

## **La protection des renseignements personnels dans le cadre de la gestion collective de droits d'auteur au Canada**

**Maxime-Pierre Gazeau\***

RÉSUMÉ .....	1413
INTRODUCTION .....	1415
I- CHAMP D'APPLICATION DES LOIS SUR LES RENSEIGNEMENTS PERSONNELS À L'ACTIVITÉ DES SGC .....	1417
A- Champ d'application matériel .....	1417
1. Qu'est-ce qu'un renseignement personnel ? .....	1417
2. Données publiques, ouvertes et renseignements personnels .....	1420
B- Champ d'application territorial .....	1423
1. Entre lois fédérales et provinciales .....	1423
2. Entre lois nationales et internationales .....	1425
3. Encadrement des transferts de données à l'étranger .....	1430
4. Base de données partagées entre SGC .....	1433

© Maxime-Pierre Gazeau, 2021.

\* Maxime-Pierre Gazeau, Conseiller à la direction, Artisti.

[Note : cet article a été soumis à une évaluation à double anonymat.]

II- CONFORMITÉ À LA LÉGISLATION APPLICABLE ET ANTICIPATION DES RÉFORMES À VENIR. . . . .	1435
A- Démarches à suivre pour se conformer à la législation applicable. . . . .	1435
B- Anticiper les réformes en cours du cadre réglementaire provincial et fédéral . . . . .	1436
1. Au niveau du Québec . . . . .	1436
2. Au niveau fédéral . . . . .	1439
CONCLUSION. . . . .	1441

## RÉSUMÉ

La protection des renseignements personnels des individus est aujourd'hui un enjeu de plus en plus important, du fait, d'abord, d'une pression accrue des citoyens, nourrie par les divers scandales touchant leurs données personnelles, mais aussi du fait de réponses réglementaires ambitieuses visant notamment à limiter l'utilisation anarchique de ces données personnelles par les GAFAM et autres entreprises de technologies. Ces réglementations ambitieuses ont vu le jour tant au niveau international – avec le *Règlement général sur la protection des données* (ci-après « RGPD ») en Europe, ou le *California Consumer Protection Act* (ci-après « CCPA ») en Californie – qu'au niveau canadien, avec le projet de loi fédéral C-11 et le projet 64 de modernisation de la loi québécoise déposés tous les deux en 2020.

Dans cet article, nous allons nous concentrer sur la protection des renseignements personnels dans le cadre de la gestion collective de droits d'auteur au Canada. Si les sociétés de gestion collective de droits d'auteur (ci-après « SGC ») ne sont pas les GAFAM de ce monde, il n'en reste pas moins que la protection des renseignements personnels reste un enjeu important pour ces sociétés, de par l'importance des données traitées dans leur activité, particulièrement dans le secteur musical. La gestion collective, comme bon nombre d'autres industries, a ainsi fait face au défi du « Big Data », ou mégadonnées, par l'explosion de l'afflux de données numériques liées à la consommation en ligne de musique. La donnée est aujourd'hui au cœur de l'activité des sociétés de gestion collective. Dans ce contexte, quelle importance peut avoir l'enjeu du respect des renseignements personnels ? Au vu des différents projets de réformes en cours au Canada, il nous paraît important de faire un état des lieux de la question pour les sociétés de gestion collective de droits d'auteur au Canada, afin d'anticiper une mise en conformité de leurs pratiques.

Cet article vise ainsi à déterminer ce que constitue un « renseignement personnel » parmi l'ensemble des données traitées par les

SGCs, et aborde l'enjeu de leur protection. Il vise ensuite à déterminer l'application territoriale des réglementations sur la protection des renseignements personnels, face aux flux transfrontaliers des données, en se posant la question notamment de l'application du RGPD aux SGCs canadiennes dans leur activité. Nous verrons ensuite les démarches à suivre pour se conformer à la législation applicable, ainsi que les pistes pour anticiper les réformes à venir du cadre réglementaire, par exemple sur les transferts hors province ou la durée de conservation des renseignements personnels.

## INTRODUCTION

La protection des renseignements personnels des individus est aujourd'hui un enjeu de plus en plus important pour les États, du fait, d'abord, d'une pression accrue des citoyens nourrie par les divers scandales touchant leurs données personnelles – pensons à Cambridge Analytica ou plus récemment à la fuite Desjardins<sup>1</sup> – mais aussi du fait de réponses réglementaires ambitieuses visant notamment à limiter l'utilisation anarchique de ces données personnelles par les GAFAM et autres entreprises de technologies, notamment au sein de l'Union européenne en 2016 avec le *Règlement général sur la protection des données* (ci-après « RGPD »)<sup>2</sup> ou de la Californie en 2018 avec le *California Consumer Protection Act* (ci-après « CCPA »)<sup>3</sup>. À l'heure où les renseignements personnels sont ainsi la nouvelle matière première de l'industrie numérique du XXI<sup>e</sup> siècle, l'enjeu de leur protection se pose comme un rempart aux dérives mercantiles de certaines entreprises et aux incidents de sécurité des pirates informatiques.

Le droit au respect de ses renseignements personnels est ainsi érigé comme un nouveau droit de l'homme du XXI<sup>e</sup> siècle. Au Canada, le droit à la protection de la vie privée est déjà reconnu comme un droit de l'homme, puisqu'il est par exemple protégé par la *Charte des droits et libertés de la personne*<sup>4</sup> au Québec, ou par l'article 8 de la

- 
1. Incident de sécurité survenu chez Desjardins : 9,7 millions de personnes au Canada et à l'étranger, dont près de 7 millions de Québécois, ont été victimes de ce vol de données. Voir COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « La Commission d'accès à l'information se prononce sur le plus important incident de sécurité affectant la protection des renseignements personnels jamais survenu au Québec », 14 décembre 2020, en ligne : <<https://www.cai.gouv.qc.ca/communique-cai-decision-enquete-desjardins/>>.
  2. *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)*, 4 mai 2016, J.O. L 119, p. 1 (ci-après « RGPD »).
  3. *California Consumer Protection Act*, California Civil Code, section 1798.100, 28 juin 2018 (ci-après « CCPA »).
  4. RLRQ, c. C-12, art. 5 : « Toute personne a droit au respect de sa vie privée ».

*Charte canadienne des droits et libertés*<sup>5</sup>. La Cour suprême du Canada reconnaît d'ailleurs que les lois qui protègent les renseignements personnels dans le secteur privé ont un statut quasi constitutionnel. La protection des renseignements personnels est donc un enjeu important dans n'importe quel secteur d'activités, mais elle prend tout son sens pour les entreprises qui sont en lien quotidiennement avec les données de leurs clients, consommateurs ou adhérents.

Nous allons nous concentrer dans cet article sur la protection des renseignements personnels dans le cadre de la gestion collective de droits d'auteur au Canada. Si les Sociétés de gestion collective de droits d'auteur (ci-après « SGC ») ne sont pas les GAFAM de ce monde, puisque bien souvent le traitement des renseignements personnels est un moyen inévitable d'assurer la distribution de redevances à des ayant droits et non une stratégie commerciale, il n'en demeure pas moins que la protection des renseignements personnels reste un enjeu important pour ces sociétés, de par l'importance des données traitées dans leur activité. La gestion collective dans le domaine musical est particulièrement intéressante puisque le secteur de la musique a subi ces dernières années, du fait du streaming, une explosion de l'échange de données. Toutefois, les enseignements tirés de nos développements peuvent s'appliquer à d'autres domaines de la gestion collective, audiovisuel ou littéraire par exemple.

Inutile de rappeler que l'écosystème de la musique s'est fortement numérisé ces dernières années, avec l'avènement du téléchargement en ligne puis des plateformes de streaming. Pour les sociétés de gestion collective, le streaming a ainsi amené un défi sans précédent de faire face à un afflux massif de données venant de ces plateformes, se matérialisant par des millions de lignes à analyser afin d'assurer la rémunération des ayants-droits associée à l'utilisation de la musique. La gestion collective, comme nombre d'autres industries, a ainsi fait face au défi du « Big Data », ou mégadonnées, par l'explosion de l'afflux de données numériques. La décennie 2010-2020 a donc vu un accroissement des données générées liées à l'usage de la musique, puisque le modèle du streaming musical permet une consommation sans limites de musique en ligne. Elle a également vu un accroissement parallèle des échanges entre sociétés de gestion collective dans le monde, en raison d'une démultiplication de l'usage international de la musique. En résumé, il y a beaucoup

---

5. Partie I de la *Loi constitutionnelle de 1982* [annexe B de la *Loi de 1982 sur le Canada*, 1982, c. 11 (R.-U.)].

de données, et elles sont davantage échangées. La donnée est donc au cœur de l'activité des sociétés de gestion collective aujourd'hui.

