Université de Montréal

La portabilité des données personnelles des consommateurs, ses aspects juridiques dans l'Union européenne, au Canada et au Québec : applications, possibilités et risques

Par

João Flávio da Silva Amorim Boueres

Faculté de Droit

Mémoire présenté en vue de l'obtention du grade de Maîtrise en droit des technologies de l'information (LL. M.)

Novembre 2023

Résumé

La portabilité des données personnelles des consommateurs est encore une question récente dans le domaine de la protection de la vie privée. Parmi les normes étudiées dans ce travail, le Règlement Général sur la Protection des Données a été le premier à aborder la portabilité et le concept qu'il a établi guide d'autres législations, telles que celles du Québec et du Canada.

L'objet de ce mémoire est de discuter de la mise en œuvre de ce nouveau droit lié aux technologies de l'information et à la circulation des données personnelles, en se concentrant sur les consommateurs et les entreprises qui feront partie de la portabilité des données personnelles.

Cette étude est divisée en trois chapitres. Le premier explore les concepts de base liés au droit à la portabilité, tels que les données personnelles, les données liées à la relation avec le consommateur, la conceptualisation de la portabilité, son application et des exemples d'opérabilité.

Le deuxième chapitre décrit comment le droit à la portabilité a été adopté dans la législation de l'Union européenne, dans le projet de loi fédérale actuellement examiné par le Parlement canadien et dans la nouvelle loi québécoise.

La troisième traite de la mise en œuvre de la portabilité. Elle aborde le point de vue des entreprises, le maintien de la portabilité en tant que droit, le besoin de régulation, l'interopérabilité et les risques.

Mots-clés : portabilité, données personnelles, vie privée, projet de loi 64, projet de loi C-27, GDPR, interopérabilité.

Abstract

The portability of consumers' personal data is still a recent subject in the field of privacy protection. Among the standards studied in this work, the General Data Protection Regulation was the first to address portability and the concept it established guides other legislation, such as that of Quebec and Canada.

The purpose of this dissertation is to discuss the implementation of this new right linked to information technologies and the circulation of personal data, focusing on the consumers and businesses that will be affected by the portability of personal data.

This study is divided into three chapters. The first explores the basic concepts related to the right to portability, such as personal data, data related to the relationship with the consumer, the conceptualisation of portability, its application and examples of operability.

The second chapter describes how the right to portability has been adopted in European Union legislation, in the federal bill currently before the Canadian Parliament and in the new Quebec law.

The third deals with the implementation of portability. It addresses the point of view of businesses, the maintenance of portability as a right, the need for regulation, interoperability, and risks.

Keywords: portability, personal data, privacy, Bill 64, Bill C-27, GDPR, interoperability.

Table des matières

Liste des figures

Liste des sigles et abréviations

CAI : Commission d'Accès à l'Information du Québec

C.c.Q : Civil Code of Quebec

CPD : *Costumer Data Platforms*

EDPB : Comité européen de la protection des données (*European Data Protection Board*)

EIF : *European Interoperability Framework*

LAI : Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnel

LP : Loi sur la protection des renseignements personnels dans le secteur privé

LPRPDÉ : Loi sur la protection des renseignements personnels et les documents électroniques

LPRP : Loi sur la protection des renseignements personnels

LPVPC : Loi sur la protection de la vie privée des consommateurs

LTPRPD : Loi sur le Tribunal de la protection des renseignements personnels et des données

RGPD : Règlement Général sur la Protection des Données

UE : Union Européenne

À mon père, Paulo.

À mon grand-père, Flávio, qui a nourri ma passion pour le droit.

Remerciements

Mes premiers remerciements vont à ma femme, Sara. Son soutien inconditionnel et sa motivation sans faille ont rendu ce travail possible. Merci, mon amour.

Je voudrais également remercier ma famille, en particulier ma mère Beatriz, dont le dévouement et l'amour pour ses enfants sont incommensurables. Ma grand-mère, Celina, la personne la plus gentille et la plus douce au monde. Ma sœur, Anapaula, un exemple éternel de courage et de tendresse.

Merci au professeur Larouche d'avoir accepté la tâche ardue d'être le directeur de recherche d'un étudiant international dont le français n'est pas la langue maternelle et qui s'est engagé sur un sujet très complexe.

Professeur Gautrais, je me souviendrai toujours de vos leçons et de vos enseignements. Votre aptitude à enseigner et votre affection pour vos étudiants sont remarquables.

Le professeur Cristiano, l'une des personnes les plus dévouées aux études que je connaisse, qui a tendu la main à un étudiant qui venait d'arriver du Brésil pendant la pandémie et l'a aidé à tracer sa voie. Je ne le remercierai jamais assez.

Enfin, merci à mes amis. Ceux qui sont restés au Brésil et ceux que je me suis fait dans ce beau pays et cette belle province.

Introduction

La portabilité des données désigne la capacité des individus à transférer leurs renseignements personnels d'une organisation (entreprise) à une autre, ou à accéder à leurs données et à les utiliser sur différents services ou plateformes. Cela signifie que les consommateurs ont le contrôle de leurs propres données.

Cela promet de permettre au consommateur une plus grande flexibilité commerciale ainsi qu'une meilleure évaluation du marché. Du point de vue du commerçant, la portabilité peut augmenter la compétitivité, ce qui se traduira par des offres plus intéressantes pour les clients, permettre à de nouvelles entreprises d'entrer sur le marché (par exemple : les *fintechs* dans le système bancaire ouvert - *open banking*).

Toutefois, la mise en œuvre de ce système de portabilité des données personnelles pour les consommateurs (clients) n'est cependant pas une tâche simple. Il existe des défis opérationnels d'un point de vue technique pour minimiser les risques de sécurité des données. Il y a également des risques liés à la sécurité des données elle-même, puisqu'elle implique la communication de données personnelles entre différentes organisations, et les principes qui régissent ce type d'opérations doivent être sauvegardés.

L'analyse de l'application de cet outil dépend donc du respect des lois en vigueur. Dans ce contexte, le droit européen traite de la question depuis plus longtemps, tandis que le Québec a précédé le Canada en traitant de la portabilité dans la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (projet de loi provinciale 64), alors que le Canada travaille toujours sur le Projet de Loi C-27 (l'ancien Projet de Loi C-11, 2020).

Sur la scène européenne, l'article 20 du Règlement général sur la protection des données (RGPD 2016/679) traite du droit à la portabilité des données et accorde à la partie intéressée (propriétaire des données), la garantie d'exiger la transmission des données à un responsable du traitement autre que le responsable du traitement d'origine, sous réserve de critères techniques. Il ressort également de la lecture du RGPD, notamment à la lumière du considérant 68, que, si le

droit à la portabilité est un encouragement à l'interopérabilité, il ne crée pas pour les agents une obligation de maintenir des systèmes interopérables, et les conflits qui en résultent doivent être résolus en fonction de ce qui est techniquement possible.

Au Canada, le Projet de Loi C-27 crée *la Loi sur la protection de la vie privée des consommateurs* (LPVPC) et son article 72 permet au consommateur de consentir (ou d'exiger) de l'institution dans laquelle il a déjà déposé des données personnelles, qu'elle procède à la portabilité de celles-ci à un tiers, mais, contrairement au RGPD, ne confère pas le même statut au droit à la mobilité des données que celui conféré au droit d'accès aux renseignements personnels

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* du Québec adopte la même ligne de conduite du projet fédéral, parce que cette loi considère la mobilité des données comme une version améliorée du droit d'accès aux informations personnelles détenues par l'entreprise, et non comme un nouveau droit véritablement distinct.

Autrement dit, la portabilité des données est le fait de transférer des données d'une entreprise à une autre, à la demande de la personne concernée. En d'autres termes, si un particulier souhaite changer de fournisseur d'un service ou d'un produit, il lui suffit de demander la portabilité et l'entreprise devra transférer ses données personnelles à l'autre. De cette manière, la législation garantit la liberté du consommateur, évitant ainsi ce que l'on appelle le « *lock in* », qui rend difficile l'échange de services en raison de difficultés et de coûts élevés. Cependant, tous ces changements en termes de contrôle accru des données nécessitent l'existence de moyens d'interopérabilité entre les systèmes.

Il est observé que la législation susmentionnée crée le droit à la portabilité dans sa sphère de compétence respective. Cependant, l'applicabilité de ce droit est conditionnée par les termes vagues de la loi, une situation qui laisse les entreprises dans l'attente d'une réglementation plus objective sur la manière de procéder à la portabilité, en les protégeant et en les exposant à d'éventuelles sanctions, ainsi qu'en sauvegardant la protection des données des consommateurs.

Il se pose une discussion importante liée à la faisabilité de la portabilité elle-même, car, malgré ses nobles finalités, son efficacité dépend essentiellement de la résolution du problème d'interopérabilité entre le responsable du traitement qui enverra les données et le propriétaire ou le nouveau responsable du traitement qui les recevra.

L'action de l'organisme de réglementation est nécessaire pour assurer un maintien adéquat de la protection, en évitant une fragilité croissante au cours du processus qui sera adopté pour la migration des données personnelles et le consentement, moteur de la portabilité, doit être préservé comme un droit du consommateur et non comme un instrument de manipulation, où le consommateur sera amené à accorder ce consentement à n'importe quelle entreprise.

Ainsi, dans ce mémoire, seront recherchés les changements permis par les lois canadiennes et québécoises, leur applicabilité, l'expérience européenne, le besoin de réglementation et ce qu'elle devrait réaliser et les risques probables pour la sécurité, ainsi que les mesures qui peuvent être adoptées, permettant une application dans le monde de l'entreprise. Bien qu'elles puissent être mentionnées, les lois extérieures à celles précédemment traitées ne font pas l'objet de cette étude.

L'étude s'appuiera sur la norme européenne, la nouvelle législation québécoise et le projet de loi actuellement en discussion au parlement fédéral.

À cette fin, un support doctrinal sera utilisé, axé sur la conceptualisation des éléments traités (données personnelles, portabilité, sécurité, etc.), sous la forme d'une révision de la doctrine, ainsi que des recherches jurisprudentielles.

Chapitre 1 – Données personnelles des consommateurs et leur portabilité

La portabilité des données personnelles est encore un nouveau sujet dans le domaine de la protection des données et de la vie privée, il est donc nécessaire d'établir des concepts de base qui serviront à guider l'étude de la nouvelle matière avant d'entrer dans la législation proprement dite.

Il est essentiel d'établir le concept de données à caractère personnel et, plus précisément, de celles qui sont inhérentes aux relations avec les consommateurs, afin de comprendre l'objet de la portabilité et, par conséquent, de la définir.

Une fois ces concepts établis, on peut passer à la définition de la portabilité des données à caractère personnel, en elle-même, ainsi qu'à ses applications (tant du point de vue des consommateurs que des entreprises) et, enfin, à l'aspect le plus difficile, à savoir l'opérationnalisation de la portabilité. Ceci, toutefois, d'un point de vue plus technique que juridique.

Une fois ces bases posées, il est possible d'aborder les éléments déjà prévus dans les législations de l'Union européenne, du Canada et surtout du Québec.

1.1 Données personnelles et de consommation

Comme indiqué ci-dessus, il est nécessaire d'établir les concepts de données personnelles générales et d'informations personnelles des consommateurs.

En ce qui concerne les données relatives aux consommateurs, une brève analyse sera faite de la collecte et du traitement des données par les responsables du traitement, comme le prévoit la législation établie précédemment, puisque la portabilité s'applique lorsque le cycle de vie des données collectées est postérieur au consentement initial du consommateur.

Il convient de noter que la conceptualisation ne sera pas développée davantage, une brève définition étant suffisante aux fins de l'analyse du thème central du présent document.

1.1.1 Définition des renseignements personnels

Les renseignements personnels sont des informations qui permettent d'identifier leur propriétaire de diverses manières :

> Les données à caractère personnel sont des informations se rapportant à une personne vivante identifiée ou identifiable. Différentes informations, dont le regroupement permet d'identifier une personne en particulier, constituent également des données à caractère personnel.[1]

Selon l'article 4 du Règlement (UE) 2016/679 relatif à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation (ci-après RGPD), les données à caractère personnel sont considérées comme toute information concernant une personne physique identifiée ou identifiable :

> données à caractère personnel», 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;[2]

Le RGPD définit les données personnelles comme toute information relative à une personne physique identifiée ou identifiable. Cela signifie que, par exemple, un nom, associé à une adresse, ou un numéro d'identification fiscale et/ou de sécurité sociale constituent des données à caractère personnel. Mais les adresses électroniques, les éléments d'identité physique,

---

[1] « À quoi correspondent les données à caractère personnel? », en ligne : <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_fr> (consulté le 11 juillet 2023).

[2] *CE, Règlement (CE) 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), 2016 JO L1191* [*TEXTE consolidé*], en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX%3A02016R0679-20160504> (consulté le 10 juillet 2023).

les éléments génétiques ou physiologiques, les données obtenues par l'intermédiaire d'appareils électroniques (adresse IP et données de localisation), les données financières, les préférences sociales, etc. constituent également des données à caractère personnel.

Comme il ressort de cette notion large de données à caractère personnel, le règlement a hypothétiquement envisagé tout ce qui peut souvent permettre d'identifier la personne concernée.

Le Canada, selon la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ), a une définition plus ouverte, moins précise que celle mentionnée précédemment, de ce qui caractérise les données à caractère personnel : le renseignement personnel est « tout renseignement concernant un individu identifiable »[3].

La Loi sur la protection des renseignements personnels (LPRP), cependant, présente un concept plus défini :

> Renseignements personnels
>
> Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment :
>
> a) les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille;
>
> b) les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé;
>
> c) tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre;
>
> d) son adresse, ses empreintes digitales ou son groupe sanguin;
>
> e) ses opinions ou ses idées personnelles, à l'exclusion de celles qui portent sur un autre individu ou sur une proposition de subvention, de récompense ou de prix à

[3] *LC 2000, c 5 | Loi sur la protection des renseignements personnels et les documents électroniques*, en ligne : <https://www.canlii.org/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html?searchUrlHash=AAAAAQAHTFBSUERFIAAAAAAB&resultIndex=1> (consulté le 11 juillet 2023).

> octroyer à un autre individu par une institution fédérale, ou subdivision de celle-ci visée par règlement;
>
> f) toute correspondance de nature, implicitement ou explicitement, privée ou confidentielle envoyée par lui à une institution fédérale, ainsi que les réponses de l'institution dans la mesure où elles révèlent le contenu de la correspondance de l'expéditeur;
>
> g) les idées ou opinions d'autrui sur lui;
>
> h) les idées ou opinions d'un autre individu qui portent sur une proposition de subvention, de récompense ou de prix à lui octroyer par une institution, ou subdivision de celle-ci, visée à l'alinéa e), à l'exclusion du nom de cet autre individu si ce nom est mentionné avec les idées ou opinions;
>
> i) son nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet;[4]

Sur la base des concepts énoncés dans la loi, la jurisprudence (Cour fédérale) a pu établir ce qui caractérise une donnée comme étant personnelle :

> 33 Ainsi, les renseignements, quels que soient leur forme et leur support, sont des renseignements « concernant » un individu s'ils « permettent » d'identifier l'individu ou « rendent possible » son identification, que ces renseignements soient utilisés seuls ou combinés avec des renseignements d'autres sources, y compris les sources auxquelles le public a accès.[5]

Cette notion s'inscrit donc dans la lignée de la législation européenne (RGPD), en mettant l'accent sur la possibilité d'identifier la personne propriétaire des données collectées :

> In conclusion, the Canadian definitions of personal information in the Privacy Act and the PIPEDA have the cumulative requirements that the information allows the identification of an individual and that it is also "about" an individual, which requires an evaluation of the link between the information and the individual. The evaluative task is to be undertaken by reference to the purpose of the legislation. Where information does not involve subject-matter that engages an individual's privacy rights, the information is not personal information, even if it may identify an individual.

[4] *LRC 1985, c P-21 | Loi sur la protection des renseignements personnels*, en ligne : <https://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-p-21/derniere/lrc-1985-c-p-21.html> (consulté le 12 juillet 2023).

