vigilant lors de la phase de développement et de programmation du SAI.

Exemple : Risques nés d'une absence de clarté des variables cibles. Réclamer à un SIA d'optimiser des prédictions au regard d'une variable cible (*target variable*) vague et subjective peut mener à des traitements discriminatoires[350]. Par exemple, développer un algorithme supervisé capable de distinguer les «bons» des «mauvais» candidats à un poste présente des risques de traitements discriminatoires puisque la définition de «bons» et de «mauvais» candidats repose sur des caractérisations subjectives et artificielles. Leurs définitions dépendront des biais, impressions et croyances des développeurs ou des personnes chargées d'étiqueter ou de produire les données qui entraineront l'algorithme[351]. À ce titre, il est souhaitable de privilégier des *variables cibles* plus objectives.

345 Cour suprême, 1990, 2 RCS 489, *Central Alberta Dairy Pool c. Alberta (Commission des droits de la personne)*, en ligne : https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/641/index.do?q=direct+discrimination (consulté le 6 octobre 2021). (Juge Wilson) citant *Commission ontarienne des droits de la personne et O'Malley c. SimpsonsSears Ltd.*, [1985] 2 R.C.S. 536 p. 551.

346 Y. Ivanova, préc., note 343, p. 8.

347 Natalia Criado et Jose Such, « Digital Discrimination », dans *Algorithmic Regulation*, Oxford, New York, Oxford University Press, 2019, p. 82-97 à la page 5, doi : 10.1093/oso/9780198838494.003.0004.

348 Hilème Kombila, « Les entraves à l'approche « intersectionnelle » canadienne de la discrimination », *La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux* 2016.9, doi : 10.4000/revdh.2056 au para 8.

349 *Withler c. Canada (Procureur général)*, [2011] 1 RCS 396 (Cour suprême du Canada), en ligne : https://canlii.ca/t/2g0mg (consulté le 27 janvier 2022) au para 58.

350 *Id.* 4.

351 *Id.* 5.

3.2. Les causes de discriminations liées à l'entrainement du SIA

Risques résultant du choix des données. Les risques de discriminations peuvent également être créés en raison de l'entrainement de l'intelligence artificielle. Ainsi, lors de l'entrainement de l'algorithme, il convient de se prémunir contre les risques causés par :

- des données d'entrainement biaisées ;
- des données d'entrainement étiquetées exclusivement par des humains ;
- des données d'entrainement surreprésentant ou sous représentant des groupes vulnérables ;

OU

- des données fortement corrélées avec des motifs de discrimination prohibés[352].

Risques résultant de l'entrainement continu. Afin d'évaluer convenablement les risques que présente l'usage du SIA, il faut d'abord identifier s'il s'entraine continuellement en collectant des renseignements auprès de ses utilisateurs. En effet, l'entrainement continu des algorithmes présente des risques tels que:

- la collecte de renseignements non représentatifs de la réalité (e.g. des minorités sont sous-représentées dans les renseignements collectés auprès des usagers) ;
- des comportements discriminatoires créés causés par l'interaction du SIA avec les usagers[353]

OU

- les résultats du SIA renforcent les stéréotypes[354].

3.3. Les causes de discriminations liées au mésusage d'un SIA

Risques résultant du mésusage. Finalement, le SIA doit être utilisé pour réaliser les tâches pour lesquelles il a été conçu. Par exemple, un algorithme visant à produire des résultats pertinents pour une section de la population pourrait produire certains résultats inattendus s'il est utilisé à d'autres sections de la population[355].

352 *Id.*; Y. Ivanova, préc., note 343, p. 9.

353 Voir l'exemple de Microsoft Tay Chatbot qui en raison de ses interactions avec les utilisateurs de Twitter a publié des commentaires racistes et discriminatoires. « Microsoft chatbot is taught to swear on Twitter », *BBC News*, sect. Technology (24 mars 2016), en ligne : https://www.bbc.com/news/technology-35890188 (consulté le 6 octobre 2021).