Mais dans ce contexte et parmi toutes ces données échangées, quelle importance peut avoir l'enjeu du respect des renseignements personnels ? Une société de gestion collective n'étant pas un réseau social ni un service de renseignement, l'enjeu semble donc plus limité, il est vrai. Toutefois, à l'heure où un projet de modernisation de la loi sur la protection des renseignements a été déposé à Ottawa le 20 novembre 2020 (le projet de loi C-11)<sup>6</sup>, et qu'un projet de modernisation de la loi québécoise déposé le 12 juin 2020 est également à l'étude (le projet de loi 64)<sup>7</sup>, il nous paraît important de faire un état des lieux de la question pour les sociétés de gestion collective de droits d'auteur au Canada, afin d'anticiper une mise en conformité de leurs pratiques.

## **I- CHAMP D'APPLICATION DES LOIS SUR LES RENSEIGNEMENTS PERSONNELS À L'ACTIVITÉ DES SGC**

### **A- Champ d'application matériel**

#### **1. Qu'est-ce qu'un renseignement personnel ?**

Parmi l'ensemble des données traitées par une SGC, il nous semble essentiel de déterminer en premier lieu ce que constitue un « renseignement personnel » au sens des diverses lois applicables. Mais d'abord, quel est l'enjeu d'une telle qualification pour une SGC ? Les données identifiées comme « renseignements personnels » auront un régime d'utilisation plus contraignant que les autres données pour les SGC. Ainsi, des précautions devront être prises pour ces renseignements, s'agissant de leur durée de conservation, de l'exercice des droits de leurs adhérents sur ces renseignements et leur information sur les caractéristiques du traitement, de leur sécurisation ou de l'encadrement de leur transfert à l'international, mais aussi, comme on le verra, s'agissant du traitement des données reçues de l'étranger, particulièrement des sociétés basées dans l'UE. Par exemple, s'agissant de la collecte de ces données, si c'est un renseignement

---

6. *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*, projet de loi n° C-11 (dépôt et 1<sup>re</sup> lecture – 17 novembre 2020), 2<sup>e</sup> sess., 43<sup>e</sup> légis. (Can.).

7. *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi n° 64 (étude détaillée – 2 septembre 2021), 1<sup>re</sup> sess., 42<sup>e</sup> légis. (Qc).

personnel, la personne doit consentir à sa collecte et son utilisation à des fins spécifiques. Par ailleurs, concernant sa diffusion, si c'est un renseignement personnel, il est nécessaire d'informer la personne des destinataires spécifiques de ses renseignements personnels dans le cas d'une diffusion à un tiers. Enfin, une autre contrainte peut concerner la durée de conservation de ces renseignements qui est en principe limitée, soit par exemple pour « la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé »<sup>8</sup>. Enfin, les personnes concernées disposent de droits sur leurs renseignements personnels (ex. : droit d'accès, de rectification, de suppression).

Au terme de la loi fédérale, la *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après « PIPEDA », l'acronyme anglais)<sup>9</sup>, un renseignement personnel désigne « Tout renseignement concernant un individu identifiable ». Au sens de l'article 2 de la loi québécoise, la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « LPRPSP ») : « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier »<sup>10</sup>. Ces définitions sont donc très larges.

Pour des SGC, cela peut ainsi concerner de nombreuses informations qu'elles utilisent quotidiennement dans leurs activités, comme les noms et prénoms légaux de leurs membres, le sexe, les dates de naissance et de décès, leurs pays de résidence fiscale, leurs adresses, leurs citoyennetés, leurs informations financières, leurs numéros de téléphone, leurs adresses de courriel, etc. En effet, l'un des enjeux centraux d'une SGC est d'identifier leurs adhérents parmi l'ensemble des données d'utilisation de musique qu'elles reçoivent, et afin d'éviter les erreurs d'identification, il est donc primordial d'avoir le plus de données pertinentes permettant cette identification. De plus, pour des raisons fiscales, les sociétés de gestion canadiennes sont souvent amenées à traiter le numéro d'assurance sociale (NAS) de leurs adhérents canadiens, ce qui est probablement l'information la plus sensible qu'elles aient à traiter, avec leurs informations

---

8. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1, art. 14 : « Le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé ».

9. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. C-5.

10. *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 8, art. 2.

financières. Il y a peu de doute que l'ensemble de ces informations constituent des renseignements personnels au sens de la loi fédérale et provinciale, et elles devront donc faire l'objet d'une attention particulière par les SGC pour se conformer à la réglementation applicable.

Par ailleurs, d'autres renseignements traités par les sociétés de gestion collective, comme les numéros d'identification professionnels ou les informations liées à la musique de leurs membres ont une qualification moins évidente de renseignements personnels, du fait de leurs accessibilités publiques.

Tout d'abord, les numéros d'identifications professionnelles sont des numéros attribués par les SGC ou d'autres organismes internationaux aux artistes, auteurs et producteurs pour faciliter leurs identifications à l'international. Parmi ces numéros, il y a par exemple l'IPN, l'ISNI, ou encore l'IPI. Ces numéros ont vocation à être partagés publiquement et le plus largement possible. Est-ce qu'ils doivent être tout de même considérés comme des renseignements personnels ? Selon la CISAC<sup>11</sup>, l'organisation internationale regroupant les SGC d'auteurs-compositeurs, au sens de la définition de « renseignements personnels » du RGPD<sup>12</sup>, il faut inclure les informations d'identifications des auteurs-compositeurs tels que l'IPI ou l'ISNI. Par analogie, il faudrait aussi y inclure pour les artistes-interprètes, le numéro IPN. Au vu de la définition large de la loi québécoise et fédérale de « renseignement personnel », il faudrait en déduire la même chose. À noter qu'au-delà des contraintes liées aux réglementations sur les renseignements personnels, des règles propres à chaque organisation encadrent la diffusion de ces identifiants professionnels, et il faut donc s'y référer également.

Enfin, qu'en est-il des informations liées à la musique en elle-même ? Par exemple, les informations liées à la participation d'un auteur-compositeur à une œuvre, ou les participations d'un artiste-interprète aux titres d'un album, les noms des choristes y prenant part, etc. À noter que toutes informations sur les producteurs

11. Voir p. 4, « CISAC Guide to the General Data Protection Regulation », May 2018.

12. Selon l'article 4 du RGPD, une donnée personnelle concerne « toute information se rapportant à une personne physique identifiée ou identifiable, c'est-à-dire 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 ».

d'enregistrements sonores ou d'éditeurs musicaux sont a priori exclues de la qualification de « renseignements personnels », puisqu'elles concernent des personnes morales, alors que les renseignements personnels concernent uniquement les personnes physiques. En ce qui a trait plus particulièrement aux informations liées à la musique composée ou interprétée par des auteurs et interprètes, pourrait-il s'agir de renseignements personnels ? En soi, un titre de morceau ou d'œuvre ne permet pas d'identifier une personne physique directement, d'autant qu'un seul titre peut regrouper plusieurs interprètes et auteurs, et leur protection relèverait plus du droit d'auteur. Par contre, un pseudonyme d'un artiste ou le nom de plume d'un auteur pourraient être considérés comme un renseignement personnel, et cela, même s'ils ont vocation à désigner publiquement un individu. De plus, ce type d'informations est souvent public, car disponible sur les plateformes en ligne comme Wikipédia, Discogs, MusicBrainz, qui répertorient les « métadonnées » liées à la musique, c'est-à-dire toutes les informations liées à un titre musical comme les crédits. Mais le fait que ces informations soient publiques leur enlève-t-il la qualification de « renseignements personnels » ?