[5] *Gordon c. Canada (Santé)*, 2008 Cour fédérale, en ligne : <https://canlii.ca/t/28x7l> (consulté le 12 juillet 2023).

> However, this determination can make difficulties in some cases, particularly where it is unclear whether the information affects an individual in a personal capacity.[6]

> Si l'on s'en remet aux définitions courantes, collecter de l'information, c'est non seulement acquérir une nouvelle information mais de surcroît disposer sur celle-ci d'un contrôle effectif. Ainsi, le Grand dictionnaire terminologique définit collecte comme étant l' « action de rassembler des données de différentes provenances en vue d'un traitement informatique » ou l' « action de rassembler les données variables destinées à un traitement.[7]

La définition utilisée au Québec, à son tour, est plus proche du concept de la LPRPDÉ et dans le cadre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnel* (LAI ou Loi sur l'accès), dont l'article 54 stipule que « dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier »[8]. Ce concept est également énoncé dans la *Loi sur la protection des renseignements personnels dans le secteur privé* (LP ou *Loi sur le privé*), dans son deuxième article :

> Renseignement personnel.
>
> 2. Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.[9]

Afin de clarifier les termes pour la population, le gouvernement du Québec définit ainsi les données personnelles :

---

[6] Normann WITZLEB et Julian WAGNER, « When is Personal Data "About" or "Relating to" an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws », (2018) 4-1 *Canadian Journal of Comparative and Contemporary Law* 293.

[7] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010, en ligne : <https://www.lccjti.ca/doctrine/gautrais-v-et-trudel-p-circulation-des-renseignements-personnels-et-web-2-0/#ancre1221>.

[8] *RLRQ c A-2.1 | Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, en ligne : <https://www.canlii.org/fr/qc/legis/lois/rlrq-c-a-2.1/derniere/rlrq-c-a-2.1.html?searchUrlHash=AAAAAQBpTG9pIHN1ciBs4oCZYWNjw6hzIGF1eCBkb2N1bWVudHMgZGVzIG9yZ2FuaXNtZXMgcHVibGljcyBldCBzdXIgbGEgcHJvdGVjdGlvbiBkZXMgcmVuc2VpZ25lbWVudHMgcGVyc29ubmVsAAAAAAE&resultIndex=1> (consulté le 11 juillet 2023).

[9] *RLRQ c P-39.1 | Loi sur la protection des renseignements personnels dans le secteur privé*, en ligne : <https://www.canlii.org/fr/qc/legis/lois/rlrq-c-p-39.1/derniere/rlrq-c-p-39.1.html?searchUrlHash=AAAAAQBLIGxvaSBzdXIgbGEgcHJvdGVjdGlvbiBkZXMgcmVuc2VpZ25lbWVudHMgcGVyc29ubmVscyBkYW5zIGxlIHNlY3RldXIgcHJpdsOpAAAAAAE&resultIndex=1> (consulté le 11 juillet 2023).

> Un renseignement est personnel lorsqu'il concerne une personne physique et qu'il en permet, directement ou indirectement, l'identification. Voici ce qui le caractérise :
>
> il doit faire connaitre quelque chose à quelqu'un;
>
> il doit avoir un rapport avec une personne physique;
>
> il doit être susceptible de distinguer cette personne par rapport à une autre ou de reconnaitre sa nature.[10]

Cette conception plus ouverte n'entraîne cependant pas nécessairement un préjudice à l'application de la norme :

> La loi québécoise adopte donc une position plus générale en encadrant tout renseignement qui permettrait d'identifier une personne physique, sans restriction quant à la qualification des informations.[11]

Comme l'a expliqué le professeur Vincent Gautrais (Directeur du Centre de recherche en droit public, CRDP) dans une lettre adressée à la Commission d'accès à l'information du Québec (CAI) lors des discussions sur la mise à jour de la LP :

> En troisième lieu, notons que cette définition « minimaliste » n'empêche aucunement une interprétation évolutive de la notion. En effet, on constate notamment que de plus en plus, la définition de renseignement personnel est attachée au « dommage » ou au « risque de dommage » que sa circulation est susceptible d'occasionner. Cette précision interprétative est en effet requise afin de traiter des situations, de plus en plus fréquentes, où des renseignements personnels sont utilisés, et ce, sans qu'aucun danger pour l'individu ne soit susceptible de survenir. Il serait toutefois possible d'envisager une modification mineure visant à préciser qu'un renseignement personnel est un renseignement qui concerne une personne physique et qui, seul ou avec d'autres, permet de l'identifier. Cette précision se trouve, par exemple, à l'article 4 de la Loi de 2004 sur la protection des renseignements personnels sur la santé, L.O. 2004, c. 3 de l'Ontario. Une telle modification permettrait de minimiser les risques d'atteintes à la vie privée découlant des activités de couplage de

[10] « Présentation des concepts-clés liés aux renseignements personnels », *Gouvernement du Québec*, en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/concepts> (consulté le 17 juillet 2023).

[11] Bertrand SALVAS, *La protection de la vie privée sur le Web avec P3P : l'arrimage incertain du technique et du juridique | CanLII*, 2001, en ligne : <https://www.canlii.org/fr/doctrine/doc/2003CanLIIDocs491?zoupio-debug#!fragment//(hash:(chunk:(anchorText:''),notesQuery:'',scrollChunk:!n,searchQuery:/13226-current-1,searchSortBy:RELEVANCE,tab:toc))> (consulté le 12 juillet 2023).

> données, et ce, sans alourdir de manière inutile la définition du renseignement personnel.[12]

Le concept de renseignements personnels, qu'il soit plus ouvert ou plus fermé, établi dans les systèmes juridiques susmentionnés est donc intrinsèquement lié à la possibilité d'identifier le sujet, la personne physique qui a soumis ses données au système, même si la définition de l'identification n'est pas claire :

> I also discuss the fact that European courts, various academics and industry players don't agree on what "identifiability" actually means. While some take the position that the only relevant criteria for evaluating the status of IP addresses is the effort (or costs) involved in the identification process (while making no distinction between legal and illegal methods) others believe that the concept of personal information should be defined pragmatically, based upon the "likelihood of identification," Using the proposed method of interpretation, as the risk of subjective harm increases, the "effort and costs" necessary to consider this data as "identifiable" tend to decrease. Interestingly, certain industry players are already suggesting or implying that the extent of the risk of harm (upon the information being disclosed) should be taken into account to avoid being regulated by a burdensome framework that protects every single piece of data in circulation.[13]

Il est important de noter qu'une fois que la relation entre les données collectées et leur propriétaire n'est plus observée, grâce aux techniques d'anonymisation qui rendent impossible l'association des deux, les données ne sont plus qualifiées de personnelles, comme l'illustre la figure suivante :

[12] Vincent GAUTRAIS, « Rapport auprès de la Commission d'accès à l'information (CAI) », *Vincent Gautrais*, en ligne : <https://www.gautrais.com/blogue/2015/12/04/rapport-aupres-de-la-commission-dacces-a-linformation/> (consulté le 12 juillet 2023).

[13] Eloïse GRATTON, *Redefining personal information in the context of the Internet*, 2013 Accepted: 2017-12-05T15:28:32Z, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/19676> (consulté le 5 juillet 2023).

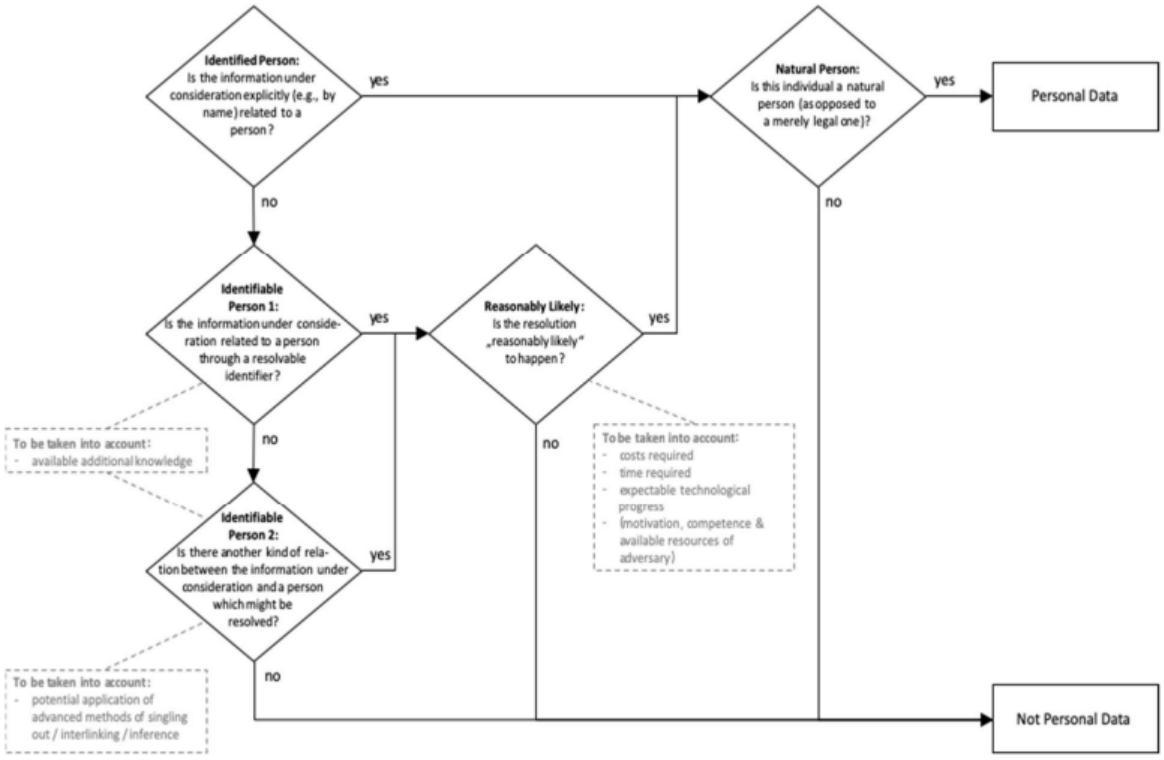

Figure 1. – « décrit le test à appliquer pour déterminer si une information constitue une donnée à caractère personnel » Michèle Finck et Frank Pallas, « They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR »,

Ainsi, une base est établie sur la notion de données personnelles faisant l'objet d'une protection juridique et nous passons aux données liées aux relations avec les consommateurs, qui représentent un sous-genre de celles traitées jusqu'à présent.

1.1.2 Définition des données relatives aux consommateurs

Les données à caractère personnel des consommateurs, c'est-à-dire les données issues de la relation entre le consommateur et le fournisseur de produits et de services, peuvent inclure certains des éléments mentionnés ci-dessus, mais peuvent être définies plus précisément comme des informations personnelles collectées, traitées et utilisées dans le cadre d'interactions, de transactions ou de relations avec les consommateurs.

Il s'agit également d'informations dérivées de l'utilisation d'Internet et pouvant provenir de l'accès aux réseaux sociaux, des services clients en ligne, des données de navigation sur les sites web, des applications, etc.

Ce type de données provient généralement de l'enregistrement des consommateurs lorsqu'ils achètent un produit ou reçoivent un service. Un autre exemple de collecte de données sur les consommateurs est l'étude de marché, dans laquelle des questions directes sont posées aux consommateurs, mais ce deuxième exemple n'a pas la même applicabilité en ce qui concerne la portabilité. Malgré l'importance de ce type des recherches, les entreprises ont privilégié les données issues des transactions commerciales qui donnent une image du profil du consommateur et sont plus complètes[14].

La collecte et l'analyse de ces données représentent un vaste champ commercial exploré par les entreprises, qui s'en servent pour gérer les relations avec les clients et les nouveaux clients potentiels. Cette méthode permet de cibler les offres et de se « rapprocher » des consommateurs.

Les données sont collectées et analysées de différentes manières, mais l'utilisation des plateformes de données clients (*Customer Data Platforms* - CDP), par exemple, est en plein essor. Il s'agit de logiciels qui combinent des données provenant de différents outils pour créer une base de données clients unique et centralisée et aider les entreprises à élaborer des stratégies de marketing. Toutefois, les entreprises sont confrontées au défi de mettre en œuvre cette pratique sans violer les droits inhérents à la protection de la vie privée.

Nous allons maintenant conceptualiser brièvement les aspects de la collecte et du traitement des données des consommateurs qui sont essentiels pour une meilleure compréhension du droit à la portabilité.

[14] Martin EVANS, « The data-informed marketing model and its social responsibility », dans *The data-informed marketing model and its social responsibility*, Policy Press, 2005, p. 99-132, DOI : 10.56687/9781847421272-006.

1.1.2.1 Le consentement

Le consentement est un élément fondamental dans la collecte des données à caractère personnel, en particulier dans le cas des consommateurs, comme décrit dans l'article 6 du RGPD, par exemple.

Le consentement est également l'un des principes régissant la mise en œuvre de la LPRPDE :

> Il est important que les organisations examinent la forme de consentement (explicite ou implicite) qui convient pour la collecte, l'utilisation ou la communication de renseignements personnels nécessitant l'obtention d'un consentement. Le consentement devrait généralement être explicite, mais un consentement implicite peut être suffisant dans des circonstances strictement définies. Les organisations doivent prendre en compte la nature sensible des renseignements et les attentes raisonnables de la personne, qui sont toutes deux fonctions du contexte.[15]

Le traitement des données est fondé sur un consentement libre, éclairé et explicite, visant à garantir la transparence de la collecte et la défense des intérêts de la personne concernée, conformément aux situations de légitimité auxquelles le responsable du traitement est soumis, sans lesquelles le traitement des données n'est pas licite.

En d'autres termes, il s'agit d'une autorisation expresse que la personne concernée donne à l'entreprise pour collecter, stocker, traiter ou utiliser ses données personnelles. Toutefois, cette autorisation doit être obtenue de manière claire et transparente, sur la base de détails concernant la finalité du traitement, les droits de la personne concernée et d'autres explications importantes afin que la personne concernée puisse prendre une décision en connaissance de cause.

D'une manière générale, c'est la personne concernée, c'est-à-dire la personne à laquelle se réfèrent les données, qui doit, si elle le souhaite - lorsqu'on le lui demande, de manière explicite

[15] Commissariat à la protection de la vie privée du CANADA, « Troisième principe relatif à l'équité dans le traitement de l'information de la LPRPDE – Consentement » (8 janvier 2018), 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/p_principle/principles/p_consentement/> (consulté le 1 août 2023).

et non équivoque - autoriser que ses informations soient utilisées par les entreprises et les organismes publics lorsqu'ils proposent des produits et des services, qu'ils soient gratuits ou non.

Commentant le projet de loi 64 du Québec, Simon Du Perron élucide la question du consentement :

> Le projet de loi prévoit que le consentement doit être demandé à chacune des fins pour lesquelles un organisme public ou une entreprise souhaite collecter, utiliser ou communiquer un renseignement personnel. Le projet de loi ajoute que la demande de consentement doit être formulée en termes simples et clairs et qu'elle doit être effectuée « distinctement de toute autre information communiquée à la personne concernée ». Cette notion de « consentement distinct » mériterait d'être éclaircie puisqu'il n'est pas clair si elle cherche à faire obstacle au consentement implicite ou si elle signifie plutôt que la politique de confidentialité d'un service doit être présentée à l'utilisateur de façon distincte et non être noyée dans des conditions générales d'utilisation. À cet égard, le projet de loi codifie une bonne pratique organisationnelle, à savoir le fait de rédiger les politiques de confidentialité en langage clair. En outre, le projet de loi spécifie que le consentement doit être manifesté de façon expresse dès qu'il s'agit de renseignement sensible, ce qui porte à croire qu'un consentement implicite serait acceptable dans des situations qui impliquent des renseignements non sensibles.[16]

Il convient de noter que le consentement est étroitement lié à la finalité, de sorte que le formulaire de consentement doit contenir une description détaillée de la finalité de la collecte des données, de la durée du traitement et de l'effacement.

Il existe également le droit de retirer son consentement, c'est-à-dire de revenir sur le consentement donné à un responsable du traitement des données. Ce droit est accordé parce que même si vous consentez au traitement, les données appartiennent toujours aux personnes concernées.