354 N. Criado et J. Such, préc., note 347 à la page 5.

355 *Id.* à la page 6; Y. Ivanova, préc., note 343, p. 9-10.

4. Mesures de protection possibles

Stratégie. Afin de se prémunir efficacement contre les risques de discriminations, il convient d'élaborer une *stratégie d'atténuation des risques de discriminations*[356]. À ce titre, il importe de désigner un *responsable de la mise en œuvre de la stratégie d'atténuation des risques de discrimination* qui incorpore les mesures et politiques qui adressent ces risques. Cette personne doit détenir l'autorité nécessaire pour accomplir son mandat.

Vérifications des données. Il convient également d'éviter de recourir à des données qui pourraient causer les problématiques susmentionnées.

Importance d'une évaluation continue. Il convient d'évaluer et de tester le SIA afin d'identifier les sources potentielles de discriminations et si les résultats des SIA sont discriminatoires. Le SIA devrait être évalué tout au long de son développement et de son utilisation. La mise en place d'un système de signalement par le public de problèmes de discrimination peut s'avérer nécessaire.

Recalibrer le SIA afin d'assurer que les groupes soient traités équitablement. Afin de contrer des conclusions discriminatoires, il peut se révéler nécessaire de recalibrer l'outil afin d'assurer des résultats qui ne sous représenteraient ou ne surreprésenteraient pas déraisonnablement certains groupes.

Recalibrer le SIA afin d'assurer que les individus soient traités équitablement. Il peut également se révéler nécessaire de recalibrer l'outil afin d'assurer que les membres de certains groupes ne soient pas disproportionnellement affectés par des conclusions erronées de l'outil. En d'autres termes, un membre d'un groupe désavantagé ne doit pas faire l'objet de faux positifs / faux négatifs disproportionnellement plus élevés en raison de son appartenance au groupe identifié.

Mesurer les risques résultant des mesures de protection. Malheureusement, il est possible que les mesures visant à atténuer le risque de discrimination créent elles-mêmes de nouveaux risques. Ainsi, la recalibration de l'outil pour des raisons d'équité peut affecter son exactitude[357]. De plus, des mesures visant à rétablir une équité chez certains groupes peuvent défavoriser directement les membres d'autres groupes vulnérables[358]. Certains spécialistes proposent également de collecter des renseignements personnels *sensibles* comme la couleur de peau afin de détecter et de remédier à la discrimination[359]. Un équilibre entre différents principes et risques peut donc s'avérer nécessaire. Afin d'identifier quels principes privilégier, il importe de bien évaluer les risques associés à la mesure imposée.

356 OBVIA, préc., note 44, 33.
357 N. Criado et J. Such, préc., note 347 à la page 5.
358 Michael KEARNS et Aaron ROTH, *The Ethical Algorithm: The Science of Socially Aware Algorithm Design*, Oxford, New York, Oxford University Press, 2019, p. 78-81.
359 Y. Ivanova, préc., note 343, p. 8.

DISTINCTIONS AVEC L'EUROPE

Les considérations liées aux traitements discriminatoires par les SIA

Il est clair que le cadre normatif européen protège les personnes concernées contre les traitements discriminatoires. Ainsi, le RGPD prévoit l'évaluation des risques pour l'ensemble des «*droits et libertés d'une personne*»[360] ce qui inclut le risque de subir un traitement discriminatoire[361]. Qui plus est, le RGPD identifie certains motifs de discrimination comme des «catégories particulières de données» qualifiés de «sensibles»[362]. Tel qu'identifié, des protections spécifiques sont prévues à l'égard de ces catégories de données. Finalement, la Commission européenne a récemment publié une *Proposition de Règlement du Parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union* qui adresse directement les risques de traitements discriminatoires par des SIA[363].

Ni C-11 ni PL64 n'adressent clairement et directement les problématiques liées à la discrimination. À première vue, les risques liés aux traitements discriminatoires semblent donc ignorés par les régimes québécois et canadiens. Cependant, il convient de rappeler que plusieurs motifs de discrimination tels que l'origine ethnique et l'orientation sexuelle sont traités comme des renseignements sensibles[364]. Or, tel qu'identifié, un renseignement personnel sensible mérite une protection accrue[365].