## **2. *Données publiques, ouvertes et renseignements personnels***

L'environnement en ligne regorge de données accessibles publiquement sur les contenus musicaux, qui peuvent contenir des renseignements personnels sur les ayants-droits associés. Ainsi les SGC pourraient être amenées à recueillir des renseignements personnels sur leurs adhérents qu'elles considèrent comme publics parce qu'ils sont largement accessibles, sans obtenir leur consentement. Toutefois, la PIPEDA limite les cas où un renseignement personnel accessible au public peut être utilisé sans consentement. Ainsi, la loi fédérale dispose qu'il n'est pas nécessaire d'informer la personne visée et d'obtenir son consentement lorsqu'il s'agit d'un renseignement personnel « auquel le public a accès ». Parmi ces catégories de renseignements auxquels le public a accès et qui sont listés par règlement, figurent « les renseignements personnels qui figurent dans une publication, y compris les magazines, livres et journaux, sous forme imprimée ou électronique, qui est accessible au public, si l'intéressé a fourni les renseignements. »<sup>13</sup> L'interprétation des tribunaux et du Commissariat à la protection de la vie privée du Canada est plutôt

---

13. *Règlement précisant les renseignements auxquels le public a accès*, DORS/2001-7, art. 1(e)

Canada est plutôt stricte<sup>14</sup>, et il est donc difficile de conclure que cela peut comprendre les encyclopédies ouvertes en ligne comme Wikipédia. Dans tous les cas, il est nécessaire d'analyser si la personne concernée est bien à l'origine de la fourniture de ses renseignements personnels sur le site Internet en question, avant de l'utiliser sans son consentement, et de déterminer si l'utilisation que la SGC souhaite en faire est directement liée aux fins pour lesquelles les personnes ont rendu publics leurs renseignements.

Existe-t-il des dispositions similaires dans la loi québécoise ? Une disposition similaire n'existe pas dans la loi provinciale, qui énonce uniquement en son article 1 que « [l]es sections II et III de la présente loi ne s'appliquent pas à un renseignement personnel qui a un caractère public en vertu de la Loi »<sup>15</sup>. La loi à laquelle il semble être fait référence ici est la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*<sup>16</sup>, qui ne concerne que les renseignements personnels de membre d'organismes publics<sup>17</sup>. Ainsi, il est raisonnable de conclure, qu'en l'état de la réglementation, ce n'est pas parce que les renseignements personnels sur des artistes ou auteurs sont déjà publics, par exemple sur Wikipédia, qu'ils perdent leurs caractéristiques de renseignements personnels. Un consentement de la personne concernée devrait donc être recherché pour utiliser de tels renseignements. Il serait nécessaire de clarifier ce point sur le régime encadrant les informations accessibles au public dans les réformes portant sur la loi fédérale, mais surtout sur la loi provinciale (voir la section suivante).

14. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Information accessible au public », mars 2014, en ligne : <[https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privée/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations\\_06\\_pai/](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privée/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_06_pai/)>.

15. *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 8, art. 1, al. 5.

16. RLRQ, c. A-2.1. Voir l'article 57 de la loi : « Les renseignements personnels suivants ont un caractère public : 1° le nom, le titre, la fonction, la classification, le traitement, l'adresse et le numéro de téléphone du lieu de travail d'un membre d'un organisme public [...] ».

17. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Rapport quinquennal 2016*, version abrégée, 2016, en ligne : <[https://www.cai.gouv.qc.ca/documents/CAI\\_RQ\\_2016\\_res.pdf](https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016_res.pdf)>. Voir note 32 à la page 22 de l'analyse des données ouvertes par la Commission : « Parmi les renseignements personnels que la loi déclare publics, on peut penser aux noms et aux coordonnées professionnelles des employés et dirigeants des organismes publics, *Loi sur l'accès*, art. 57, al. 1, par. 1, 2 et 3 et au rôle d'évaluation, *Loi sur la fiscalité municipale*, RLRQ, c. F-2.1, art. 73 ».

Au-delà, de leurs caractères publics, est-ce que les renseignements relatifs à des contenus musicaux pourraient être partagés de manière ouverte ? Tout d'abord, afin de dissiper toute incompréhension, il est nécessaire de distinguer les « données ouvertes » des « données publiques ». Les données ouvertes désignent davantage une manière de diffuser la donnée, plutôt qu'une caractéristique. Les données diffusées de manière « ouverte » englobent généralement toutes les données non protégées par des droits de propriété intellectuelle ou tout autre droit ayant des effets similaires. Les données ouvertes sont ainsi librement accessibles et réutilisables sans contrainte. Elles sont généralement diffusées par les administrations publiques, mais cela peut être tout autre organisme suivant la même méthode, sous une licence ouverte garantissant leur libre accès et leur réutilisation.

Ce sont par exemple les études, les rapports de recherches ou de statistiques, produits par un organisme public dont la diffusion présente un intérêt pour l'information du public<sup>18</sup>, ou des données qui permettent de savoir quelle part de l'argent de nos impôts est consacrée aux marchés publics par exemple<sup>19</sup>. Cependant, toutes les données ne peuvent pas être diffusées de manière ouverte. Ainsi, les renseignements personnels ne peuvent être diffusés de manière ouverte, de même que les informations confidentielles, ou celles couvertes par un droit d'auteur sans l'autorisation de l'ayant droit. D'où l'importance pour une organisation de bien identifier au préalable les renseignements personnels dans les informations qu'elle souhaite diffuser de manière ouverte. Ainsi, selon la Commission d'accès à l'information du Québec :

La loi québécoise permet la diffusion de données ouvertes sur des individus dans la mesure où elles sont anonymisées, c'est-à-dire dépouillées « de l'ensemble des informations permettant d'identifier directement ou indirectement un individu ».<sup>20</sup>

De même, selon le site de Données Québec, les données publiées comme données ouvertes ne peuvent contenir des renseignements

18. GOUVERNEMENT DU QUÉBEC, CONSEIL DU TRÉSOR, *Guide de priorisation et de diffusion des données ouvertes*, 2018, en ligne : <[https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/SCT/vitrine\\_numeriQc/gouvernement\\_ouvert/Guide\\_priorisation.pdf?1595962618](https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/SCT/vitrine_numeriQc/gouvernement_ouvert/Guide_priorisation.pdf?1595962618)>.

19. GOUVERNEMENT DU CANADA, « L'abc des données ouvertes », en ligne : <<https://ouvert.canada.ca/fr/principes-de-donnees-ouvertes>>.

20. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Rapport quinquennal 2016*, préc., note 17, p. 23.

personnels, même des renseignements personnels à caractère public<sup>21</sup>. Les données ouvertes ne peuvent donc pas contenir, en principe, de renseignements personnels. Les contraintes prévues par les réglementations sur l'utilisation des renseignements personnels viennent en effet en contradiction avec les principes de données ouvertes : selon ces réglementations, il faut notamment informer l'individu de toute utilisation et communication de ces renseignements, et du nom des tiers auxquels les renseignements personnels pourraient être communiqués, alors que le principe de données ouvertes est de disséminer l'information sans contrainte.

Nous avons vu quels types de données des SGC pourraient être concernées par les réglementations sur les renseignements personnels ; il faut désormais s'interroger sur l'application territoriale de telles réglementations face aux flux transfrontaliers des données.

## B- Champ d'application territorial

### 1. *Entre lois fédérales et provinciales*

Au niveau fédéral, la PIPEDA s'applique aux organisations qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre d'« activités commerciales ». A priori, les organismes à but non lucratif sont donc exclus, comme les organismes de défense des droits, les groupes communautaires, ou les clubs<sup>22</sup>. Les sociétés de gestion collective, pour la plupart, ont ce statut d'organisme sans but lucratif puisqu'elles ne prélèvent généralement que des frais d'administration sur les redevances qu'elles collectent

21. GOUVERNEMENT DU QUÉBEC, *Guide de priorisation et de diffusion des données ouvertes*, préc., note 18, p. 5 :

« [...] Préciser les enjeux reliés à la protection des renseignements personnels (PRP). Déterminez les renseignements personnels, c'est-à-dire ceux qui concernent une personne physique et qui permettent de l'identifier, en vue de les anonymiser ou de les retirer à une étape ultérieure.