La conceptualisation du consentement est très importante pour la notion de portabilité, car les données à caractère personnel couvertes par le consentement sont celles fournies avec

[16] Simon DU PERRON, « Projet de loi 64 : une réforme à l'Européenne du droit à la protection des renseignements personnels », *Laboratoire de cyberjustice*, en ligne : <https://www.cyberjustice.ca/2020/06/17/projet-de-loi-64-une-reforme-a-leuropeenne-du-droit-a-la-protection-des-renseignements-personnels/> (consulté le 1 août 2023).

votre accord et celles générées par l'activité de la personne concernée, par exemple lorsqu'elle utilise un service ou un appareil.

En outre, il n'y a pas de circulation de données sans consentement :

> Dans l'immense majorité des lois visant à assurer la protection des renseignements personnels, le consentement est partout. Une fréquence d'ailleurs qui ne semblait pas forcément de mise dans les tous premiers textes internationaux évoquant la protection des renseignements personnels. Ainsi, il est clairement établi qu'aucune « circulation » ne peut être faite – que ce soit sous l'appellation de « communication », « collecte », « utilisation », etc. – sans que l'individu concerné n'ait consenti à cette opération.[17]

Le consentement change donc quelque peu de définition lorsqu'on parle de portabilité, il devient une sorte de demande de transmission de la part du détenteur, comme nous le verrons plus loin.

1.1.2.2 La finalité

En résumé, la finalité du traitement des données n'est rien d'autre que la raison pour laquelle des données à caractère personnel sont collectées, stockées, consultées et éliminées.

Déterminer la finalité du traitement des données signifie effectuer le traitement pour des finalités légitimes, déterminées et explicites, connues de la personne concernée, sans possibilité de traitement ultérieur d'une manière incompatible avec ces finalités.

Il en va de même pour la nécessité de la collecte, qui doit tenir compte de la finalité du traitement afin d'identifier les données minimalement nécessaires à sa réalisation, ce qui permet d'éviter l'utilisation indiscriminée et excessive des données à caractère personnel ainsi que l'impossibilité d'effectuer le traitement à des fins discriminatoires, illégales ou abusives.

[17] V. GAUTRAIS et P. TRUDEL, préc., note 7.

Quant à la nécessité, elle consiste à limiter le traitement au minimum nécessaire pour atteindre ses objectifs (finalités), l'étendue des données étant pertinente, proportionnée et non excessive par rapport aux finalités du traitement des données.

Seules les données pertinentes doivent être traitées, c'est-à-dire celles qui sont essentielles à la réalisation de l'objectif précédemment exposé. Il ne peut en être autrement, car il serait tout à fait inapproprié de traiter des données qui ne sont pas pertinentes et adaptées au traitement en question.

Le principe de finalité a été réaffirmé par le RGPD à son article 5, 1, b). Si la finalité du traitement est différente de celle initiale, il conviendra de solliciter un nouveau consentement de la personne concernée. Cette dernière doit garder la maîtrise effective de ses données :

> Considérant 39 : « (39) Tout traitement de données à caractère personnel devrait être licite et loyal. Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées. Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. Ce principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement. Les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement. En particulier, les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées lors de la collecte des données à caractère personnel. Les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique. Il y a lieu de prendre toutes les mesures raisonnables afin de garantir que les données à caractère personnel qui sont inexactes sont rectifiées ou supprimées. Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité

appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement ».[18]

Considérant 50 : « (50) Le traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne devrait être autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement. Dans ce cas, aucune base juridique distincte de celle qui a permis la collecte des données à caractère personnel n'est requise. Si le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, le droit de l'Union ou le droit d'un État membre peut déterminer et préciser les missions et les finalités pour lesquelles le traitement ultérieur devrait être considéré comme compatible et licite. Le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques devrait être considéré comme une opération de traitement licite compatible. La base juridique prévue par le droit de l'Union ou le droit d'un État membre en ce qui concerne le traitement de données à caractère personnel peut également constituer la base juridique pour un traitement ultérieur. Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.

Lorsque la personne concernée a donné son consentement ou que le traitement est fondé sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir, en particulier, d'importants objectifs d'intérêt public général, le responsable du traitement devrait être autorisé à effectuer un traitement ultérieur des données à caractère personnel indépendamment de la compatibilité des finalités. En tout état de cause, l'application des principes énoncés dans le présent règlement et, en particulier, l'information de la personne concernée au sujet de ces autres finalités et de ses droits, y compris le droit de s'opposer au traitement, devraient être assurées. Le fait, pour le responsable du traitement, de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à caractère personnel concernées dans des cas individuels ou dans plusieurs cas relatifs à une même infraction pénale ou à des mêmes menaces pour la sécurité

[18] *Considérant 39 📖 RGPD | GDPR-Text.com*, (14 octobre 2019), en ligne : <https://gdpr-text.com/fr/read/recital-39/> (consulté le 1 août 2023).

> publique devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement. Néanmoins, cette transmission dans l'intérêt légitime du responsable du traitement ou le traitement ultérieur des données à caractère personnel devrait être interdit lorsque le traitement est incompatible avec une obligation de confidentialité légale, professionnelle ou toute autre obligation de confidentialité contraignante ».[19]

Toutes ces notions qui, intégralement, sont conformes à la finalité admise, doivent être portées à la connaissance du titulaire qui, avec son accord, délimitera l'objet du traitement, domaine qui ne pourra pas être modifié par la suite, à moins d'obtenir un nouvel accord spécifique et exprès de la part du titulaire.

1.1.2.3 Libre accès

Le principe de libre accès garantit aux personnes concernées la possibilité de s'informer librement et facilement sur la forme et la durée du traitement ainsi que sur l'intégrité de leurs données personnelles. La personne qui a collecté les données doit savoir où elles se trouvent, avec qui et où elles sont partagées.

Ce droit est par exemple garanti par l'article 9 de la *Loi sur l'accès* (LAI) et l'article 1 de la *Loi sur le privé* (LP) :

> 9 Toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public.
>
> Ce droit ne s'étend pas aux notes personnelles inscrites sur un document, ni aux esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature.[20]
>
> 1. La présente loi a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil.

[19] *Considérant 50 📖 RGPD | GDPR-Text.com*, (14 octobre 2019), en ligne : <https://gdpr-text.com/fr/read/recital-50/> (consulté le 1 août 2023).

[20] *RLRQ c A-2.1 | Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 8.

> Elle s'applique à ces renseignements quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles: écrite, graphique, sonore, visuelle, informatisée ou autre.
>
> Elle s'applique aussi aux renseignements personnels détenus par un ordre professionnel dans la mesure prévue par le Code des professions (chapitre C-26).
>
> La présente loi ne s'applique pas à la collecte, la détention, l'utilisation ou la communication de matériel journalistique, historique ou généalogique à une fin d'information légitime du public.[21]
>
> Les 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.

La qualité des données est la garantie pour les personnes concernées que les données sont exactes, claires, pertinentes et mises à jour en fonction des finalités pour lesquelles elles seront traitées.

La transparence, quant à elle, garantit aux personnes concernées des informations claires, précises et facilement accessibles sur la manière dont les données sont traitées et sur les agents de traitement respectifs, tout en respectant les secrets commerciaux et industriels.

La notion de libre accès va de pair avec l'idée de portabilité, comme nous le verrons plus loin, les lois qui traitent du sujet traitent de la livraison des données aux détenteurs, une situation qui entre dans le droit d'accès.

Ces trois principes de traitement des données des consommateurs sont étroitement liés à la portabilité.

1.2 Portabilité des données à caractère personnel

A la lumière de l'importance incontestable du traitement des données personnelles sur le marché numérique, il est nécessaire de fournir à leurs détenteurs des outils leur permettant de mieux les contrôler et de tirer profit de cette économie en pleine expansion. Donner à la personne

[21] *RLRQ c P-39.1 | Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 9.

concernée un plus grand contrôle sur les informations qui la concernent, en évitant qu'elle ne devienne un simple objet de transaction.

Compte tenu de l'importance que la connaissance des consommateurs a acquise dans l'économie d'aujourd'hui, les données personnelles sont devenues un capital essentiel pour le succès de nombreuses entreprises. Ainsi, dans le contexte de l'économie de production flexible, on assiste à l'émergence d'une véritable « industrie des bases de données », dont l'objectif principal est de fournir aux secteurs intéressés les données personnelles de catégories de consommateurs, par le biais de la commercialisation ou de la cession. Il en résulte une large circulation des informations personnelles dans la société, générant des bénéfices pour les secteurs concernés, mais aussi de grands risques pour les consommateurs, dont les données sont collectées, traitées et transférées :

> Today, corporations are desperate for whatever consumer information they can glean, and their quest for information is hardly perceived as democratic. The data collected extends beyond information about consumers' views of the product to information about the consumers themselves, often including lifestyle details and even a full-scale psychological profile.[22]

Le droit à la portabilité des données à caractère personnel (en utilisant la notion de droit, car c'est celle qui est la plus adoptée dans la législation étudiée) découle du droit fondamental à l'autodétermination informationnelle, dans la mesure où il présuppose que les données appartiennent à leur détenteur, qui a un contrôle, même s'il n'est pas absolu, sur l'utilisation qui en est faite. En même temps que l'institut renforce l'autonomie de la personne concernée, il constitue également un outil important pour le développement économique et concurrentiel.

En d'autres termes, la portabilité renforce la liste des droits de la personne concernée et se présente également comme un outil de stimulation de la concurrence, car elle est capable d'atténuer les distorsions informationnelles qui contribuent aujourd'hui à maintenir des concentrations dans divers secteurs de l'économie dans divers secteurs de l'économie.

[22] Daniel J. SOLOVE, *The Digital Person: Technology and Privacy in the Information Age*, Rochester, NY, 2004, en ligne : <https://papers.ssrn.com/abstract=2899131> (consulté le 10 juillet 2023).

La portabilité des renseignements personnels doit être perçue sous différents angles, car en même temps qu'elle est l'externalisation d'un des aspects du droit à l'autodétermination informationnelle, associé à la protection de la vie privée de la personne concernée, elle a également une dimension économique, avec des répercussions sur le droit de la consommation et de la concurrence :

> Data portability has a hybrid nature. What emerged as a data protection concept is now also becoming part of policies aiming to stimulate competition and innovation. […] Data portability can empower individuals and business users to make better choices, but more asymmetric enforcement is needed to ensure that data portability will stimulate competition.[23]

Ainsi, en plus de garantir l'accès à ses propres informations (droit d'accès), le droit à la portabilité des données personnelles permet aux individus non seulement d'accéder à leurs données, mais aussi de les transférer entre différents services ou plateformes, ce qui favorise l'autonomie numérique et encourage une saine concurrence entre les entreprises à l'ère des technologies de l'information.

1.2.1 Définition

La portabilité des données désigne la capacité des individus à transférer leurs renseignements personnels d'une organisation à une autre, ou à accéder à leurs données et à les utiliser sur différents services ou plateformes. Cela signifie que les consommateurs pourront mieux contrôler leurs propres données, ainsi que l'endroit où elles sont stockées et la manière dont elles sont utilisées, en fonction de la nature du service ou du produit.

La garantie de portabilité vise à permettre à la personne concernée de transférer ses données à caractère personnel d'un responsable du traitement à un autre sans obstacles techniques ou autres. Elle compléterait donc les droits de la personne concernée en renforçant son intérêt, dans un contexte de multiplication des communications en ligne, à obtenir des copies de ses données à caractère personnel afin de les réutiliser sur d'autres plates-formes. Ainsi, en

[23] Inge GRAEF, *The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation*, SSRN Scholarly Paper, Rochester, NY, 26 novembre 2020, en ligne : <https://papers.ssrn.com/abstract=3740185> (consulté le 27 octobre 2023).

plus de renforcer la protection de la personne concernée en lui permettant de jouir effectivement de son droit de choisir, la mesure stimule la concurrence, puisqu'elle limite la possibilité d'enfermer les utilisateurs dans certains produits ou services.

Ainsi, le droit à la portabilité vise à permettre le contrôle effectif du détenteur sur ses données personnelles. En plus de créer de nouvelles opportunités de développement et d'innovation, en facilitant le partage des données personnelles, de manière sécurisée et sous le contrôle de la personne concernée.

Les données personnelles couvertes par le droit à la portabilité sont celles fournies avec le consentement et les données générées par l'activité de la personne concernée, par exemple lorsqu'elle utilise un service ou un appareil.

Les principaux objectifs et avantages de la portabilité du point de vue du consommateur sont les suivants : éviter le *lock-in*, accroître le contrôle de la circulation des données par leur propriétaire, renforcer l'équilibre entre les grandes entreprises qui exploitent les données personnelles et le consommateur, accroître la flexibilité de l'économie et de l'utilisation des données personnelles[24]. Cela promet de permettre au consommateur une plus grande flexibilité commerciale ainsi qu'une meilleure évaluation du marché :

> It can be a business strategy of service providers to prevent users to transfer their data to a competing service. By limiting the possibility of data portability, service providers are creating switching costs. These costs arise if a user finds it costly to switch from one service provider to another. Switching costs are created as soon as the user makes an investment specific to his current service provider that must be duplicated for any new provider. Due to switching costs, users can become locked-in to a given service. Irrespective of the potential higher quality of a different service, users will stay with their current provider. The degree of lock-in is determined by the switching costs. If the switching costs are high, providers will be able to create a high degree of user lock-in.24 For providers that heavily rely on data provided by users, restricting data portability is a way to tie users to their services.[25]

[24] Vitor Palmela FIDALGO, « *O direito à portabilidade de dados pessoais* », en ligne : <https://blook.pt/PHfS> (consulté le 15 juillet 2023).

[25] Inge GRAEF, Jeroen VERSCHAKELEN et Peggy VALCKE, *Putting the Right to Data Portability into a Competition Law Perspective*, SSRN Scholarly Paper, Rochester, NY, 2013, en ligne : <https://papers.ssrn.com/abstract=2416537> (consulté le 23 mars 2023).

Il s'agit donc d'un droit dont l'un des principaux objectifs est de permettre et de renforcer l'autodétermination de la personne concernée en matière d'information. En fait, la portabilité vise à permettre à la personne concernée d'exercer un contrôle effectif sur ses données pour les finalités les plus diverses, en permettant leur gestion et leur réutilisation, y compris dans le but de faciliter la migration de la personne concernée vers des services concurrents.

Cela permet d'éviter que les consommateurs ne soient enfermés dans un fournisseur particulier (effet de verrouillage ou *lock-in*) en raison des difficultés ou même des coûts élevés de changement qui résulteraient de la « perte » des données :

> Regarding lock-in effects, some authors argue that digital monopolies have incentives to protect their competitive advantage and lock in consumers. Once users have made an investment in their current platform, the new platform has to duplicate that effort. In this sense, 'the degree of lock-in is determined by the level of switching costs. Users experience switching costs when they assess the investment required for changing to a new platform. This investment could be in a new equipment, in learning how to use a product, or even psychological. In the case of online platforms such as social networks for example the investment is not an equipment or price, but the time and effort it takes to upload again all the contact details, pictures, friends, etc. We might add psychological switching costs because the dependence that the user create with the social network would be high.[26]

D'où l'idée que le droit à la portabilité, pour atteindre ces objectifs, doit être facile, gratuit et garanti de manière à permettre une utilisation efficace et sûre des données.

Outre la protection de la personne concernée, le droit à la portabilité a également d'importantes implications concurrentielles, puisque, partant du principe que les données sont les intrants les plus importants de l'économie fondée sur les données - voire des installations essentielles -, la portabilité peut faciliter le transfert de données aux fins de l'entrée de nouveaux entrants ou de start-ups sur le marché ou même pour stimuler la concurrence entre les rivaux existants, en évitant que l'accumulation de données par un seul ou certains acteurs ne constitue

[26] Carolina BANDA, *Enforcing Data Portability in the Context of EU Competition Law and the GDPR*, SSRN Scholarly Paper, Rochester, NY, 13 septembre 2017, en ligne : <https://papers.ssrn.com/abstract=3203289> (consulté le 31 juillet 2023).

une véritable barrière à l'entrée ou un facteur qui met en péril la rivalité avec les acteurs de moindre importance.