De plus, les développeurs ou utilisateurs de SIA doivent respecter les protections conférées par la *Charte des droits et libertés de la personne*[366]. À ce titre, bien que PL64 ne propose pas *directement* d'évaluer les risques liés à la discrimination cela n'implique pas que ces derniers devraient être ignorés.

Toutefois, contrairement au Québec et au Canada, le régime européen prévoit des règles capables d'adresser *spécifiquement* les enjeux de discriminations créés par les SIA. L'article 10(5) de la proposition de *Règlement européen sur l'IA* illustre bien cette capacité. Tel qu'identifié précédemment, répondre aux risques liés aux traitements discriminatoires peut réclamer la collecte de renseignements personnels sensibles des usagers à des fins de détection et de correction de biais jugés discriminatoires. L'inconvénient de cette mesure est qu'en collectant des renseignements sensibles, l'entreprise peut compromettre la vie privée de ses usagers. Le respect de certaines normes légales peut donc se faire directement au détriment du respect d'autres normes ce qui peut positionner la personne qui exploite une entreprise dans une situation assez difficile.

Or, l'article 10(5) de la proposition de *Règlement européen sur l'IA* prévoit qu'une entité peut traiter «des catégories particulières de données à caractère personnel»[367] dans la mesure «où cela est strictement nécessaire aux fins de la surveillance, de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque» sous certaines circonstances[368]. Cette disposition, qui ne trouve pas d'équivalent dans PL64 et C-11, permet de guider adéquatement les entreprises dans leurs choix de mesures à privilégier en cas de tensions entre protection de différents droits et libertés individuelles.

360 *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 (Règlement général sur la protection des données) (RGPD)*, préc., note 16., art 34.

361 *Id.* art 9(1).

362 *Id.* au préambule 10 et art 9 à 10.

363 Voir par exemple la *Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union*, préc., note 65. art 3 (35), 5, 52.

364 Commissariat à la protection de la vie privée du Canada, préc., note 78.

365 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 108. art 10.

366 *Charte des droits et libertés de la personne*, préc., note 102. art 10.

367 *Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union*, préc., note 65. art 10(5).

368 *Id.* art 10(5).

PARTIE C
ÉVALUATION FINALE

Évaluation finale. Dans cette partie, l'évaluateur est appelé à offrir son évaluation finale du projet. Un tableau intégrant les éléments nécessaires à la réalisation de l'évaluation finale est présenté en Annexe.

1. Compte rendu de l'évaluation des principes

Évaluation des principes. L'évaluateur doit noter si le projet, sous sa forme actuelle, respecte, oui ou non, chacun des principes susmentionnés. Cette évaluation doit être justifiée au regard des risques ou des obligations légales qui n'ont pas été respectées par l'entreprise.

Émettre des recommandations. Si les risques restent trop importants ou si l'évaluateur juge que le projet pourrait bénéficier de l'adoption de certaines mesures alors ce dernier propose et décrit les principales mesures capables de répondre adéquatement aux risques. Il peut, par exemple : proposer de retirer certaines opérations prévues jugées trop risquées ou modifier les politiques et pratiques de gouvernance des renseignements personnels de l'entreprise.

Déploiements des recommandations. À la réception de l'évaluation, le *Responsable de la protection des renseignements personnels* prend position sur les recommandations émises par l'évaluateur. S'il accepte les recommandations, il doit identifier la personne responsable de leurs mises en œuvre. Le *Responsable de la protection des renseignements personnels* prévoit également un échéancier pour la mise en œuvre des recommandations acceptées.

2. Compte rendu de l'évaluation du projet

Évaluation finale. L'évaluateur doit prendre position sur l'acceptabilité des risques du projet face aux bénéfices appréhendés. Naturellement, l'évaluateur peut référer à son évaluation de la section *Justification sociale.*

CENTRE
DE RECHERCHE
EN DROIT
PUBLIC

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