[...] **Recenser les renseignements personnels à caractère public en vue de les retirer.** Certains renseignements personnels sont déclarés publics par diverses lois dans un objectif précis. Ces renseignements, compte tenu du cadre légal actuel, ne peuvent, sauf exception, être inclus dans des jeux de données ouvertes. À cette étape, assurez-vous de les recenser en vue de les retirer avant la diffusion du jeu de données. »

22. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Application de la LPRPDE aux organisations caritatives et à but non lucratif », juin 2019 (dernière révision), en ligne : <[https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r\\_o\\_p/02\\_05\\_d\\_19/](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/02_05_d_19/)>.

et n'ont pas pour objectif de faire du profit. Elles pourraient donc être soustraites à l'application de la PIPEDA.

Toutefois, les organisations à but non lucratif ne sont pas systématiquement soustraites à son application<sup>23</sup>. Par exemple, la vente ou la location de listes d'adhérents est considérée comme étant une activité commerciale. Ainsi, toutes les activités commerciales des SGC sont soumises à la PIPEDA. De plus, certaines sociétés de gestion collective n'ont pas ce statut d'OBNL et il faut donc faire une analyse au cas par cas.

Par ailleurs, pour l'Alberta, la Colombie-Britannique et le Québec, il y a une substitution de la loi provinciale sur les renseignements personnels à la PIPEDA pour les affaires qui concernent leurs provinces. L'analyse des lois pour l'Alberta et la Colombie-Britannique ne sera pas faite dans cet article, mais il est important de s'y référer dans le cas d'une SGC établie dans ces provinces qui pourrait y être soumise, même avec le statut d'OBNL. Ainsi, au Québec, la loi provinciale vient se substituer à la PIPEDA dans le cadre des affaires interprovinciales et à la différence de la PIPEDA, elle n'exclut pas son application aux organismes sans but lucratif, et s'applique à toutes « entreprises ». Cela comprend les associations au terme de l'article 96 de la loi<sup>24</sup>. Les sociétés de gestion collective établies au Québec sont donc en principe soumises à cette loi, même avec un statut d'association.

Cependant, lorsqu'une loi provinciale se trouve à s'appliquer en lieu et place de la loi fédérale, la PIPEDA considère qu'elle continue à s'appliquer concernant les transferts interprovinces et internationaux de données. Toutefois, quelle est la compatibilité entre les dispositions de la loi provinciale et fédérale sur les dispositions sur les transferts

---

23. « La question de savoir si des renseignements personnels sont recueillis, utilisés ou communiqués dans le cadre d'une activité commerciale ne dépend pas du fait que l'organisation est une organisation à but non lucratif ou non aux fins de l'imposition (*Rodgers c. Calvert*, [2004] 244 D.L.R. (4th) 479) » : Commissariat à la protection de la vie privée du Canada, en ligne : <[https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations\\_03\\_ca/](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_03_ca/)>.

24. Art. 96 LPRPSP : « Une association ou une société qui exploite une entreprise et détient des renseignements personnels sur ses membres ou sur des tiers a les mêmes droits et les mêmes obligations à l'égard de ses membres et des tiers que la personne qui exploite une entreprise. »

internationaux ? Ainsi, le groupe d'étude européen sur la protection des données personnelles a pointé ces incohérences :

En conclusion, les positions prônées par l'État fédéral et la province sur le champ d'application de la loi québécoise divergent. Si le Commissariat à la protection de la vie privée du Canada considère que la législation fédérale s'applique aux transferts tant interprovinciaux qu'internationaux des renseignements personnels, la CAI considère que la loi québécoise s'applique toujours aux situations internationale.<sup>25</sup>

Il est donc souhaitable que ces incohérences soient réglées par les réformes à venir des lois provinciales et fédérales.

## **2. *Entre lois nationales et internationales***

Les flux de renseignements personnels sont aujourd'hui, avec l'essor d'Internet et des technologies du numérique, par nature, transfrontaliers et internationaux. Les législations venant réglementer ces flux de données personnelles ont donc dû s'adapter à cette extraterritorialité. Ainsi, alors que les lois sont, par principe, attachées à une juridiction et à un État, certaines réglementations sur les données personnelles ont adopté un champ d'application extraterritoriale afin de faire face à cette nature transfrontalière des flux de données. C'est le cas du RGPD qui a, de manière inédite, une application extraterritoriale s'étendant à des entreprises situées en dehors du sol de l'Union européenne et qui peut donc s'appliquer à des sociétés canadiennes qui traitent des renseignements personnels sur son sol ou des renseignements de citoyens européens.

Dans le cadre des SGC du domaine musical, une société représente, d'une part, des musiciens de son pays d'établissement, mais qui peuvent résider ou non dans ce pays, ou être ou non citoyens de ce pays. D'autre part, elle représente, du fait des accords de réciprocité qu'elle a conclus avec ses sociétés sœurs à l'étranger, des musiciens d'autres pays dont elle gère les droits d'auteur au Canada. Cela peut ainsi comprendre de nombreux citoyens de l'UE.

Il est donc légitime de se demander si le RGPD peut s'appliquer aux SGC canadiennes dans leur activité.

---

25. COMMISSION EUROPÉENNE, Groupe de travail sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel, *Avis 7/2014 sur la protection des données à caractère personnel au Québec*, 4 juin 2014, p. 5, en ligne : <<https://www.dataprotection.ro/servlet/ViewDocument?id=1290>>.

- *Dans le traitement des données des adhérents des SGC canadiennes*

On l'a dit, l'une des particularités du RGPD est son application extraterritoriale, ce qui en fait un texte de loi inédit sur le plan international, puisqu'il va s'appliquer à des entreprises étrangères qui sont *a priori* en dehors de la juridiction de l'Union européenne, mais qui traitent des renseignements personnels d'Européens. À noter tout d'abord qu'il ne s'agit pas nécessairement de citoyens européens, mais de personnes localisées sur le territoire de l'UE, indépendamment de leur nationalité ou de leur lieu de résidence. Inversement, le traitement de renseignements à caractère personnel de citoyens européens qui sont localisés au Canada (par exemple, des résidents permanents adhérents d'une société de gestion canadienne) n'entraîne pas pour autant l'application du RGPD. Toutefois, le seul fait de traiter les données à caractère personnel d'une personne qui se trouve sur le territoire de l'Union ne suffit pas en soi à déclencher l'application du RGPD, il est nécessaire qu'un élément de « ciblage » soit présent dans le traitement, que ce soit en offrant des biens ou des services aux personnes concernées ou en suivant leur comportement.

Plus particulièrement, selon l'article 3 du RGPD, celui-ci s'applique dans les cas suivants :

- lorsqu'un traitement de données est effectué par un responsable de traitement ou un sous-traitant établi sur le territoire de l'Union européenne (que le traitement soit effectué ou non sur le territoire de l'UE) ;
- lorsque le traitement des données à caractère personnel est relatif à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non des dites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

Sur ce point de l'application du RGPD aux entreprises québécoises, le gouvernement du Québec a d'ailleurs réalisé un guide<sup>26</sup>, qui dispose notamment que :

26. INVESTISSEMENT QUÉBEC INTERNATIONAL, « Règlement général sur la protection des données de l'Union européenne – Quelles répercussions sur

toute entreprise et tout organisme québécois faisant le traitement de données d'individus (personnes physiques) se trouvant sur le sol européen peuvent être concernés, que les données personnelles soient hébergées au Canada, en UE ou ailleurs dans le monde. Toute entreprise doit donc se conformer au règlement si elle effectue du traitement de données à caractère personnel et offre des biens et des services à des personnes physiques sur le territoire de l'UE, qu'il y ait vente ou non. Le règlement touche également les responsables du traitement des données ou les sous-traitants, tant québécois qu'euro péens, qui effectuent des activités de suivi du comportement dans le but d'établir un profilage d'une personne physique, « de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit ». <sup>27</sup>

Tout d'abord, à quoi fait référence ce dernier critère du « suivi de comportement » ? Cela fait référence à un traitement de renseignements personnels de personnes physiques suivies sur Internet, consistant en un profilage de la personne, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit. Plus précisément, les situations de profilage réfèrent par exemple aux situations :

pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements, dès lors qu'il produit des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative. <sup>28</sup>

Compte tenu de ces considérations, le profilage ne se trouve pas à s'appliquer dans le cadre de la gestion collective.