Parallèlement aux évolutions concurrentielles, le droit à la portabilité peut également générer un certain nombre d'avantages pour le marché, car il peut également être utilisé pour échanger des données entre des services complémentaires, ce qui facilite la vie des parties concernées.

1.2.2 Application

La portabilité des données peut être utilisée des façons les plus diverses, mais celle qui attend certainement avec impatience son application est le milieu bancaire, puisqu'elle permettra l'existence de l'*open banking* au Canada, comme cela a déjà été expérimenté dans d'autres pays (l'*open banking* est utilisé depuis 2018 au Royaume-Uni, par exemple).

L'o*pen banking* permet à l'utilisateur d'être le protagoniste du contrôle et de l'accès des institutions financières à ses informations personnelles. Le but de cette fonctionnalité est d'élargir les offres de produits et services bancaires à moindre coût, créant une sorte de concurrence plus saine entre les banques et les *fintechs*.

Avec l'utilisation de la portabilité, basé sur l'existence d'un système d'interopérabilité, comme nous le verrons plus loin, le client peut demander à sa banque de transférer des données vers une autre banque (ou *fintech*) et ainsi avoir accès à des services et produits à un prix très compétitif, sans avoir besoin de créer une nouvelle base de données dans l'autre établissement, ou perdre des données précédemment enregistrées.

Cela peut également s'appliquer aux services de *streaming*, par exemple, car cela garantirait la migration des données faisant référence aux préférences et aux habitudes, sans qu'il soit nécessaire de créer un nouvel enregistrement sans information initiale.

Il s'ensuit donc que cet outil, en permettant à une personne concernée de déplacer ses données d'un commerçant à un autre, a des implications concurrentielles et consuméristes : il réduit les coûts de changement, car il permet au consommateur de changer plus facilement de

fournisseur ; et évite au consommateur de se faire piéger, étant donné qu'il peut choisir librement son fournisseur, et non rester chez celui qui possède déjà beaucoup de ses données car l'échange serait gênant ou très coûteux. Un large éventail *data-driven business* peuvent tirer parti de la portabilité :

> In other words, the taxonomy classifies a company as having a data-driven business models if it features the following characteristics: a) The collection or aggregation of data. This is the case with social networks, search engines or any online platform that collects data of their users. It may also be the case with health insurance companies or companies selling wearable devices that collect data through sensors. b) The marketing of other products that rely on data and the performance of activities that use data as a key resource, as it is the case for targeted advertisement in online platforms; and c) uses data to conduct the business, this element cross board all the digital economy.[27]

La portabilité permet aux individus d'avoir une plus grande autonomie et un meilleur contrôle sur leurs données personnelles, améliorant ainsi leur autodétermination informationnelle, et s'applique à un large éventail de secteurs, comme l'illustre Peter Swire :

> In addition, the EU has had sectoral initiatives in the automobile, energy, and digital content areas, further highlighting the variety of PORTability requirements as well as the growing number of sectors with these requirements. In the automobile sector, there has been tension between the interests of car manufacturers and providers of third-party aftersales services as regards data access. The latter have wished to access in-vehicle data in order to provide services. Car manufacturers had resisted such access, however, citing security and safety risks. Since 2007, an EU Regulation has required manufacturers to provide standardized access for vehicle repair and maintenance information to independent operators. Recently, two additional sectors added PORTability initiatives. In the energy sector, Member States must specify rules on access to customer data by eligible parties, such as data required for customer switching. Under the Digital Content Directive, consumers have a right, in the event of termination of the contract for the supply of digital content or a digital service, to retrieve content other than personal data which was provided or created by the consumer when using digital content or digital service. [28]

Même les systèmes de streaming populaires envisagent d'adopter la portabilité. En 2022, Netflix a intégré cet outil dans son système, permettant de migrer un profil d'un compte à un

[27] *Id.*

[28] Peter SWIRE, « The Portability and Other Required Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations », 2022, DOI : 10.2139/ssrn.3689171.

autre sans perdre de données. Selon la société, le déménagement facilite l'indépendance entre les abonnements, en conservant toutes les recommandations personnalisées, l'historique d'accès et d'autres listes personnelles. La nouvelle fonctionnalité a commencé à être déployée en octobre 2022 pour les utilisateurs du monde entier[29]. Bien qu'il s'agisse d'un système mis en œuvre au sein du service, il montre l'existence d'un ensemble de données spécifiques (parmi lesquelles les préférences et les habitudes du consommateur devraient être mises en évidence) qui peut éventuellement être transféré à d'autres diffuseurs par le biais d'une plateforme d'interopérabilité.

Autrement dit, la portabilité des données est le fait de transférer des données d'une entreprise à une autre, à la demande de la personne concernée. En d'autres termes, si un particulier souhaite changer de fournisseur d'un service ou d'un produit, il lui suffit de demander la portabilité et l'entreprise devra transférer ses données personnelles à l'autre. De cette manière, la législation garantit la liberté du consommateur, évitant ainsi ce que l'on appelle le « lock in », qui rend difficile l'échange de services en raison de difficultés et de coûts élevés.

Comme l'explique la professeure Teresa Scassa :

> A data mobility right, in theory, allows an individual to port their data to the new entrant. The more level playing field fosters competition that is in the individual's interest and serves the broader public interest by stimulating competition.[30]

On observe donc que le nouvel institut prévu dans la loi vise à créer un environnement plus concurrentiel et plus convivial pour les consommateurs, en plus d'élargir le contrôle sur leurs données.

---

[29] « With Profile Transfer, Keep Your Netflix Experience a Constant Even in Times of Change », *About Netflix*, en ligne : <https://about.netflix.com/en/news/profile-transfer-keeps-netflix-experience-constant> (consulté le 13 juillet 2023).

[30] Teresa SCASSA, « Data Mobility (Portability) in Canada's Bill C-11 », en ligne : <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=338:data-mobility-portability-in-canadas-bill-c-11&Itemid=80> (consulté le 23 mars 2023).

1.3 Opérationnalisation de la portabilité des renseignements personnels

Comme nous l'avons vu précédemment, les exigences en matière de portabilité des données garantissent généralement que les personnes peuvent facilement obtenir, déplacer, copier, transférer et réutiliser leurs données à caractère personnel dans différents services et environnements informatiques.

Il est généralement exigé que les données soient fournies dans un format couramment utilisé et lisible par machine. Ce point spécifique mérite une étude plus approfondie qui fera l'objet d'un chapitre séparé sur l'interopérabilité.

Il est possible de donner quelques exemples de mise en œuvre de la portabilité qui existent déjà dans le monde.

1.3.1 L'*open banking* au Brésil

En ce qui concerne l'*open banking*, par exemple, il convient de mentionner la manière dont la mesure a été adoptée au Brésil.

Décrit comme un système financier ouvert, il s'agit de la possibilité pour les clients de produits et services financiers d'autoriser le partage de leurs informations entre différentes institutions autorisées par la Banque centrale (*Banco Central do Brasil*) et le mouvement de leurs comptes bancaires à partir de différentes plateformes.

La réglementation relative à l'adoption du système a été établie par la Banque centrale brésilienne et le Conseil monétaire national (*Conselho Monetário Nacional*), qui ont publié la

résolution conjointe n° 1[31] et la circulaire n° 4 015[32], et suit les dispositions de la loi générale brésilienne sur la protection des données (*Lei Geral de Proteção de Dados – LGPD*).

L'opérationnalisation a été divisée en plusieurs étapes pour permettre l'adaptation du marché et le développement de solutions. Elle a débuté en février 2021 (quelques mois seulement après l'approbation de la LGPD) et s'est achevée en mai 2022.

Au cours de la première phase de mise en œuvre, les données des institutions participantes sur les canaux de service, les produits et les services disponibles pour les contrats relatifs aux comptes à vue ou d'épargne, aux comptes de paiement ou aux opérations de crédit seront partagées ; au cours de la deuxième phase, les informations relatives à l'enregistrement des clients et des représentants et les données transactionnelles des clients relatives aux produits et aux services indiqués au cours de la première phase ; dans la troisième phase, les données relatives aux services d'initiation d'opérations de paiement et de transmission de propositions d'opérations de crédit ; et dans la quatrième phase, les données sur les produits et services et les transactions des clients relatives aux opérations de change, aux services d'accréditation dans les arrangements de paiement, aux investissements, aux assurances, aux régimes de retraite complémentaire ouverts et aux comptes de salaire.

Plus précisément, la première étape consiste à mettre à la disposition des clients des banques les canaux de service, les produits financiers et les services offerts par les participants au système ouvert. À ce stade, l'idée n'était pas que les titulaires de comptes bancaires partagent leurs données, mais plutôt qu'ils comparent les différentes offres, ce qui leur permettrait de choisir plus facilement celle qui répondait le mieux à leurs besoins.

La deuxième étape concerne le partage des données des clients des banques, sous réserve de leur autorisation préalable (consentement), d'informations sur les services bancaires, telles

[31] Brésil, *Resolução Conjunta n° 1 de 4/5/2020*, en ligne : <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=1> (consulté le 1 août 2023).

[32] Brésil, *Circular n° 4.015 de 4/5/2020*, en ligne : <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=4015> (consulté le 1 août 2023).

que les transactions entre leurs comptes et leurs cartes de crédit. Ce partage des données des utilisateurs de services financiers, qui est la principale caractéristique de l'*open banking*, ne se fait qu'avec leur autorisation expresse. En outre, cette autorisation a une finalité et une échéance précises, et peut également être annulée à tout moment.

La troisième étape ouvre la porte à un accès plus facile aux services financiers pour les utilisateurs des banques. Les clients des banques pourront utiliser des environnements électroniques pour demander des offres de crédit à différentes institutions et trouver ainsi plus facilement celle qui répond le mieux à leurs besoins.

La quatrième et dernière phase concerne l'échange de données sur les devises, l'accréditation (ouverture des informations sur les distributeurs de cartes), l'assurance, les régimes de retraite et la capitalisation.

Seules les institutions financières soumises à la réglementation de la banque centrale peuvent participer à la portabilité via l'*open banking*.

Le règlement définit toutefois que les organisations considérées comme grandes (10 % ou plus du produit intérieur brut) et moyennes (entre 1 % et 10 % du PIB) seront obligées d'adhérer au système, tandis que les autres institutions y adhéreront sur une base volontaire.

Bien que la participation obligatoire ne s'applique pas à toutes les entreprises, une caractéristique importante de l'*open banking* est la réciprocité. En d'autres termes, toutes les entreprises qui adhèrent auront le droit de recevoir des données de leurs concurrents, mais seront également obligées de partager les données de leurs bases respectives - lorsque les clients y consentent.

Par conséquent, si une fintech ou une autre institution, qui a une participation volontaire, veut rejoindre l'*open banking*, elle doit partager les données de ses clients, s'ils le demandent, avec toute autre banque ou fintech participant à l'*open banking*.

La demande de partage des données des clients implique les étapes de consentement, d'authentification et de confirmation, généralement pour s'assurer que des informations fiables sur le partage sont fournies et que le client est correctement identifié.

Cet exemple d'innovation dans le système bancaire brésilien démontre que l'adoption de la portabilité, même si elle ne concerne qu'un seul secteur, présente plusieurs défis, nécessite des lois et des règlements, ainsi que des incidences sur les types de données à caractère personnel les plus variés (des consommateurs et même des entreprises) et démontre un respect clair des principes de consentement, de finalité et d'accès.

1.3.2 *The Data Transfer Project*

Un autre exemple d'application de la portabilité provient d'un système complètement différent, il s'agit du *Data Transfer Project* créé par Apple, Google et Meta :

> The Data Transfer Project (DTP) extends data portability beyond a user's ability to download a copy of their data from their service provider ("provider"), to providing the user the ability to initiate a direct transfer of their data into and out of any participating provider.
>
> The Data Transfer Project is an open source initiative to encourage participation of as many providers as possible. The DTP will enhance the data portability ecosystem by reducing the infrastructure burden on both providers and users, which should in turn increase the number of services offering portability. The protocols and methodology of the DTP enable direct, service-to-service data transfer with streamlined engineering work.[33]

L'idée née en 2018 s'est transformée en le *Data Transfer Initiative:*

> The Data Transfer Initiative invests dedicated engineering and product resources to the design and implementation of data transfer tools. These contributions will continue to be maintained in an open source GitHub repository to encourage broader adoption of and contributions to the code base. DTI will also offer its expertise with user-driven data transfers as an important resource to policymakers. Data portability continues to be a key element of policy discussions around the world, and

[33] « Data Transfer Initiative », en ligne : <https://dtinit.org/> (consulté le 2 août 2023).

> DTI will seek to help translate principle to practice, catalyzing greater user agency and empowerment.[34]

L'idée de base est de donner aux utilisateurs le contrôle de leurs données et de faciliter le transfert de ces données entre différents services en ligne. Par exemple, si un utilisateur souhaite migrer d'une plateforme de stockage de photos à une autre, le DTP vise à rendre ce processus plus simple et plus direct. Le modèle, cependant, ne montre pas encore beaucoup de progrès.

De plus, alors que Meta prétendait être en totale conformité avec la législation européenne, il est connu pour avoir été sévèrement sanctionné par le Comité européen de la protection des données pour avoir violé les règles de transfert de données de l'Europe vers les États-Unis.[35]

Ainsi, nous pouvons constater que la portabilité des données à caractère personnel concerne plusieurs secteurs et peut être abordée de manières très différentes.

Alors que le modèle de banque ouverte au Brésil est une application locale de la portabilité, limitée aux normes brésiliennes, le modèle proposé par Meta (à l'époque encore seulement Facebook) se veut plus internationalisé, étant donné le contenu des réseaux sociaux au-delà des frontières.

Toutefois, on ne peut exclure la nécessité de respecter la législation en vigueur dans chaque pays, car la portabilité peut entraîner l'extrapolation des barrières.

1.4 Mise en œuvre en Europe, au Canada et au Québec

Sur la scène européenne, l'article 20 du règlement général sur la protection des données (RGPD 2016/679) traite du droit à la portabilité des données et accorde à la partie intéressée (propriétaire des données), la garantie d'exiger la transmission des données à un responsable du traitement autre que le responsable du traitement d'origine, sous réserve de critères techniques.

[34] *Id.*

[35] « 1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board », en ligne : <https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_fr> (consulté le 2 août 2023).

Il ressort également de la lecture du RGPD, notamment à la lumière du considérant 68, que, si le droit à la portabilité est un encouragement à l'interopérabilité, il ne crée pas pour les agents une obligation de maintenir des systèmes interopérables, et les conflits qui en résultent doivent être résolus en fonction de ce qui est techniquement possible.

Au Canada, le Projet de loi C-27 (ancien Projet de loi C-11 de 2020) crée la Loi sur la protection de la vie privée des consommateurs (LPVPC) et son article 72 permet au consommateur de consentir (ou d'exiger) de l'institution dans laquelle il a déjà déposé des données personnelles, qu'elle procède à la portabilité de celles-ci à un tiers, mais, contrairement au RGPD, ne confère pas le même statut au droit à la mobilité des données que celui conféré au droit d'accès aux renseignements personnels

La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels du Québec adopte la même ligne de conduite du projet fédéral, parce que cette loi considère la mobilité des données comme une version améliorée du droit d'accès aux informations personnelles détenues par l'entreprise, et non comme un nouveau droit véritablement distinct.

Chapitre 2 – La portabilité des données et son application dans les systèmes européen, canadien et québécois

L'objectif de ce chapitre est de présenter les définitions de la portabilité dans les législations étudiées et d'établir les parallèles et les différences entre elles.

2.1 La portabilité conforme à la législation

A présent, nous allons analyser la question dans chacun des systèmes juridiques précédemment établis.

2.2 Législation de l'Union Européenne

2.2.1 Règlement général sur la protection des données (RGPD 2016/679)

Lorsqu'il est question de portabilité, le Règlement général sur la protection des données (RGPD) de l'Union Européenne dans son article 20 précise que :

> Article 20 – Droit à la portabilité des donnés
>
> 1. La personne concernée a le droit de recevoir les données à caractère personnel la concernant et qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et le droit de transmettre ces données à un autre responsable du traitement.
>
> a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b); et
>
> b) le traitement est effectué à l'aide de procédés automatisés.
>
> Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

> L'exercice du droit, visé au paragraphe 1 du présent article s'entend sans préjudice de l'article 17. Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.[36]

Premièrement, la disposition légale stipule que la portabilité des données à caractère personnel est un droit et que ce droit vise à permettre aux personnes concernées d'obtenir et de réutiliser leurs données à caractère personnel à leurs propres fins dans différents services :

> During the GDPR's legislative process, it was advocated the possibility to add the right to data portability in the right of access. It was not the accepted option on the final Regulation's text, ending up consecrating data portability as an autonomous right and distinct from the right of access.[37]

> The right to data portability, therefore, can be seen as a step forward, an evolution in light of the right of access, as the data format would no longer be limited to what was chosen by the data controller, besides enabling data reuse (DUARTE; GUSEINOV, 2019, p. 110) by the data subject itself or by another data controller. It is a novelty brought through the GDPR, since the former Directive 95/46/EC had not brought such modern right.

> Another difference between right of access and right to data portability in the European scope is their limit and applicability. Data portability includes only data provided by the data subject and only when the data processing is automated and consent-based or based on a contract execution (GRAEF et al., 2017, p. 1367). Such restrictions and limitations, however, do not apply to the right of access as provided through the GDPR so that the right of access and the right to data portability end up complementing each other (STIFTUNG DATENSCHUTZ, s.d.).[38]

L'article susmentionné définit également que le droit à la portabilité permet de recevoir des données à caractère personnel, de les transmettre à un tiers ou de demander directement leur transmission entre responsables du traitement, ce qui donne lieu à trois formes d'application.

[36] *TEXTE consolidé*, préc., note 2.

[37] V. P. FIDALGO, préc., note 24.

[38] Daniela Copetti CRAVO, « The Right of Data Portability in EU's GDPR and Brazil's LGPD », (2022) 50-1 *Revista da Faculdade de Direito da Universidade Federal de Uberlândia* 89-121, DOI : 10.14393/RFADIR-50.1.2022.62778.89-121.

Il est aussi précisé qu'en aucun cas l'exercice du droit à la portabilité ne peut porter atteinte aux droits des tiers, ni à la nécessité d'assurer la compatibilité entre le droit à la portabilité et le droit à l'effacement ou à l'oubli.

Il est important de noter que les données anonymes, en raison de la perte de qualité des données personnelles, ne sont pas soumises à la portabilité, mais celles qui permettent l'identification (pseudo-anonymes), selon les termes du RGPD, peuvent faire l'objet d'une demande de portabilité[39].

Il ressort également de la lecture du RGPD, notamment à la lumière du considérant 68, que, si le droit à la portabilité est un encouragement à l'interopérabilité, il ne crée pas pour les agents une obligation de maintenir des systèmes interopérables, et les conflits qui en résultent doivent être résolus en fonction de ce qui est techniquement possible :

> Considérant 68 : « (68) Pour renforcer encore le contrôle qu'elles exercent sur leurs propres données, les personnes concernées devraient aussi avoir le droit, lorsque des données à caractère personnel font l'objet d'un traitement automatisé, de recevoir les données à caractère personnel les concernant, qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé, lisible par machine et interopérable, et de les transmettre à un autre responsable du traitement. Il y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données. Ce droit devrait s'appliquer lorsque la personne concernée a fourni les données à caractère personnel sur la base de son consentement ou lorsque le traitement est nécessaire pour l'exécution d'un contrat. Il ne devrait pas s'appliquer lorsque le traitement est fondé sur un motif légal autre que le consentement ou l'exécution d'un contrat. De par sa nature même, ce droit ne devrait pas être exercé à l'encontre de responsables du traitement qui traitent des données à caractère personnel dans l'exercice de leurs missions publiques. Il ne devrait dès lors pas s'appliquer lorsque le traitement des données à caractère personnel est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Le droit de la personne concernée de transmettre ou de recevoir des données à caractère personnel la concernant ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles. Lorsque, dans un ensemble de données à caractère personnel, plusieurs personnes sont concernées, le droit de recevoir les données à caractère personnel devrait s'entendre sans préjudice des droits et libertés des autres

[39] Nicholas VOLLMER, *Raison 26 EU règlement général sur la protection des données (EU-RGPD)*, 4 avril 2023, en ligne : <https://www.privacy-regulation.eu/fr/r26.htm> (consulté le 15 juillet 2023).

personnes concernées conformément au présent règlement. De plus, ce droit ne devrait pas porter atteinte au droit de la personne concernée d'obtenir l'effacement de données à caractère personnel ni aux limitations de ce droit comme le prévoit le présent règlement et il ne devrait pas, notamment, entraîner l'effacement de données à caractère personnel relatives à la personne concernée qui ont été fournies par celle-ci pour l'exécution d'un contrat, dans la mesure où et aussi longtemps que ces données à caractère personnel sont nécessaires à l'exécution de ce contrat. Lorsque c'est techniquement possible, la personne concernée devrait avoir le droit d'obtenir que les données soient transmises directement d'un responsable du traitement à un autre. »[40]

Comme Cravo l'explique:

> In Europe, it is understood that for compliance to data portability purposes, the entity responsible for data processing must provide personal data in an interoperable, structured, of current use and of automated reading format (Recital 68 of the GDPR). However, even if interoperability is desirable (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 17), there is no obligation to comply with it36, as provided through the Recital 68: The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.[41]

Et aussi, Wong et Henderson :

> The right to receive portable personal data is not the same as making data interoperable across different platforms. In the EU, interoperability is defined as "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems" (Article 2) [10]. Article 20's requirements for structured and machine-readable formats and clearly-defined metadata are important for data files to be interoperable, but despite pressure from lawyers and academics, mandatory interoperability provisions have not been included in the GDPR.[42]

---

[40] *Considérant 68 📖 RGPD | GDPR-Text.com*, (14 octobre 2019), en ligne : <https://gdpr-text.com/fr/read/recital-68/> (consulté le 12 juillet 2023).

[41] D. C. CRAVO, préc., note 38.

[42] Janis WONG et Tristan HENDERSON, *How Portable is Portable? Exercising the GDPR's Right to Data Portability*, *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, coll. UbiComp '18, New York, NY, USA, Association for Computing Machinery, Outubro 2018, p. 911-920, DOI : 10.1145/3267305.3274152.

Un autre point fort de la règle est l'absence d'expiration, puisqu'il n'y a pas de disposition à ce sujet, le droit à la portabilité reste donc intact tant que les données à caractère personnel se trouvent dans le système.

Selon Peter Swire, le droit établi par la législation européenne présente cinq points saillants :

> Because so much of this article discusses the direct and indirect effects of the EU enacting the RtDP, I highlight five points here. First, as I wrote in 2013, the GDPR's RtDP was without precedent as a legal mandate. Actual experience with implementing the right began only in May 2018, when the GDPR went into effect. The European Data Protection Board has issued nonbinding guidance on Article 20, but that guidance does not provide detailed analysis of how to meet possibly conflicting goals such as competition, privacy, and cybersecurity. Second, as mentioned in the introduction, the word "portability" has become a term of art for European lawyers, focused on implementing the requirements of Article 20 into practice. This article thus limits the term "portability" to transfers of an individual's data. Third, some EU scholars have highlighted how portability exists at the intersection of data protection, competition, and consumer protection law. Different EU regulators typically enforce in these distinct areas of law, so there are intricate institutional questions about which actors are charged with enforcement, and the possibility exists that no one enforcement agency has legal competence to assess how best to meet the goals of data protection, competition, and consumer protection law. Fourth, EU scholars have also explained that the RtDP is designed to foster individual autonomy, i.e., individuals' control over their own data. The RtDP applies not only to large platforms but also to small and medium enterprises, demonstrating that the right goes beyond prevention of monopoly market power. Fifth, possible amendment to the RtDP is under consideration. The EU issued a proposed Data Strategy in early 2020. As part of that strategy, the EU has put forward a proposed Data Act that could include, among other things, new rules to broaden the RtDP. According to the Data Act Inception Impact Assessment published by the EU, the Data Act aims to improve technical standards for portability, including for sectors such as smart home appliances, wearables, and home assistants. The EU's proposal for a Digital Markets Act (which targets large online platforms designated as 'gatekeepers') would expand portability to require gatekeepers to include continuous and real-time access. Implementation of a PORT-IA, as proposed by this article, could be useful as the EU seeks to meet the multiple goals put forward in its Data Strategy.[43]

Parmi ces points, l'innovation présente dans le RGPD se distingue, qui a servi et sert de base aux lois de protection des données les plus diverses dans les systèmes juridiques les plus divers, ainsi qu'à l'application de la portabilité comme intersection des notions de protection des

[43] P. SWIRE, préc., note 28.

données, de concurrence et de protection des consommateurs, avec pour résultat une plus grande autonomie pour ces derniers.

Selon le RGPD la portabilité est une sorte d'accès qualifié aux données à caractère personnel, puisqu'elle garantit à la personne concernée le droit d'accéder à ses données et d'en disposer de manière qu'elles puissent être transmises, sur son ordre, à un tiers.

Le droit à la portabilité reconnaît le droit de la personne concernée de recevoir un ensemble de données à caractère personnel et de transmettre ces données entre responsables du traitement. Il s'agit avant tout du droit de recevoir un sous-ensemble de données à caractère personnel, de stocker ces données sur un dispositif privé, sans nécessairement suivre une transmission immédiate à un autre responsable du traitement[44].

Proche du droit d'accès, il est en fait plus que cela : il en est le complément. La spécificité de la portabilité est qu'elle offre un outil pratique à la personne concernée pour gérer et réutiliser les données la concernant, en fonction de ses souhaits et de ses intérêts.

Enfin, le droit à la portabilité des données à caractère personnel doit conduire le responsable du traitement à s'efforcer de fournir un meilleur service, faute de quoi la personne concernée demandera le transfert des données à un concurrent et, éventuellement, exercera également le droit à l'oubli des données par le premier.

Par conséquent, on peut conclure que, dans le contexte européen, le droit à la portabilité s'applique lorsque le traitement des données est automatisé, lorsqu'il résulte du consentement de la personne concernée ou lorsqu'il est nécessaire à l'exécution d'un contrat. Toutes les autres hypothèses sont en dehors de son champ d'application, qui inclut celles où le traitement découle d'obligations légales auxquelles le responsable du traitement est tenu. Il est également clair qu'en aucun cas l'exercice du droit à la portabilité ne peut porter atteinte aux droits des tiers, ainsi que

[44] Graça Canto MONIZ, *Anuário da Proteção de Dados: 2018*, Lisboa, Faculdade de Direito, Universidade Nova de Lisboa, 2018.

la nécessité d'assurer la compatibilité entre le droit à la portabilité et le droit à l'effacement ou à l'oubli.

Dans l'ensemble, le règlement sur la portabilité des données dans l'Union européenne est une réponse directe à la nécessité de responsabiliser les individus par rapport à leurs données personnelles et de favoriser un environnement de protection des données plus transparent et axé sur l'utilisateur. Il joue un rôle clé dans la promotion de la vie privée, du choix des consommateurs et de la concurrence sur le marché numérique.

Il ressort également de la lecture du RGPD, notamment à la lumière du considérant 68, que si le droit à la portabilité est un encouragement à l'interopérabilité, il ne crée pas d'obligation pour les acteurs de maintenir des systèmes interopérables, et que les conflits qui en découlent devraient être résolus sur la base de ce qui est techniquement faisable.

2.2.2 Mise en œuvre de la portabilité en droit européen

L'interopérabilité des systèmes est l'un des défis majeurs de l'exercice du droit à la portabilité, comme nous le verrons plus loin.

La Commission européenne, afin de guider l'adoption de pratiques d'interopérabilité dans les services publics, a publié la *European Interoperability Framework* (EIF) :

> The European Interoperability Framework (EIF) is part of the Communication (COM (2017) 134) from the European Commission adopted on 23 March 2017. The framework gives specific guidance on how to set up interoperable digital public services.
>
> It offers public administrations 47 concrete recommendations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that both existing and new legislation do not compromise interoperability efforts.
>
> The new EIF is undertaken in the context of the Commission priority to create a Digital Single Market in Europe. The public sector, which accounts for over a quarter of total employment and represents approximately a fifth of the EU's GDP through public procurement, plays a key role in the Digital Single Market as a regulator, services provider and employer.

> The successful implementation of the EIF will improve the quality of European public services and will create an environment where public administrations can collaborate digitally.[45]

L'objectif principal du FEI est de garantir que les différents systèmes informatiques utilisés par les gouvernements, les entreprises et les organisations de l'UE puissent fonctionner ensemble de manière efficace et efficiente, en permettant l'échange d'informations et de services d'une manière harmonisée.

L'EIF a été élaboré en réponse à la complexité et à la diversité croissantes des systèmes informatiques dans l'Union européenne. Il définit un ensemble de principes et de lignes directrices techniques visant à faciliter l'échange de données et de services entre des systèmes hétérogènes. Cela est particulièrement important à une époque où les gouvernements et les entreprises dépendent de plus en plus des systèmes informatiques pour fournir des services publics, prendre des décisions éclairées et faciliter la coopération transfrontalière.

Le cadre souligne l'importance des normes ouvertes et des solutions technologiques interopérables. Il encourage l'adoption de formats de données et de protocoles de communication qui permettent à différents systèmes de comprendre et de traiter les informations de manière cohérente. Cela permet non seulement de réduire la complexité technique, mais aussi de promouvoir l'innovation et la collaboration.

En outre, l'EIF souligne l'importance de la collaboration et de la coordination entre les différentes parties prenantes, qu'il s'agisse de gouvernements, d'entreprises ou d'organisations à but non lucratif. Il souligne la nécessité d'une approche holistique de l'interopérabilité, prenant en compte les aspects techniques et organisationnels.

[45] Alain DE GANCK, « The New European Interoperability Framework », *ISA² - European Commission* (16 février 2017), en ligne : <http://webserver:8080/isa2/eif_en> (consulté le 28 juillet 2023).

2.3 Législation canadienne

2.3.1 L'ancien Projet de Loi C-11 (2020)

La principale loi fédérale canadienne traitant de la protection des données personnelles dans le secteur privé était la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui ne contient pas de dispositions spécifiques pour la portabilité des données comme celles que l'on trouve dans le Règlement général sur la protection des données (RGPD) de l'Union européenne.

Conscient de la nécessité de mettre à jour sa législation en matière de protection de la vie privée pour tenir compte des exigences croissantes des consommateurs et des défis posés par les nouvelles technologies et pratiques commerciales, le Canada a commencé à se pencher sur des réformes législatives qui pourraient inclure des droits plus spécifiques, tels que ceux liés à la portabilité des données.

Le Projet de Loi C-11, présenté à la Chambre des communes en 2020, visait à mise en œuvre de la Charte du numérique, sous la forme de la *Loi édictant la Loi sur la protection de la vie privée des consommateurs* (LPVPC) et la *Loi sur le Tribunal de la protection des renseignements personnels et des données* (LTPRPD) et apportant des modifications corrélatives et connexes à d'autres lois.

Il convient de noter que le projet de loi a été vivement critiqué par le commissaire à la protection de la vie privée (CPVP) de l'époque, Daniel Therrien :

> Comme je l'ai indiqué lors de ma comparution dans le cadre du Budget principal des dépenses et de votre étude sur la technologie de reconnaissance faciale, je crois que le projet de loi C-11 représente globalement un recul par rapport à notre loi actuelle et qu'il nécessite des changements importants si l'on veut rétablir la confiance dans l'économie numérique. Mon mémoire décrit les nombreuses améliorations nécessaires pour que les organisations puissent innover de façon

> responsable tout en reconnaissant et en protégeant le droit à la vie privée des Canadiens.[46]

Cependant, parmi les nouveautés apportées par la norme, l'article 72 se démarque :

> Communication conformément à un cadre de mobilité des données
>
> 72 Sous réserve des règlements et sur demande de l'individu, une organisation communique, dès que possible, les renseignements personnels qu'elle a recueillis auprès de lui à l'organisation que ce dernier désigne si ces deux organisations sont soumises à un cadre de mobilité des données prévu par règlement.[47]

Malheureusement, ce projet est mort au feuilleton lors du déclenchement des élections fédérales de 2021. La tentative de réforme a toutefois été déposée à nouveau, le 16 juin 2022, sous la forme du Projet de Loi C-27. Cette nouvelle tentative de mise à jour des règles de protection des données des consommateurs revient sur le texte précédemment publié.