L'autre critère pouvant donner lieu à l'application du RGPD est lié à l'offre de biens ou de services à des personnes concernées dans l'Union, qu'un paiement soit exigé ou non des dites personnes. La plupart des adhérents des SGC canadiennes sont résidents au Canada

---

les entreprises québécoises ? », en ligne : <<https://www.economie.gouv.qc.ca/bibliotheques/outils/outils-a-lexportation/reglement-general-sur-la-protection-des-donnees-de-lunion-europeenne/>>.

27. *Ibid.*

28. *Attendu 71, Règlement Général sur la Protection des Données, (UE) 2016/679.*

et/ou de nationalité canadienne. Pour ces derniers, le traitement de leurs renseignements personnels n'est pas soumis au RGPD, mais aux lois fédérales et provinciales canadiennes. Toutefois, certains adhérents de ces sociétés sont résidents dans l'Union européenne. Pour les sociétés de gestion collective québécoises par exemple, plusieurs auteurs ou artistes de musique bien connus ont leurs résidences en France. Est-ce que le RGPD s'applique à eux pour le traitement de leurs renseignements personnels ?

Selon les lignes directrices relatives au champ d'application du RGPD<sup>29</sup> du Comité européen sur la Protection des Données, il est nécessaire qu'il y ait un ciblage, une offre de service qui cible un résident de l'UE. Toutefois :

[...] la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention.<sup>30</sup>

Ainsi, si une SGC canadienne adopte des démarches spécifiques de recrutement pour s'adresser à des résidents européens, par l'intermédiaire de la publicité ou d'affichage sur son site Internet par exemple, elle pourrait être soumise au RGPD pour le traitement des renseignements personnels des résidents européens. Mais s'il s'agit simplement d'un adhérent qui a déménagé en Europe, le traitement de ces renseignements personnels ne sera pas nécessairement soumis au RGPD et restera soumis aux réglementations canadiennes fédérales et/ou provinciales. Ainsi, si une société de gestion canadienne n'a pas l'intention de recruter des adhérents sur le territoire de l'Union européenne, en proposant par exemple d'administrer leurs droits d'auteur et de percevoir leurs redevances pour ces territoires, alors le critère de ciblage ne sera très probablement pas constitué, et le RGPD ne s'appliquera pas à ce traitement de données.

Toutefois, attention, cela ne signifie pas que le RGPD ne va pas trouver à s'appliquer à l'ensemble de l'activité d'une telle société de gestion canadienne, qui pourrait être soumise aux obligations de sous-traitant ou de co-traitant en tant que récipiendaire de renseignements

29. COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (art. 3)*, version 2.0, 12 novembre 2019, en ligne : <[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_3\\_2018\\_territorial\\_scope\\_fr.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_fr.pdf)>.

30. *Ibid.*, p. 19.

personnels de ses sociétés sœurs à l'international, comme nous le verrons dans la section suivante.

– *Dans le traitement des données de ses sociétés sœurs*

Lorsqu'une SGC canadienne communique les renseignements personnels de ses adhérents à une société sœur basée dans l'Union européenne, elle est assujettie aux obligations de la loi provinciale et fédérale de protection des renseignements personnels sur les transferts internationaux (voir la section suivante sur l'encadrement des transferts de données à l'étranger).

De son côté, la société sœur, lorsqu'elle est basée dans l'UE, sera assujettie au RGPD dans son activité et devra encadrer le transfert des renseignements personnels de ses adhérents vers le Canada par les mécanismes contractuels appropriés (soit, le plus souvent, par une décision d'adéquation ou une clause contractuelle Type). Mais lorsqu'elle reçoit les renseignements personnels de ses sociétés sœurs étrangères, la SGC canadienne intervient-elle comme « sous-traitante » de la société européenne, ou bien comme « responsable de traitement », ou encore « responsable conjointe » du traitement, au sens du RGPD ?

Il est important de déterminer ce statut au sens du RGPD, car cela détermine le degré de responsabilité de la SGC canadienne par rapport aux données transmises par sa société partenaire européenne. Ainsi, comme la CISAC le confirme dans son étude, les organisations de gestion collective non européennes recevant des données personnelles depuis des sociétés de gestion européennes engagent leur responsabilité envers les individus concernés par le transfert de données<sup>31</sup>. Même le sous-traitant peut voir sa responsabilité engagée directement envers les personnes concernées.

Cette évaluation du statut est toujours délicate à faire et il faut généralement regarder la situation au cas par cas. Cela peut en effet dépendre des accords conclus entre chaque société de gestion. Par principe, un responsable de traitement détermine les moyens et les buts du traitement des renseignements personnels, alors qu'un sous-traitant traite les données au nom d'un responsable de traitement et selon ses instructions. Si le sous-traitant participe à définir les buts du traitement et les moyens, ou traite des données personnelles en dehors des instructions du responsable de traitement, alors il pourra

---

31. Voir p. 12, « CISAC Guide to the General Data Protection Regulation », May 2018.

être considéré comme un responsable conjoint<sup>32</sup>. Les contrôleurs de données conjoints doivent répartir leurs responsabilités respectives concernant le respect du RGPD, notamment lorsqu'il s'agit d'exercer le droit des personnes, et ils devront établir un contrat pour déterminer pour quelle obligation chacun d'entre eux sera considéré comme responsable.

Dans le cas de la gestion collective, une SGC canadienne pourrait être amenée à traiter les données en tant que sous-traitant d'une société de l'UE, mais aussi en tant que responsable conjoint puisqu'elle va parfois traiter les données selon ses propres moyens (sa base de données ou sa technologie de « matching » avec ses données d'usage domestique), en dehors d'instructions spécifiques et parfois pour ses propres finalités. Toutefois, la CISAC ne retient pas cette qualification de « responsable conjoint » dans le cas des sociétés de gestion collective d'auteurs. Ainsi, selon l'organisation, les sociétés membres qui partagent des renseignements personnels sur leurs adhérents sont des contrôleurs de données indépendants, et non des contrôleurs joints, sauf exception<sup>33</sup>. Ainsi, selon cette qualification, chaque société de gestion collective serait un contrôleur indépendant en relation avec les renseignements personnels qu'elle traite pour les finalités de leur accord bilatéral et est responsable de s'assurer de la conformité du traitement avec la loi sur la protection des données applicables lorsqu'elle collecte les renseignements personnels auprès de ses adhérents, lorsqu'elle les traite et les fait parvenir à une société étrangère, mais aussi lorsqu'elle reçoit et traite les renseignements personnels des adhérents de sa société sœur, dans le but d'exécuter l'accord bilatéral et de collecter les redevances des ces derniers dans son pays de localisation.

### **3. Encadrement des transferts de données à l'étranger**

Dans le cadre des échanges entre les sociétés sœurs, chaque société fait parvenir des informations sur son répertoire aux autres sociétés avec lesquelles elle a des accords, et reçoit également des informations du répertoire de ces sociétés.

---

32. Voir p. 3, « CISAC Guide to the General Data Protection Regulation », May 2018.

33. « As a rule, ciSac Societies sharing Personal data on affiliates are independent (and not joint) data controllers. However, there may be circumstances where one ciSac member society acts as a data processor on behalf of another ciSac member society. The ciSac society requesting the service of the other member of society is the only data controller », p. 15, « CISAC Guide to the General Data Protection Regulation », mai 2018.

– *Données transférées du Canada vers l'étranger*

Dans le cas de transfert de données interprovinciales ou vers l'international, la Commission d'accès à l'information, organisme gouvernemental québécois responsable de mettre en œuvre les politiques de protection des renseignements personnels au Québec, considère qu'à la fois la loi fédérale PIPEDA et la loi québécoise s'appliquent<sup>34</sup>. Ainsi, tout d'abord, la loi québécoise dispose, concernant l'encadrement des transferts internationaux, que les renseignements personnels communiqués doivent bénéficier d'« un degré comparable de protection » comparativement à celui dont elles jouissent au Canada. De même, le principe 4.1.3 de l'annexe 1 de la loi PIPEDA dispose que :

Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

Dans les deux cas, les SGC canadiennes devront donc s'assurer que les sociétés à qui elles transfèrent des renseignements personnels respectent un degré de protection comparable à la loi applicable à sa situation. Le respect de ces engagements se fait généralement par le biais des accords de représentation bilatéraux ou unilatéraux entre sociétés.