2.3.2 Projet de Loi C-27 : Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois

Comme indiqué précédemment, le nouveau projet de loi reprend la plupart des textes juridiques antérieurs, en innovant dans le domaine de l'intelligence artificielle, de sorte que les études réalisées sur les règlements antérieurs s'appliquent au projet de loi actuel soumis au Parlement canadien.

---

[46] Commissariat à la protection de la vie privée du CANADA, *Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la Loi de 2020 sur la mise en œuvre de la Charte du numérique*, 11 mai 2021, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_ethi_c11_2105/> (consulté le 15 août 2023).

[47] « Projet de loi émanant du Gouvernement (Chambre des communes) C-11 (43-2) - Première lecture - Loi de 2020 sur la mise en oeuvre de la Charte du numérique - Parlement du Canada », en ligne : <https://www.parl.ca/DocumentViewer/fr/43-2/projet-loi/C-11/premiere-lecture> (consulté le 15 juillet 2023).

Au départ, le texte présente le même exposé sur la portabilité :

> Mobilité des renseignements personnels
>
> 72 Communication conformément à un cadre de mobilité des données

Comme on peut le voir, cet article permet au consommateur de consentir (ou d'exiger) de l'institution dans laquelle il a déjà déposé des données personnelles, qu'elle procède à la portabilité de celles-ci à un tiers :

> La LPVPC intègre le concept de portabilité des données dans la loi, sous la forme d'un droit à la mobilité des renseignements personnels. Ce droit permet à un individu de demander que les renseignements personnels qu'une organisation a recueillis auprès de lui soient transmis à une autre organisation de son choix. Cependant, ce transfert n'est permis que lorsque les deux organisations en question sont soumises à un cadre de mobilité des données prévu par un règlement à venir.[48]

Cette portabilité est présentée comme un nouveau moyen de transmission et communication des données des consommateurs, doté toutefois de quelques particularités.

Comme expliquent les Professeures Gautrais et Trudel :

> La communication se distingue donc de la transmission qui consiste à rendre disponible un document pour une communication. Tant que le document n'est que transmis, il n'est pas effectivement communiqué. Par contre, la transmission se présente habituellement comme une situation ayant vocation à mener à la communication du document.[49]

Ce type de communication de données nécessite le véritable partage des éléments avec un tiers, afin que l'entreprise qui reçoit les données sans ingérence de la part du consommateur (en dehors de son consentement préalable) :

> Ce droit s'appliquera uniquement aux renseignements personnels recueillis auprès des individus (c'est-à-dire, pas auprès de tiers). Les cadres de mobilité des

[48] *Résumé législatif du 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* [*Résumé législatif du projet de loi C-11*], en ligne : <https://lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/LegislativeSummaries/432C11E> (consulté le 13 juillet 2023).

[49] V. GAUTRAIS et P. TRUDEL, préc., note 7.

> données qui seront créés par voie réglementaire devront comporter des garanties pour la divulgation sécurisée des renseignements et des paramètres pour les moyens techniques permettant d'assurer l'interopérabilité (art. 120). Ils devront également préciser les organisations soumises au cadre, qui appartiendront probablement à des secteurs industriels spécifiques tels que les systèmes bancaires ouverts ou les télécommunications.[50]

Comme le souligne la professeure Scassa, dans le modèle prévu par le droit canadien, contrairement aux dispositions de la norme de l'Union européenne, les données circulent entre les organisations à la demande de l'individu, sans passer par lui. Ceci est dû au fait que l'applicabilité de la portabilité est liée à la présence d'une structure qui permet la communication.

Il existe également des vides juridiques qui doivent être comblés afin de garantir la sécurité des données personnelles, comme la définition de « structure de mobilité des données » :

> The regulations provide for frameworks that will impose security safeguards on participating organizations, and ensure data interoperability. Paragraph 120(b) also suggests that not all organizations within a sector will automatically be entitled to participate in a mobility framework; they may have to qualify by demonstrating that they meet certain security and technical requirements. A final (and interesting) limitation on the mobility framework relates to exceptions to disclosure where information that might otherwise be considered personal information is also proprietary or confidential commercial information. This gets at the distinction between raw and derived data – data collected directly from individuals might be subject to the mobility framework, but profiles or analytics based on that data might not – even if they pertain to the individual.[51]

Il est important de souligner la présence du terme « cadre de mobilité des données », car il s'agit d'une différence majeure par rapport au RGPD. Le cadre de mobilité peut être compris comme une structure qui décrit les lignes directrices et les règlements relatifs au transfert et au mouvement des données entre différentes entités ou plateformes (en d'autres termes : l'interopérabilité).

---

[50] Éloïse GRATTON, Elisa HENRY, François JOLI-COEUR, Max JARVIE, Daniel J MICHALUK, Katherine M STRANGER, Andy NAGY et Ira PARGHI, « Loi sur la protection de la vie privée des consommateurs du Canada (projet de loi C-27) : incidences sur les entreprises », *BLG*, en ligne : <https://www.blg.com/fr/insights/2020/11/canadas-consumer-privacy-protection-act-impact-for-businesses> (consulté le 23 mars 2023).

[51] T. SCASSA, préc., note 30.

Approfondir le concept, nous pouvons comprendre qu'il fait référence à l'ensemble des protocoles, outils et lignes directrices qui permettent le transfert sécurisé de données à caractère personnel entre différentes plateformes, services ou juridictions. Dans un monde où les gens utilisent de multiples services en ligne et transfèrent leurs données en permanence, une définition claire et complète de ce terme est essentielle. En l'absence d'une définition claire, les entreprises et les particuliers peuvent trouver des failles qui permettent d'utiliser les informations à mauvais escient, voire de les vendre sans le consentement adéquat.

En outre, en établissant un cadre clair pour la mobilité des données, les gouvernements et les institutions peuvent créer des normes qui garantissent la protection des données en transit. Ainsi, quel que soit l'endroit où les données sont stockées ou traitées, des mesures de sécurité uniformes seront mises en place.

Comme nous le verrons dans le dernier chapitre de ce travail, la loi, comme le RGPD, établit une notion générale de portabilité qui devrait faire l'objet d'une réglementation spécifique pour permettre son fonctionnement.

2.4 Législation québécoise

La législation québécoise a fait l'objet d'une importante mise à jour en matière de traitement, de conservation et de protection des données à caractère personnel, comme on le verra ci-dessous.

2.4.1 La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*

Le Projet de Loi n° 64, présenté en 2020, a été adopté le 21 septembre 2021 par l'Assemblée nationale du Québec. La nouvelle *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi nº 25) vise à actualiser le régime de protection des données dans les sphères privée et publique.

Cette nouvelle loi :

> […] modernise l'encadrement applicable à la protection des renseignements personnels dans diverses lois, dont la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels dans le secteur privé.[52]

La modernisation est une étape législative importante qui vise à améliorer la confidentialité des données et à renforcer la protection des consommateurs dans la province de Québec. Introduit en réponse aux nouveaux défis liés à la protection de la vie privée et à l'utilisation des données personnelles à l'ère numérique, le projet de loi vise à moderniser les réglementations existantes et à s'aligner sur les normes internationales en matière de protection de la vie privée.

L'une des principales caractéristiques du Projet de Loi nº 64 est le renforcement du contrôle de l'individu sur ses propres données personnelles. Il propose la mise en œuvre de mesures plus strictes en matière de consentement éclairé, garantissant que les citoyens comprennent clairement comment leurs données seront collectées, utilisées et partagées. En outre, la législation proposée cherche à faciliter l'exercice des droits d'accès, de rectification et de suppression des données, donnant aux individus un plus grand degré d'autonomie sur leurs informations personnelles.

Un autre aspect pertinent du projet de loi est l'accent mis sur la responsabilité des organisations qui collectent et traitent des données à caractère personnel. Il exige des entreprises qu'elles adoptent des mesures de cybersécurité adéquates pour protéger les données des consommateurs contre les violations et les fuites. En outre, il introduit l'obligation de notification immédiate en cas d'incidents de sécurité, afin de minimiser les dommages et d'accroître la transparence.

Le projet de loi nº 64 reconnaît également l'importance de la conformité réglementaire au niveau mondial. En mettant en œuvre des exigences plus strictes pour le transfert international

[52] *LQ 2021, c 25 | Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, en ligne : <https://www.canlii.org/fr/qc/legis/loisa/lq-2021-c-25/derniere/lq-2021-c-25.html?searchUrlHash=AAAAAQBmTG9pIG1vZGVybmlzYW50IGRlcyBkaXNwb3NpdGlvbnMgbMOpZ2lzbGF0aXZlcyBlbiBtYXRpw6hyZSBkZSBwcm90ZWN0aW9uIGRlcyByZW5zZWlnbmVtZW50cyBwZXJzb25uZWxzAAAAAAE&resultIndex=1> (consulté le 13 juillet 2023).

de données, le Québec cherche à aligner sa législation sur les normes internationales en matière de protection de la vie privée, telles que le RGPD de l'Union européenne.

Ce processus a débuté en 2020, avec la présentation du projet de loi, a produit ses premiers effets en 2022 et représente une avancée majeure dans le domaine de la vie privée et de la protection des données, avec en point d'orgue le droit à la portabilité, qui entrera en vigueur en 2024 :

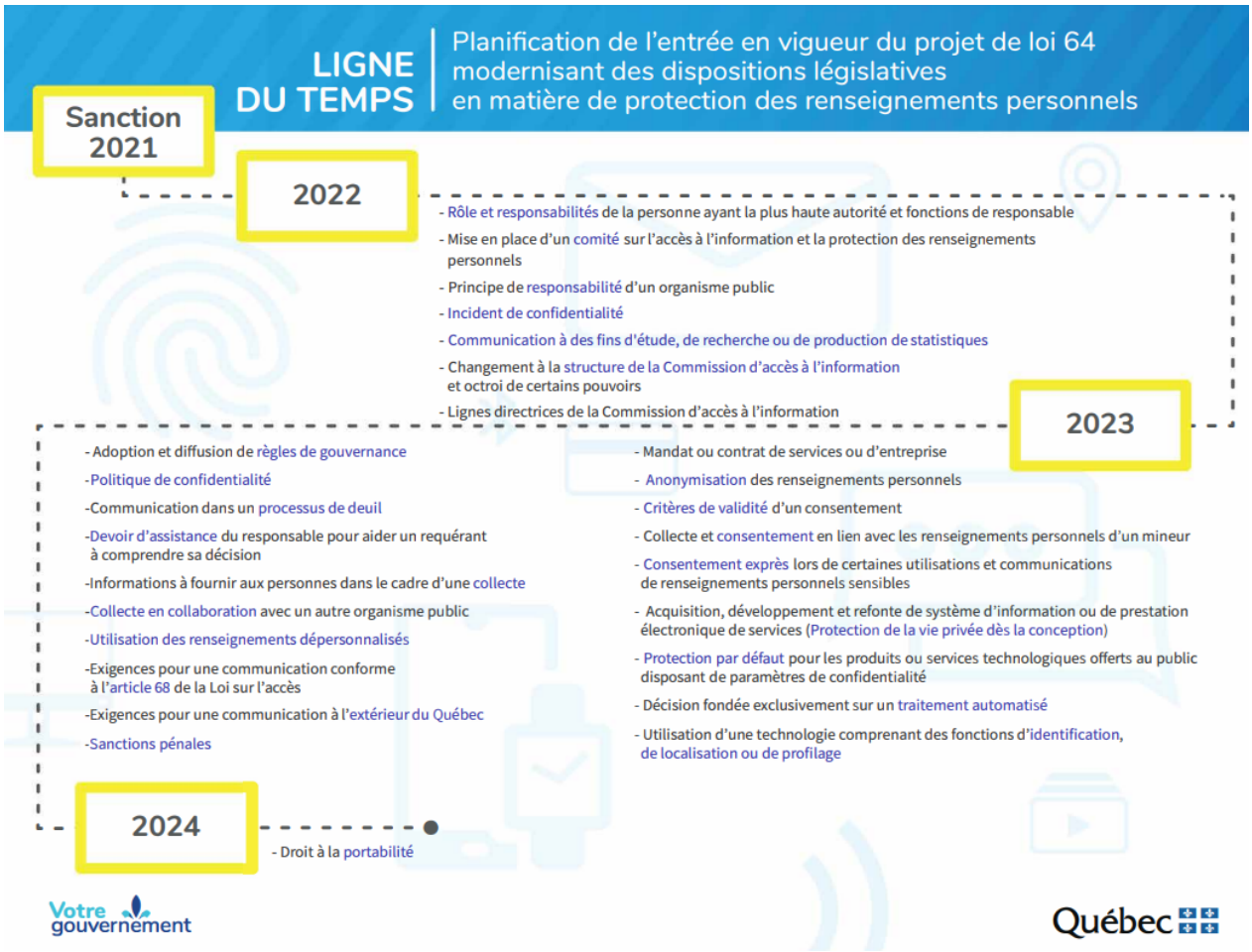

Figure 2. – Ligne du temps – Projet de loi nº 64 du Québec « https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/LigneTemps_PL64.pdf »

Le premier changement majeur est la présence du délégué à la protection des données personnelles, tout comme le responsable du traitement dans le RGPD (articles 37 et 38), mais il y a quelques différences entre les deux figures :

> La Loi 64 n'exige pas l'allocation de ressources au responsable de la PRP.
>
> La Loi 64 n'interdit pas à l'entreprise de donner des instructions au responsable de la PRP.
>
> La Loi 64 ne prévoit pas, non plus, d'interdictions de représailles à l'endroit du responsable de la PRP (toutefois, toute personne qui dépose une plainte ou coopère à une enquête de la CAI est protégée contre les représailles).
>
> Une entreprise n'est pas tenue de communiquer les coordonnées du responsable de la PRP à la CAI (bien que la CAI ait des pouvoirs étendus pour demander ces informations; ces informations doivent également être publiées sur le site Internet de l'entreprise).[53]

Le Projet de loi nº 64 suit de plus près l'approche normative du RGPD et inclut de nouveaux droits à la vie privée tels que la portabilité des données et le droit à l'oubli, tout en appelant à une plus grande transparence et à un meilleur contrôle (la figure du responsable de la protection des renseignements personnels se démarque).

L'innovation en matière de portabilité réside dans deux articles de la loi qui modifient les règles existantes.

2.4.2 Portabilité dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*

L'article 30 du projet susmentionné modifie l'article 84 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels:

[53] Éloïse GRATTON, Elisa HENRY, François JOLI-COEUR, Simon DU PERRON, Max JARVIE, Julie M. GAUTHIER, Andy NAGY, Danie-Nicolas EL KHOURY, Anthony HÉMOND et CAtherine LABASI-SAMMARTINO, *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*, en ligne : <https://blgaccprd10-cm.azurewebsites.net/fr/insights/2021/11/quebec-privacy-law-reform-a-compliance-guide-for-organizations> (consulté le 2 août 2023).

> 30. L'article 84 de cette loi est modifié par l'insertion, après le deuxième alinéa, du suivant :
>
> « À moins que cela ne soulève des difficultés pratiques sérieuses, un renseignement personnel informatisé recueilli auprès du requérant, et non pas créé ou inféré à partir d'un renseignement personnel le concernant, lui est, à sa demande, communiqué dans un format technologique structuré et couramment utilisé. Ce renseignement est aussi communiqué à sa demande à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement. ».[54]

L'article délimite les données pouvant faire l'objet d'une portabilité comme étant celles qualifiées d'« informations personnelles informatisées collectées auprès du demandeur », à l'exclusion des données générées par le système lui-même, c'est-à-dire celles provenant du traitement propre de l'organisme.

En outre, la portabilité, comme le montrent les modèles législatifs précédemment cités, est subordonnée à la demande de la personne concernée et dépendra toujours d'un format technologique structuré. Cependant, la loi ne détermine pas quel est ce « format ».

2.4.3 Portabilité dans la *Loi sur la protection des renseignements personnels dans le secteur privé*

L'article 120, quant à lui, traite de la modification de l'article 27 de la *Loi sur la protection des renseignements personnels dans le secteur privé* :

> 120. L'article 27 de cette loi est modifié par le remplacement du premier alinéa par les suivants :
>
> « Toute personne qui exploite une entreprise et détient un renseignement personnel sur autrui doit, à la demande de la personne concernée, lui en confirmer l'existence et lui donner communication de ce renseignement en lui permettant d'en obtenir une copie.
>
> À la demande du requérant, un renseignement personnel informatisé doit être communiqué sous la forme d'une transcription écrite et intelligible.

[54] *LQ 2021, c 25 | Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, préc., note 52.

> À moins que cela ne soulève des difficultés pratiques sérieuses, un renseignement personnel informatisé recueilli auprès du requérant, et non pas créé ou inféré à partir d'un renseignement personnel le concernant, lui est, à sa demande, communiqué dans un format technologique structuré et couramment utilisé. Ce renseignement est aussi communiqué à sa demande à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement ».[55]

La formulation choisie crée le droit à la portabilité, avec les objectifs précédemment détaillés, à savoir : faciliter la réutilisation des données et améliorer la capacité des consommateurs à changer de fournisseur, renforçant ainsi le contrôle individuel sur leurs informations personnelles et incitant à une plus grande concurrence.

Il convient de souligner l'absence de disposition relative à un cadre de mobilité des données, contrairement à la loi fédérale.

Il convient de noter que l'article aborde directement le droit d'accès en autorisant la confirmation de l'existence de l'information et l'accès à celle-ci, avec la fourniture de copies, qui peuvent être obtenues sous la forme d'une transcription écrite et intelligible, à l'exemple de la législation européenne

Ce droit, fondamental dans les sociétés démocratiques, garantit que les individus ont le pouvoir non seulement de valider la présence d'informations spécifiques, mais aussi de demander et d'obtenir un accès complet à ces informations. L'importance de ce droit est amplifiée si l'on considère la transparence, la responsabilité et l'autodétermination en matière d'information comme des piliers fondamentaux de l'interaction entre les citoyens et les institutions.

En outre, le texte juridique reconnaît la nécessité de fournir des moyens pratiques pour l'exercice de ce droit. Cela se traduit par la fourniture explicite de copies des informations demandées. Ces copies, comme stipulé, doivent être mises à disposition de manière qu'elles soient non seulement physiquement accessibles, mais aussi compréhensibles pour le demandeur. En d'autres termes, la transcription des informations doit être claire, lisible et structurée de manière à faciliter la compréhension et l'analyse critique par le demandeur.

[55] *Id.*

Contrairement à la loi régissant les actions des organismes publics, la loi sur le secteur privé semble s'adresser au responsable du traitement des données dans l'entreprise plutôt qu'à la personne concernée elle-même.

Il existe cependant de grandes similitudes dans la formulation, toujours liée à la demande de l'individu propriétaire des données, excluant celles créées ou déduites d'informations personnelles relatives au demandeur et, encore une fois, traitant du concept de format technologique structuré et couramment utilisé, sans l'approfondir.

Enfin, il convient de noter que ces deux modifications de la législation québécoise n'entreront en vigueur qu'en septembre 2024.

2.5 Les différentes approches

Sur la base de la brève analyse de la législation étudiée, il est possible de percevoir l'existence de similitudes et de distances entre les normes.

Tout d'abord, nous soulignons les différentes étapes du processus législatif de chacune d'entre elles : le RGPD est une réglementation établie de longue date ; la loi fédérale canadienne est encore en deuxième lecture à la Chambre des communes et constitue la deuxième tentative de mise à jour et de modernisation des règles fédérales de protection de la vie privée ; et, bien que ce projet d'avancement de la matière soit déjà devenu la loi québécoise n° 25, les articles faisant référence à la portabilité ne sont pas encore en vigueur.

Un deuxième point est la distinction claire dans le traitement de la notion de portabilité. Le règlement européen établit clairement que la portabilité est un droit, ce qui n'est pas le cas dans le projet de loi soumis au Parlement canadien :

> De plus, le projet de loi C-11, contrairement au RGPD, ne confère pas le même statut au droit à la mobilité des données que celui conféré au droit d'accès aux renseignements personnels, ou au nouveau droit permettant de demander le retrait de renseignements personnels. Plus précisément, le projet de loi C-11 n'exige pas que le droit à la mobilité soit mentionné dans les déclarations sur la protection des renseignements personnels destinées au public (c'est-à-dire le résumé des politiques et pratiques d'une organisation en matière de protection des renseignements

> personnels généralement affiché sur les sites Web). Le projet de loi n° 64 du Québec adopte la même ligne de conduite — probablement parce que, comme nous l'avons déjà mentionné, ce projet de loi traite la mobilité des données comme une version améliorée du droit d'accès plutôt que comme un droit véritablement distinct.[56]

En revanche, si les articles des lois modifiées par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* ne mentionnent pas la portabilité comme un droit, l'ensemble du projet de modernisation, ainsi que les canaux de communication officiels du gouvernement provincial, le reconnaissent.

Il est observé, de façon générale, que la législation susmentionnée crée le droit à la portabilité dans sa sphère de compétence respective. Cependant, l'applicabilité de ce droit est conditionnée par les termes vagues de la loi, une situation qui laisse les entreprises dans l'attente d'une réglementation plus objective sur la manière de procéder à la portabilité, en les protégeant et en les exposant à d'éventuelles sanctions, ainsi qu'en sauvegardant la protection des données des consommateurs :

> Il est à noter que l'article 72 du projet de loi concerne la communication directe de renseignements personnels d'une organisation à une autre. Il ne confère pas à un individu le droit d'obtenir une copie de ses propres renseignements personnels dans un format utilisable, comme le prévoit la loi n° 64 du Québec aux termes de laquelle les individus peuvent demander et obtenir leurs propres renseignements personnels dans un « format technologique structuré et couramment utilisé.[57]

Il y a un débat important lié à la faisabilité de la portabilité elle-même, car, malgré ses nobles objectifs, son efficacité dépend essentiellement de la résolution du problème d'interopérabilité entre le contrôleur de données qui enverra les données et le propriétaire ou le nouveau contrôleur de données qui les recevra, puisque la portabilité vise à donner aux individus un plus grand contrôle sur leurs données et à accroître la compétitivité entre les entreprises. Toutefois, en l'absence de règles claires, il peut y avoir des ambiguïtés sur la manière et le

[56] Daniel FABIANO et Julie UZAN-NAULIN, « Projet de loi C-11 – Mobilité des données : un pas supplémentaire vers le RGPD » (15 décembre 2020), en ligne : <https://www.fasken.com/fr/knowledge/2020/12/15-bill-c-11-data-mobility-another-step-towards-the-gdpr> (consulté le 23 mars 2023).

[57] *Id.*

moment où les données peuvent être transférées, ce qui peut entraîner des violations involontaires des droits des personnes concernées.

Il semble que ce soit la raison pour laquelle toutes les normes mentionnées précédemment présentent des termes vagues lorsqu'elles traitent du cadre de la portabilité, ce qui ouvre la porte à l'adoption d'une réglementation pertinente dans les différents secteurs et marchés qui appliqueront la portabilité.

L'action de l'organisme de réglementation est nécessaire pour assurer un maintien adéquat de la protection, en évitant une fragilité croissante au cours du processus qui sera adopté pour la migration des données personnelles et le consentement, moteur de la portabilité, doit être préservé comme un droit du consommateur et non comme un instrument de manipulation, où le consommateur sera amené à accorder ce consentement à n'importe quelle entreprise.

Chapitre 3 – La faisabilité de la portabilité en pratique

Le nouveau droit à la mobilité des informations personnelles reflète la réalité des temps modernes et la nécessité de transférer des données entre organisations. Lorsque deux organisations ou plus sont soumises au cadre juridique de la mobilité des données, une personne peut demander à une organisation de divulguer les informations personnelles qu'elle détient à son sujet à une autre organisation désignée.

Comme indiqué précédemment, la portabilité des données, c'est-à-dire la possibilité pour les individus d'obtenir et de réutiliser leurs données personnelles d'une entité à l'autre, a pris de l'importance avec l'avènement de l'économie numérique et la numérisation accrue des services. Ce droit, essentiel à la promotion de l'autonomie individuelle et de la concurrence sur le marché numérique, nécessite une réglementation adéquate pour être mis en œuvre de manière efficace et sûre.

Le transfert de données entre entités présente des risques pour la sécurité des entreprises et des utilisateurs. Une réglementation appropriée établirait des protocoles et des normes de sécurité à respecter, garantissant que les données d'un individu sont transférées de manière sécurisée, minimisant ainsi le risque de fuites ou d'accès non autorisé.

L'un des objectifs de la portabilité, outre les avantages qu'elle confère aux consommateurs, est de stimuler la concurrence en permettant aux utilisateurs de changer facilement de fournisseur de services. Une réglementation claire garantirait que toutes les entreprises opèrent sur un pied d'égalité, encourageant l'innovation et empêchant les pratiques monopolistiques.

En outre, l'un des plus grands défis, sinon le plus grand, pour l'adoption de la portabilité est l'interopérabilité des systèmes, car pour que la portabilité des données soit efficace, les différents systèmes et plateformes doivent pouvoir communiquer entre eux. La réglementation devrait définir des normes techniques pour garantir cette interopérabilité.

Les fournisseurs de services et les entreprises ont besoin de lignes directrices claires sur la manière de procéder à la portabilité. Dans certains contextes, il peut ne pas être approprié ou possible d'autoriser la portabilité des données. En cas de non-respect des règles de portabilité, il doit y avoir des mécanismes efficaces de responsabilité et de recours.

Il est donc impératif de définir la manière dont la portabilité devrait affecter les entreprises, ainsi que la manière dont elle sera maintenue en tant que droit des consommateurs et, par le biais de la réglementation, de résoudre les problèmes d'interopérabilité et d'atténuer les risques.

3.1 La portabilité des données du point de vue des entreprises

Pour les entreprises, la question de la portabilité représente une intersection complexe entre la technologie, la réglementation, la stratégie concurrentielle et les droits des consommateurs.

Les entreprises ne sont plus assurées de conserver les utilisateurs sur la seule base de la possession exclusive de leurs données. Cela pourrait stimuler la concurrence, car les nouveaux arrivants sur le marché peuvent plus facilement attirer les clients en leur promettant de meilleurs services grâce à la portabilité des données :

> Dans ce contexte, le droit à la portabilité pourrait permettre aux entreprises de récupérer l'intégralité des données générées et qui sont stockées et/ou traitées chez un fournisseur de services numériques, afin notamment de les transférer chez un autre prestataire de services. Il s'agirait ainsi d'un outil de promotion de la concurrence et de l'innovation sur le marché européen du *cloud computing*. Plus généralement, en redonnant aux entreprises la maîtrise de leurs données, la portabilité pourrait être un instrument de rééquilibrage de l'asymétrie de pouvoirs entre utilisateurs et services de l'économie numérique. Un tel droit permettrait de lutter contre les effets de verrouillage et de fuite de la valeur en rendant possible le développement de services en interne ou au niveau d'un secteur professionnel.[58]

[58] Célia ZOLYNSKI et Marylou LE ROY, « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », (2017) 59-2 *LEGICOM* 105-113, DOI : 10.3917/legi.059.0105.

La portabilité des données impose aux entreprises le défi technique de créer des systèmes permettant un transfert efficace et sécurisé des données. En outre, les données, une fois transférées, doivent être compatibles avec les systèmes du nouveau service ou fournisseur. Cela nécessite des normes techniques et des formats interopérables qui continuent d'évoluer. L'absence de normes universelles peut conduire à des solutions fragmentées et à une augmentation des coûts pour les entreprises.

Les entreprises doivent non seulement s'assurer que les données peuvent être transférées, mais aussi que ce transfert ne viole pas d'autres normes de protection des données ou les droits de tiers. Le non-respect de ces règles peut entraîner des sanctions importantes, comme cela a été le cas pour Facebook. Il convient de souligner que toutes les lois étudiées ici tiennent le responsable du traitement pour responsable de la mauvaise gestion des données à caractère personnel :

> Le principe de responsabilité appliqué au responsable de traitement, défini à l'article 24 du RGPD, oblige celui-ci à mettre en place une véritable démarche de conformité. Le texte prévoit que « le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées » pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent RGPD. La mise en œuvre de politiques appropriées a été en grande partie anticipée au sein des grandes entreprises. C'est donc surtout sur les entreprises de plus petites tailles que cette charge va peser. À cette fin, la CNIL a, par ailleurs, commencé à préparer l'entrée en vigueur des textes par la création du label gouvernance Informatique et libertés. Celui-ci définit clairement les procédures à mettre en place pour une bonne gestion des données personnelles.[59]

La croissance de la concurrence, autre point important du droit à la portabilité, présente également ses défis :

> It is still unclear what impact the GDPR's right to data portability exactly has on competition and innovation and if it can indeed foster competition between data controllers and encourage data-driven innovation, as was expected as a positive side effect of the new right at the time of adoption. In particular, competition may increase in markets where data portability would make it easier for individuals to switch

[59] Romain GOLA, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », (2017) 59-2 *LEGICOM* 29-38, DOI : 10.3917/legi.059.0029.

> between services by taking their data with them. A prerequisite for this is that individuals actively invoke their right to data portability.
>
> Despite its potential to stimulate competition and innovation, concerns are now expressed that data portability can strengthen the position of established players by letting their users invoke the right to data portability to get even more data. This would lower competition because smaller firms would then see their users move with their data to the established players. For instance, economic modelling has suggested that data portability's prospect of easier switching can lure consumers into providing more data to the incumbent. Because of the additional data, the incumbent gets a competitive advantage in performing data analytics that can raise entry barriers for newcomers. A recent review of economic literature expects data portability not to lead to less or more competition in established digital markets by itself, but does point at its ability to encourage innovation in complementary and new digital markets by letting innovation at the service and at the data analytics levels take place within different firms at the same time.[60]

Malgré les défis, la portabilité des données offre également des opportunités. Les entreprises peuvent se différencier par la manière dont elles facilitent la portabilité pour leurs utilisateurs, devenant ainsi des leaders en matière de pratiques éthiques de gestion des données. En outre, le besoin de systèmes interopérables peut stimuler l'innovation et créer de nouveaux créneaux pour les solutions de portabilité.

Bien qu'elle pose des défis importants en termes de mise en œuvre et de conformité, les entreprises proactives qui considèrent la portabilité comme une opportunité stratégique sont bien placées pour exceller dans un marché axé sur le consommateur. À long terme, la portabilité des données pourrait bien être le catalyseur d'un environnement numérique plus transparent, plus compétitif et plus centré sur l'utilisateur.

3.2 Le maintien de la portabilité en tant que droit du consommateur

La portabilité des données doit être effectuée dans un environnement sécurisé. Ce n'est pas parce qu'un responsable du traitement devra transmettre les données à un autre, ce qui peut

[60] I. GRAEF, préc., note 23.

même aller à l'encontre de ses intérêts économiques, qu'il doit négliger l'obligation de protéger ces données.

Le nouveau responsable du traitement qui recevra les données doit avoir le même souci de sécurité. Il devra également adopter des mesures susceptibles de maintenir la protection des données.