– *Données transférées de l'UE vers le Canada et le Québec*

Plusieurs mécanismes existent pour encadrer le transfert des données de l'UE vers l'étranger. Tout d'abord, si le pays de réception des données a été reconnu comme offrant une protection adéquate par une décision d'adéquation de la Commission européenne, alors le transfert peut se faire selon les moyens réguliers mis en œuvre par le RGPD. Le Canada est un des seuls pays à bénéficier d'une telle décision d'adéquation. Cependant, cette décision ne concerne que les situations où la loi fédérale « PIPEDA » trouve à s'appliquer<sup>35</sup>. Comme on l'a vu, cette loi s'appliquant aux entreprises, elle a donc

34. COMMISSION EUROPÉENNE, *Avis 7/2014 sur la protection des données à caractère personnel au Québec*, préc., note 25.

35. *Décision 2002/2/CE de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents*

une application limitée aux sociétés de gestion collective, qui sont bien souvent des organismes sans but lucratif. De plus, cette décision date de 2001 et est basée sur l'ancienne directive européenne précédant le RGPD ; il est donc recommandé de l'analyser avec précaution. C'est l'une des raisons pour lesquelles le gouvernement fédéral cherche à moderniser la loi par le projet de loi C-11, afin de s'aligner sur les nouvelles exigences de la législation européenne.

Par ailleurs, concernant le Québec, un avis du groupe de travail européen sur les données personnelles dit « de l'article 29 » qu'il est venu relativiser en 2014 l'application de la décision d'adéquation de la Commission européenne au Canada, s'agissant de la loi québécoise sur la protection des renseignements personnels<sup>36</sup>. Cette étude intéressante démontre les lacunes importantes de la loi québécoise qui date de 1993. On l'a vu, le groupe de travail a d'abord pointé des incohérences entre les domaines d'applications de la loi fédérale et provinciale sur les transferts de données en dehors de la province et à l'étranger. Alors que l'office fédéral considère que la législation fédérale s'applique à la fois aux transferts interprovinciaux et internationaux, la CAI provinciale considère que la loi québécoise s'applique toujours dans les situations de transferts internationaux. Selon le groupe de travail, il était donc essentiel de clarifier ce point avant que la décision d'adéquation de la Commission européenne s'applique à la législation québécoise. À noter que la réforme de la loi sur les renseignements personnels amenés par le projet de loi 64 pourrait répondre aux incohérences pointées par ce groupe de travail, notamment sur cette question du champ d'application pour les transferts internationaux.

En l'absence de décision d'adéquation, le RGPD permet également d'encadrer le transfert de données par d'autres mécanismes : dans le cas d'un groupe d'entreprises ou de sociétés engagées dans une activité économique conjointe, des règles d'entreprise contraignantes ; des dispositions contractuelles avec le destinataire des données à caractère personnel (il existe des clauses contractuelles types approuvées par la Commission européenne) ; ou encore, l'application d'un code de conduite ou d'un mécanisme de certification.

Sur cette question, la CISAC considère enfin que les transferts internationaux entre sociétés de l'UE et non UE devraient bénéficier de l'exemption de l'article 49 du RGPD. Le transfert de telles données

---

*électroniques [notifiée sous le numéro C(2001) 4539], [2002] J.O. L 2/13, en ligne : <<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002>>.*

36. COMMISSION EUROPÉENNE, *Avis 7/2014 sur la protection des données à caractère personnel au Québec*, préc., note 25.

fait en effet partie des fonctions fondamentales des SGC et ces organisations ont traditionnellement encadré ces transferts dans leurs accords de représentation, ainsi qu'informé leurs adhérents de l'utilisation de leurs données dans leur contrat d'adhésion. La CISAC a fait valoir que ces transferts devraient être considérés comme occasionnels et non répétitifs, et donc bénéficier de cette exemption. Toutefois, en attendant d'avoir les lignes directrices sur cet article 49, la CISAC recommande de faire appel à des clauses contractuelles types pour encadrer les transferts.

En l'attente de clarification sur le champ d'application de la décision d'adéquation à la législation québécoise, il est sans doute préférable de faire appel à de telles clauses types pour les transferts internationaux entre sociétés européennes et québécoises.

#### **4. Base de données partagée entre SGC**

On l'a dit, plusieurs organisations internationales regroupent des SGC de plusieurs pays et ont adopté des politiques communes afin de faciliter l'identification de leurs adhérents partout dans le monde à l'aide d'identifiants uniques. C'est par exemple le cas de la CISAC du côté auteurs-compositeurs qui a recours à l'IPI, ou la SCAPR du côté artistes-interprètes qui a recours à l'IPN. Que ce soit la CISAC ou la SCAPR, les deux organisations internationales ont leur siège dans des pays de l'Union européenne et ont un important nombre de sociétés membres basées dans l'UE. Quel est le régime de responsabilité relatif aux renseignements personnels présents sur ces bases de données partagées ?

S'agissant de la CISAC, elle considère que :

For the relationship between CISAC member societies and CISAC, member societies can be considered as Joint Data Controllers for the use of CISAC Tools and CISAC Directory. They must establish a contract between them to allocate responsibilities for compliance with GDPR. It is important for CISAC member societies to inform data subjects on the communication of Personal Data to CISAC, third parties and other CISAC member societies.<sup>37</sup>

De plus, le traitement des données sur cette base est soumis au RGPD :

---

37. Voir p. 6, « CISAC Guide to the General Data Protection Regulation », May 2018.

When Personal Data is transferred to be processed in a centralised EU-hosted and managed data basis (e.g. CIS-Net or CISAC Directory), access to and use of such Personal Data by the non-EU exporting entity is subject to GDPR compliance.<sup>38</sup>

Selon la CISAC, lorsque les sociétés membres téléchargent des renseignements personnels sur les outils communs mis en place par l'organisation, la CISAC et les sociétés membres sont donc soumises au RGPD en tant que « responsables conjoints » des renseignements personnels figurant sur ces outils. Ils ont donc une responsabilité commune, la CISAC ayant déterminé précisément dans ces directives le partage de responsabilité entre elle et les organisations membres.

La SCAPR (*Societies' Council for the Collective Management of Performers' Rights*) est une organisation à but non lucratif basée à Bruxelles, en Belgique, et qui regroupe les principales sociétés de gestion collective des droits des artistes-interprètes musicaux à travers le monde. La SCAPR met à la disposition de ses sociétés membres deux bases de données partagées pour faciliter leur collaboration : l'*International Performers Database* (IPD), et la *Virtual Recording Database* (VRDB). L'IPD permet d'identifier les artistes-interprètes en tant qu'individus qui se voient octroyer chacun un numéro distinct, l'IPN (*International Performer Number*). À la différence de l'IPD, la VRDB permet d'identifier les enregistrements sonores et les œuvres audiovisuelles auxquels ils participent. Ces deux bases de données permettent aux sociétés de gestion collective de différentes juridictions d'avoir un outil commun pour regrouper les enregistrements sonores et œuvres audiovisuelles et identifier les artistes-interprètes en cause.

Chaque société téléverse dans ces deux bases de données les informations relatives à ses adhérents et à leur participation. L'accès à ces bases de données est autorisé par la SCAPR à chaque société. Au même titre que la CISAC, la SCAPR considère que l'ensemble des sociétés qui téléversent des renseignements personnels sur les bases de données communes de l'IPD et de la VRDB sont collectivement considérées comme des « responsables conjoints » au sens du RGPD, selon les conditions posées par les accords relatifs à l'accès à ces bases de données. Toutefois, à la différence de la CISAC, la SCAPR n'interviendrait pas comme responsable conjoint avec les sociétés membres, mais comme sous-traitant de ces sociétés.

---

38. Voir p. 12, « CISAC Guide to the General Data Protection Regulation », May 2018.

On le voit, déterminer l'application aussi bien matérielle que territoriale est un enjeu complexe pour les SGC, tant le type de données qu'elles traitent est varié et le nombre qu'elle communique à l'étranger est important. Déterminer ce champ d'application précisément est donc une étape primordiale à leur processus de mise en conformité avec les réglementations sur les renseignements personnels.

## **II- CONFORMITÉ À LA LÉGISLATION APPLICABLE ET ANTICIPATION DES RÉFORMES À VENIR**

### **A- Démarches à suivre pour se conformer à la législation applicable**

Afin de se conformer aux règles applicables en matière de protection des renseignements personnels, la première étape pour une SGC canadienne est de déterminer la réglementation applicable au traitement des renseignements personnels de ses adhérents, entre la loi fédérale et provinciale, dépendant de sa localisation, mais aussi de son statut (organisation sans but lucratif ou non). De plus, il est important d'évaluer si l'organisation peut être soumise à des réglementations étrangères, dépendant du ciblage qu'elle pourrait être amenée à effectuer sur d'autres territoires, cela pourrait être le RGPD, mais aussi la loi américaine par exemple (la loi californienne est ainsi très protectrice des données personnelles des Californiens).

Une fois cette détermination effectuée, il est important de faire un état des lieux de la gestion des données personnelles par l'organisation, afin d'analyser quels renseignements personnels, au sens de la loi qui lui est applicable, elle collecte, où elle les conserve, pour quelle durée, et si leur conservation demeure nécessaire. Il est également important de noter que les SGC doivent collecter seulement les renseignements personnels nécessaires à la réalisation des fins pour lesquelles elles opèrent cette collecte ; il ne s'agit donc pas, par exemple, de demander l'orientation sexuelle de ses adhérents si ce n'est pas nécessaire au versement de leurs redevances.

Ensuite, il est important de vérifier que le recueil du consentement de collecte de renseignements personnels est bien valide selon la loi applicable à sa situation, ce consentement devant être par exemple manifeste, libre, éclairé, donné à des fins spécifiques et pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé, selon la réglementation québécoise. Il est également

nécessaire d'informer les adhérents de l'organisation sur la gestion de leurs renseignements personnels, par une politique de confidentialité des données adéquate, ainsi que sur leurs droits.

Par ailleurs, il est important de s'assurer d'encadrer les transferts de données personnelles des membres en dehors du Québec ou de la province en question, et particulièrement vers l'Union européenne, soit par des clauses contractuelles types, ou tout autre accord pertinent. Il faut également mener un audit des mesures de sécurité mises en place pour protéger les données personnelles au sein de l'organisation (mesures physiques, technologiques et administratives) et élaborer une politique de sécurité interne. Enfin, il est important de former les équipes de l'organisation concernant l'utilisation des données personnelles de ses adhérents, leurs exactitudes et mises à jour (notamment au moment des paiements), l'exercice des droits des adhérents sur leurs données, et les mesures de sécurité applicables.

## **B- Anticiper les réformes en cours du cadre réglementaire provincial et fédéral**

### **1. Au niveau du Québec**

Au niveau provincial d'abord, le gouvernement du Québec a déposé le projet de loi 64 le 12 juin 2020 visant à moderniser les dispositions législatives en matière de protection des renseignements personnels. Ce projet de loi vient notamment réformer la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « LPRPSP »). Avec ce projet de loi, le Québec pourrait devenir la première juridiction canadienne à suivre la tendance initiée par le RGPD, et plus récemment, par le *California Consumer Privacy Act* (CCPA) de 2018, et deviendrait la province canadienne ayant les obligations les plus strictes en matière de vie privée.

Cette réforme était nécessaire, tant le cadre juridique provincial datant de 1993 semblait aujourd'hui dépassé face aux flux de données personnelles, aux incidents récurrents touchant les renseignements personnels des Québécois, mais aussi à la nécessité d'être en conformité avec le cadre européen afin de permettre les échanges de données avec l'UE intrinsèques aux relations commerciales des entreprises. Toutefois, ce projet de loi ne devrait pas entrer en vigueur avant le début de l'année 2022, et l'étude du projet de loi en 2021 patine<sup>39</sup>.

39. Anthony AYLWIN *et al.*, « Le bout du tunnel est de moins en moins visible », *La Presse*, 1<sup>er</sup> avril 2021, en ligne : <<https://www.lapresse.ca/debats/opinions/>>

Deux des principaux enjeux pour les sociétés de gestion collective vont être le transfert des données personnelles hors Québec, ainsi que la durée de conservation des renseignements personnels.

- Transferts hors Québec (art. 17 du projet de loi) : Comme nous l'avons vu, les sociétés de gestion collective canadiennes ont des accords de réciprocité avec de nombreuses sociétés étrangères encadrant le transfert de renseignements personnels de leurs adhérents mutuels.

Le projet de loi 64 prévoit que les entreprises devront, avant de communiquer des renseignements personnels à l'extérieur du Québec, effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) afin de déterminer si les renseignements bénéficieront d'un niveau de protection équivalent dans le pays de destination et que, si à la suite de cette EFVP, le régime étranger n'est pas considéré comme équivalent, les renseignements personnels ne doivent pas être transmis. Cette évaluation doit notamment tenir compte de la sensibilité du renseignement, de la finalité de son utilisation, des mesures de protection dont le renseignement bénéficierait et du régime juridique applicable dans l'État où le renseignement serait communiqué. De plus, une liste des pays reconnus comme offrant une protection équivalente pourra être publiée (pour l'instant, cette liste n'est pas connue).

Nombre d'observateurs ont exprimé leurs réserves par rapport à cette évaluation, craignant que cela empêche les entreprises et organisations québécoises de transférer des renseignements personnels avec leurs partenaires étrangers, puisque de nombreux pays pourraient être considérés comme n'offrant pas une protection équivalente à la nouvelle législation québécoise.

Toutefois, il est important de préciser que le régime juridique applicable dans l'État où le renseignement communiqué ne serait qu'un des facteurs parmi d'autres à évaluer dans l'analyse préalable à la décision de communiquer ou non un renseignement à l'extérieur du Québec. Si le régime juridique ne fait pas partie de la liste des États et qu'il n'est pas considéré comme équivalent par rapport aux principes de protection des renseignements personnels applicables au Québec, il pourrait tout de même être possible de communiquer un renseignement personnel à l'extérieur du Québec. En effet,

---

[2021-04-01/protection-des-renseignements-personnels/le-bout-du-tunnel-est-de-moins-en-moins-visible.php](https://www25.international.gc.ca/2021-04-01/protection-des-renseignements-personnels/le-bout-du-tunnel-est-de-moins-en-moins-visible.php)>.

l'évaluation pourrait démontrer que le renseignement bénéficierait d'une protection équivalente si, par exemple, le transfert était encadré par des clauses contractuelles suffisantes et des mesures de sécurité adéquates au regard de la sensibilité des renseignements, conclues avec les sociétés présentes dans ce pays pour permettre de démontrer que le renseignement bénéficierait d'une protection équivalant à celle prévue à la *Loi sur le secteur privé* et permettre un transfert de renseignements personnels. Cependant, il serait nécessaire de confirmer cette possibilité dans la loi.

À l'heure actuelle, cette exigence du projet de loi 64 a été identifiée par le Commissaire à la protection de la vie privée du Canada comme un domaine où le projet de loi serait plus exigeant que le RGPD, en ne prévoyant pas formellement de mécanisme d'autorisation des transferts tels que les clauses types, les codes de conduite et règles d'entreprise contraignantes<sup>40</sup>.

- Conservation des données (art. 23 du projet de loi) : le projet de loi prévoit que, lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la société doit le détruire ou l'anonymiser selon les meilleures pratiques généralement reconnues en cette matière, sous réserve d'un délai de conservation prévu par une loi. Concernant cette dernière réserve, cela désigne les délais nécessaires pour respecter des obligations légales, par exemple en matière fiscale.

L'article 95 du projet de loi (3.2 de la *Loi sur le secteur privé*) précise qu'une entreprise doit établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels et propres à assurer la protection de ces renseignements, et doit notamment prévoir la durée de conservation et la destruction de ces renseignements. Ainsi, le délai de conservation d'un renseignement personnel doit être déterminé par l'entreprise en fonction des fins pour lesquelles les renseignements ont été recueillis et utilisés.

Dans le cadre de la gestion collective des droits d'auteur, les sociétés de gestion collective peuvent être amenées à conserver des

---

40. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Questions et réponses – projet de loi n° 64 », 24 septembre 2020, en ligne : <[https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/qa\\_20200924/](https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/qa_20200924/)>.

renseignements personnels à la suite du départ d'un adhérent, pour des impératifs de paiement de redevances ou de réclamations, pour des durées pouvant être liées à la prescription légale ou celle de protection des droits d'auteur, et il est fort probable que cela soit conforme aux exigences de durée du projet de loi, puisque cela correspond aux finalités de leur activité de gestion collective.

– Autres points de réformes importants :

D'autres enjeux du projet vont intéresser les SGC, par exemple l'octroi de nouveaux droits pour les individus inspirés du droit européen comme le droit à la portabilité des données et le droit à l'oubli, ou la création d'un nouveau rôle de « responsable de la protection des renseignements personnels » qui incomberait par défaut au président de l'entreprise, qui pourrait déléguer cette fonction par écrit à un membre du personnel, en tout ou en partie. Le projet de loi pose également l'obligation pour les entreprises d'établir, de mettre en œuvre et de publier sur leur site Web des politiques et pratiques, qui doivent prévoir « l'encadrement applicable à la conservation et à la destruction de ces renseignements, prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ceux-ci ». En termes de transparence des organisations, certaines informations spécifiques doivent être rendues disponibles lors de la collecte de renseignements personnels (notamment les fins auxquelles ces renseignements sont recueillis, les moyens de collecte, les droits d'accès et de rectification, etc.). Un autre point important concerne les exigences de consentement renforcées, et notamment la nécessité que ce consentement soit demandé à chacune des fins de collecte, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. Enfin, en termes de sanctions financières, la CAI aura le pouvoir d'imposer des sanctions pouvant aller jusqu'à un maximum de 25 millions \$ ou 4 % du chiffre d'affaires mondial.

Mais quelle va être l'harmonisation de ce projet de loi 64 avec le cadre fédéral et le projet de loi C-11 ?

## **2. Au niveau fédéral**

Le 17 novembre 2020, le gouvernement fédéral a présenté un projet de loi C-11, « Loi de 2020 sur la mise en œuvre de la Charte numérique », contenant une réforme de la PIPEDA dont la partie 1

pourrait être abrogée et remplacée par deux nouvelles lois sur les renseignements personnels, la *Loi sur la protection de la vie privée des consommateurs* (ci-après « LPVPC ») et la *Loi sur le Tribunal de la protection des renseignements personnels et des données* (ci-après « LTPRPD »).

Tout d'abord, un point important qui est modifié concerne le champ d'application de la loi. On l'a vu, la PIPEDA s'applique aux organisations qui recueillent et utilisent des renseignements personnels dans le cadre d'« activités commerciales », qui réfère à « la vente, troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds ». La LPVPC comprend une nouvelle définition de l'« activité commerciale », laquelle s'entend désormais de « toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial, compte tenu des objectifs de l'organisation qui exerce l'activité ou commet l'acte, du contexte dans lequel l'activité est exercée ou l'acte est posé, des personnes en cause et des résultats de l'activité ou de l'acte ». Cette définition d'activité commerciale, plus large que la précédente, pourrait avoir pour conséquence de concerner davantage les sociétés de gestion collective ayant un statut d'OBNL. Est-ce que, par exemple, le fait de prélever des frais de gestion sur les redevances qu'elle perçoit peut rendre l'activité de la société comme une « activité commerciale » au sens de cette nouvelle définition ?

De plus, concernant toujours le champ d'application de la LPVPC, celle-ci va être substituée par les lois provinciales dans la collecte, l'utilisation ou la communication des renseignements personnels survenant dans cette province. Toutefois, la LPVPC, au même titre que la PIPEDA, continuerait de s'appliquer aux communications d'une province à l'autre ou vers l'international. Il demeure donc a priori toujours les incohérences entre les domaines d'applications de la loi fédérale et québécoise sur l'encadrement des transferts de données en dehors de la province et à l'étranger, dont nous avons parlé ci-dessus.

Par ailleurs, concernant son contenu, le projet de loi crée des obligations renforcées pour les entreprises concernant la protection des renseignements personnels, dont les suivantes sont intéressantes pour les SGC : obtenir un consentement valide de leurs membres concernant le traitement de leurs renseignements personnels en leur expliquant dans un langage clair les traitements de leurs données dans le cadre de leur activité de gestion collective ; mettre à jour leurs politiques, pratiques et procédures pour se conformer aux nouvelles exigences de la loi ; ou encore, mettre en œuvre de

nouveaux droits des adhérents sur leurs renseignements personnels en plus des droits d'accès et de rectification déjà prévus, comme le droit à la « mobilité des renseignements », c'est-à-dire le droit de transférer leurs données d'une organisation à l'autre. Toutefois, ce droit ne s'appliquerait que si les deux organisations sont soumises à un « cadre de mobilité des données » prévu par règlement ; il faudra donc examiner si ce droit pourrait s'appliquer dans le cadre des SGC. Concernant, plus particulièrement, l'exigence de consentement, le projet de loi C-11 prévoit que l'organisation qui recueille, utilise ou communique des renseignements personnels doit d'abord obtenir le consentement de l'individu concerné, au plus tard au moment de la collecte des informations, ou, s'il s'agit d'autres fins que celles établies, avant de les utiliser ou de les communiquer à ces autres fins. Toutefois, le projet de loi introduit de nouvelles exemptions à l'exigence de consentement, notamment pour la collecte et l'utilisation de renseignements personnels effectuées dans le contexte d'une des « activités d'affaires » prévues, et cela à condition qu'une personne raisonnable s'attende à cette collecte et cette utilisation, et que les renseignements ne sont pas recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu. Parmi les « activités d'affaires » prévues figurent les activités nécessaires à la prestation d'un service demandé par l'individu. Compte tenu du fait que les adhérents de SGC fournissent généralement leurs renseignements personnels en connaissance de cause lors de leurs adhésions, et s'attendent raisonnablement à ce que leurs renseignements soient utilisés par la société dans son activité de gestion de ses redevances de droits d'auteur, les SGC pourraient probablement bénéficier de cette exemption au recueil de consentement, dans le cas où la loi fédérale s'appliquerait à leur situation. Toutefois, les autres obligations, liées notamment à l'information de l'adhérent, demeurent.

Enfin, de nouvelles sanctions sont prévues puisque le Commissaire à la protection de la vie privée du Canada pourrait, après investigation, transmettre à un nouveau Tribunal de protection des renseignements personnels des données un dossier de contravention, et les sanctions pécuniaires pourraient aller jusqu'à 25 millions \$ du CA ou un montant égal à 5 % du revenu global brut de l'organisation pour l'exercice précédent pour les manquements les plus graves.

## **CONCLUSION**

L'enjeu de la protection des renseignements personnels dans le cadre des SGC au Canada se concentre autour de quelques points

clés, qui concernent d'abord la question du champ d'application matérielle et territoriale des lois applicables à leur situation, tant le type de données qu'elles traitent est varié et le nombre qu'elle communique à l'étranger peut être important. Cela concerne aussi les questions de transfert de ces renseignements personnels à l'étranger, de l'exercice des droits de leurs adhérents sur leurs renseignements (notamment, un éventuel nouveau droit à la portabilité des données) ou encore de durées de conservation de ces renseignements, nécessaire à la continuité de leur activité. Il apparaît important que le cadre juridique québécois et canadien sur les renseignements personnels se modernise, notamment pour préciser des questions comme la collecte de renseignements déjà publics sur Internet, mais aussi régler les incohérences sur l'application des lois quant aux transferts interprovinciaux et internationaux.

S'ils sont adoptés, les projets de loi C-11 et 64 sont des projets ambitieux qui vont dans la bonne direction, mais il reste à garantir l'adéquation de ces deux nouveaux régimes entre eux, et aussi avec les législations a priori plus protectrices comme le RGPD. S'il reste du chemin avant l'adoption définitive de ces deux projets de loi, il est important de suivre avec attention les développements législatifs de ces prochains mois et les SGC pourront d'ores et déjà commencer à analyser leurs pratiques à l'aune de ces projets de loi sur un enjeu souvent délaissé, afin d'adopter une protection des renseignements personnels de leurs adhérents en conformité avec ces nouvelles exigences.