L'opération de transmission des données à des fins de portabilité, bien qu'elle soit effectuée à la demande de la personne concernée, doit être réalisée avec le même soin que tout autre traitement :

> Considering the shortcomings of competition law, especially the lack of tools for assessing dominance in a specific market for personal data, it seems very hard to protect consumers from lock-in effects and switching costs and also interoperability without first defining a relevant market for personal data. As we saw, for its characteristics is hard to categorise data as an essential facility, especially because it does not easily comply with test such as refusal to grant access and refusal to deal. We cannot oblige big undertakings if first we do not prove that they are dominant and they are committing an abuse. Consequently, as data protection is the area which overlaps with competition law in terms of consumer welfare, we recommend to analyse the rules of the GDPR regarding the right to data portability in order to reduce the user lock-in effect and switching cost. From the phrasing of the GDPR, seems that the right to data portability does not only empower consumers to control the flow of their data, but it also could foster the creation of interoperability and consequently grant data access to other firms to personal data of users who want to switch.[61]

La portabilité des données n'est pas effectuée sur la base du consentement de la personne concernée, mais en réponse à sa demande expresse. En d'autres termes, dans cette opération spécifique, la personne concernée agit comme le véritable responsable du traitement de l'opération, qui sera effectuée sur son ordre et dans son intérêt exclusif :

> The second and proper aspect of the right to data portability can be found in the second sentence of Article 15(2a) of the amended proposal which gives users the right to transfer their personal data to another processing system. This aspect of the right to data portability goes beyond the right to obtain a copy as contained in the first

[61] C. BANDA, préc., note 26.

> sentence of Article 15(2a), since it requires controllers to transmit the data directly to another controller at the request of the data subject.[62]

En ce sens, il serait raisonnable de comprendre que le responsable du traitement qui transmet les données à caractère personnel à un autre fournisseur agit comme un simple opérateur de l'activité.

Cela ne signifie toutefois pas que le responsable du traitement qui transmet les données n'est pas tenu d'assurer la sécurité de l'opération. Au contraire, le responsable du traitement qui transmet les données doit même s'assurer que les données ont été correctement transmises au destinataire.

Mais la responsabilité s'arrête à la transmission sécurisée des données. Le responsable du traitement qui transmet les données ne peut être tenu responsable des violations des droits de la personne concernée causées par le nouveau responsable du traitement. Le choix du destinataire des données appartenant exclusivement à la personne concernée, celle-ci ne pourra évidemment pas engager la responsabilité du responsable du traitement qui transmet les données pour un traitement abusif effectué par le responsable du traitement qui reçoit les données.

En effet, le responsable du traitement qui transmet les données ne peut être tenu responsable du traitement effectué que jusqu'à la portabilité - ou plutôt jusqu'à la conclusion de la transmission des données au nouveau responsable du traitement - sauf dans les cas où il dispose d'un support juridique et conserve des copies des données transférées et continue, sous sa seule responsabilité, à les traiter.

Le responsable du traitement qui reçoit les données est quant à lui responsable de tous les traitements qu'il effectue avec les données à caractère personnel reçues, et il est responsable du respect des règles juridiques applicables et des finalités pour lesquelles il a reçu les données.

[62] I. GRAEF, J. VERSCHAKELEN et P. VALCKE, préc., note 25.

3.3 Le besoin de réglementation

Il est certain qu'avec une réglementation adéquate, il serait beaucoup plus facile de garantir l'interopérabilité sur la base de critères raisonnables et réalisables, ce qui est particulièrement important pour les petites et moyennes entreprises, pour lesquelles il faut trouver un terrain d'entente afin qu'elles puissent remplir correctement les obligations de la loi grâce à des outils appropriés et compatibles, en particulier du point de vue des coûts.

Une étude réalisée en 2018 sur la base de l'article 20 du GDPR a montré que les responsables du traitement des données et les propriétaires de données ne sont pas certains de l'efficacité de la portabilité, même si les définitions des termes « structuré » et « lisible par machine » existent dans la loi :

> There was little consensus on what is required for full compliance with Article 20. Importantly, although all data controllers indicated that their responses comply with Article 20, it is questionable whether data were always delivered in a "structured, commonly used, machine-readable format".
>
> […]
>
> Our results show problems around portability both for data controllers, who may misunderstand requirements or provide data in inappropriate or incomplete formats, and data subjects, who may be unable to verify their identity or verify the veracity of the data returned by a controller.
>
> […]
>
> In this paper we examined the GDPR's RtDP by making 230 real-world requests. We found a variety of file formats being returned by data controllers, some of which may not comply with the obligations in Article 20, and some confusion between the various rights in the GDPR on the part of data controllers.[63]

Une réglementation appropriée établirait des protocoles et des normes de sécurité à respecter, garantissant que les données d'un individu sont transférées de manière sécurisée, minimisant ainsi le risque de fuites ou d'accès non autorisé.

[63] J. WONG et T. HENDERSON, préc., note 42.

Grâce à une réglementation claire, toutes les entreprises seraient sur un pied d'égalité, ce qui encouragerait l'innovation et empêcherait les pratiques monopolistiques. Elles peuvent également fixer des normes techniques pour garantir une telle interopérabilité.

Des réglementations bien définie apportent clarté et orientation, réduisant les incertitudes juridiques et les litiges potentiels, et peut fixer des limites claires, protégeant les intérêts légitimes et les sensibilités particulières, telles que les secrets commerciaux ou les données sensibles, ainsi que les intérêts de toutes les entreprises.

En résumé, si la portabilité des données est un droit essentiel à l'ère numérique, son efficacité et sa sécurité dépendent d'une réglementation solide et bien pensée. Une telle réglementation assurerait un équilibre entre la promotion de l'autonomie individuelle et la garantie d'un traitement responsable et sûr des données.

De manière non exhaustive, on peut penser aux réglementations qui prévoient l'adoption de systèmes compatibles dans des secteurs identiques ou similaires, la détermination de délais et de sanctions pour l'exécution des demandes d'accès et la portabilité des données (en fonction de la législation régissant le cas spécifique), par exemple.

Jusqu'à ce que les divergences soient résolues, on peut se demander dans quelle mesure la bonne foi qui devrait prévaloir dans les relations entre les responsables du traitement et les personnes concernées conduirait au moins à renverser la charge de la preuve à l'encontre du responsable du traitement, de sorte qu'il lui incomberait de prouver qu'il a pris, dans la mesure du possible, les mesures nécessaires et appropriées pour permettre l'exercice du droit à la portabilité.

3.4 La résolution du problème d'interopérabilité

L'interopérabilité est probablement le plus grand défi de la mise en œuvre de la portabilité, comme Facebook l'a expliqué en 2018 lorsqu'il a lancé le *Data Transfer Project* :

> Moving your data between any two services can be complicated because every service is built differently and uses different types of data that may require unique

> privacy controls and settings. For example, you might use an app where you share photos publicly, a social networking app where you share updates with friends, and a fitness app for tracking your workouts. People increasingly want to be able to move their data among different kinds of services like these, but they expect that the companies that help them do that will also protect their data.[64]

C'est un concept central dans le domaine des technologies de l'information et joue un rôle crucial dans la liaison et la collaboration entre des systèmes hétérogènes. Avec les progrès croissants de la technologie et la prolifération des systèmes d'information, la capacité de partager et d'utiliser les données de manière efficace et efficiente est devenue un besoin pressant. Dans ce contexte, l'interopérabilité des données apparaît comme la solution pour surmonter les obstacles et promouvoir une intégration harmonieuse entre des systèmes disparates. Cet article explore la signification, les défis et les avantages de l'interopérabilité des données, en soulignant son importance dans le paysage universitaire et commercial.

En Europe, la Commission Européenne définit l'interopérabilité comme « La capacité d'organisations disparates et diverses à interagir pour atteindre des objectifs fixés d'un commun accord et offrant des avantages mutuels, impliquant le partage d'informations et de connaissances entre lesdites organisations, par le biais de processus pris en charge par celles-ci, au moyen d'échanges de données entre leurs systèmes respectifs de TIC ».

Elle peut être définie comme la capacité de différents systèmes, applications ou appareils à échanger des informations et à utiliser ces données de manière cohérente et sémantique. Elle va au-delà du simple transfert de données et permet la compréhension mutuelle et l'interprétation correcte des données entre des systèmes hétérogènes. Le manque d'interopérabilité peut entraîner des redondances, des inefficacités et des difficultés à prendre des décisions éclairées.

L'un des principaux défis de l'interopérabilité des données est la disparité des structures et des formats de données. Les systèmes développés indépendamment utilisent souvent des schémas de données différents, ce qui rend difficile la communication entre eux. En outre, les

[64] Steve SATTERFIELD, « Working Together to Give People More Control of Their Data », *Meta* (20 juillet 2018), en ligne : <https://about.fb.com/news/2018/07/data-transfer-project/> (consulté le 2 août 2023).

questions de sémantique et de normalisation constituent également des obstacles importants. Pour relever ces défis, il faut adopter des normes ouvertes et des protocoles de communication partagés qui permettent une représentation et une interprétation cohérentes des données.

L'interopérabilité désigne la mesure dans laquelle l'infrastructure d'une plateforme peut fonctionner avec d'autres. Dans le jargon des logiciels, l'interopérabilité est généralement assurée par des interfaces de programmation d'applications (API) - des interfaces qui permettent à d'autres développeurs d'interagir avec un service logiciel existant.

L'API (*Application Programming Interface*) est la ressource choisie par la Banque centrale du Brésil qui permettra aux institutions de partager des informations dans l'écosystème Open Banking de manière standardisée.

Le format des « données portables » est également un aspect crucial pour l'efficacité et la faisabilité de la portabilité, car l'agent « destinataire » doit être en mesure de les traiter sans compromettre leur qualité et à leur exactitude.

En ce sens, le droit à la portabilité ne sera effectif que s'il existe une structure qui permet ce transfert sécurisé et gratuit de données entre les responsables du traitement, selon le choix de la personne concernée. Ainsi, la réalisation du droit à la portabilité est indissociable d'un système d'interopérabilité :

> Before the legal texts analysis (GDPR and LGPD) to inquire what they provide about interoperability, it is necessary to differentiate the concepts of “interoperable format” and of “interoperability”. Interoperable format would be minimum patterns for ensuring the possibility of data exchange and reuse (EUROPEAN COMMISSION, 2018), as it is the following set: structured format, commonly used and machine-readable (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, p. 17).
>
> An interoperable system or the interoperability, however, are related to the capability of communication, to program execution or to data transfer between distinct functional units, without needing to know exclusive characteristics of each unit (PUCCINELLI, 2017, p. 207). The thematic of an interoperable system is covered through the ISO/IEC 2382–01.[65]

[65] D. C. CRAVO, préc., note 38.

En d'autres termes, il est nécessaire de développer un système intégré dans lequel il y a compatibilité entre l'envoi du « paquet » de données d'une personne physique et la réception de ces données. Il s'agit d'un travail technique et technologique qui doit être développé afin de réaliser le droit à la portabilité.

Le Projet de loi c-27 (LPVPC) prévoit que « *le droit à la mobilité s'applique seulement si les deux organisations sont soumises à un cadre de mobilité des données. Ces cadres seront prévus par règlement (article 120). Les sociétés d'assurances doivent s'assurer de leur interopérabilité pour remplir les obligations qui leur incombent à cet égard* »[66].

Concernant les défis, le premier qui se pose est le besoin d'un système intégré dans lequel il y ait une compatibilité entre l'envoi d'un « paquet » de données d'une personne et la réception de ces données. Voici un travail technique et technologique qui doit être développé pour que le droit à la portabilité soit réalisé[67].

Cet obstacle n'est pas traité dans le texte de loi, il doit donc être traité par voie réglementaire.

Ce n'est pas quelque chose de simple, mais l'un des plus gros obstacles et l'un des risques probables pour la sécurité des données qui font l'objet d'une migration entre banques de stockage :

> One of the challenges with the GDPR's data portability right is that not all data will be seamlessly interoperable from one service provider to another. This could greatly limit the usefulness of the data portability right. It could also impose a significant burden on SMEs who might face demands for the production and transfer of data that they are not sufficiently resourced to meet. It might also place individuals'

[66] Chantal BERNIER, « Projet de loi C-11 édictant la Loi sur la protection de la vie privée des consommateurs – Répercussions principales sur le secteur de l'assurance », en ligne : <https://www.dentons.com/fr-ca/insights/articles/2021/january/8/projet-de-loi-c-11-edictant-la-loi-sur-la-protection-de-la-vie-privee-des-consommateurs> (consulté le 23 mars 2023).

[67] « Portabilité des données | CPA Canada », en ligne : <https://www.cpacanada.ca/fr/interet-public/politiques-publiques-relations-gouvernements/politiques-publiques-representation/gouvernance-donnees/portabilite-donnees> (consulté le 2 août 2023).

> privacy at greater risk, potentially spreading their data to multiple companies, some of which might be ill-equipped to provide the appropriate privacy protection.[68]

Ainsi, des préoccupations concernant la sécurité des opérations de portabilité émergent ; avec la manière correcte de répondre à une demande ; avec le fardeau que la portabilité peut générer pour les petites entreprises ; concernant d'éventuelles normes d'interopérabilité ; avec la protection des secrets commerciaux et industriels ; avec des droits de tiers ; avec des données d'inférence ; entre autres.

Un exemple de cette difficulté à assurer la portabilité a été le processus de mise en œuvre de l'*open banking* au Brésil, qui a été divisé en un an et a eu pour première étape, toujours en 2021, la mise à disposition du public d'informations standardisées des institutions financières participantes, sans il y a partage de données.

Cela a été fait par l'intermédiaire de la Banque centrale du Brésil, qui s'est occupée de l'homogénéisation et est responsable de la réglementation, en plus de la supervision.

Ainsi, l'un des premiers enjeux d'un point de vue réglementaire est de fixer le mode de stockage qui permet la communication entre les bases de données. Le problème, comme l'a dit la professeure Scassa, est que la grande majorité des entreprises ne bénéficient pas du soutien financier et opérationnel des banques.

Mais même dans le système bancaire, à partir du moment où le consommateur ouvre cet univers d'informations gardées confidentielles, il est également soumis à une plus grande probabilité de recevoir des arnaques, car l'univers des personnes à l'intérieur du système bancaire qui prendront connaissance de ses applications et de son compte.

En d'autres termes, même si une institution dispose de moyens de protection adéquats, les données, lorsqu'elles sont migrées vers quelqu'un d'autre, ne bénéficient pas nécessairement de la même protection.

[68] T. SCASSA, préc., note 30.

Un problème de protection de transmission peut être atteint :

> La transmission doit donc s'effectuer de manière à protéger la confidentialité des renseignements. Le choix des moyens quant à la façon d'assurer la protection des renseignements confidentiels lors de la transmission d'un document est laissé à ceux qui en ont la responsabilité. Ceux-ci doivent cependant être en mesure de fournir, au besoin, la documentation expliquant comment les moyens pris permettent d'assurer la protection de la confidentialité. Cette documentation pourra établir, si requis, que la confidentialité a été maintenue lors de la transmission.[69]

Les *fintechs*, par exemple, ont tendance à avoir plus de services *cloud* et ont de nombreuses adresses IP à attaquer, ce qui les rend plus vulnérables.

Dans un cas comme celui-ci, il est difficile de déterminer l'étendue de la responsabilité des gestionnaires de bases de données, une question qui peut être posée est de savoir s'ils encourraient des risques et des responsabilités s'ils transféraient des données à un fournisseur de services avec une protection insuffisante de la vie privée ou de la cybersécurité.

Ce n'est pas parce qu'un responsable de traitement devra transmettre les données à un autre, ce qui peut même aller à l'encontre de ses intérêts économiques, qu'il doit négliger le devoir de protection de ces données.

Le même souci de sécurité des données doit avoir le nouveau responsable du traitement qui les recevra. Il devra également adopter des mesures capables de protéger les données.

L'opération de transmission de données à des fins de portabilité, tout en étant effectuée à la demande du titulaire, doit être effectuée avec le même soin que celui requis pour tout autre traitement :

> Une fois qu'une demande portant sur la mobilité des données est satisfaite, l'organisation qui communique les renseignements doit-elle les détruire ou les anonymiser ? Par exemple, selon l'interprétation de l'article 20(3) du RGPD, l'entreprise qui fait l'objet d'une demande de portabilité des données n'est pas tenue de supprimer ces renseignements. Nous nous attendons à ce qu'il en soit de même en vertu de la législation fédérale proposée : le fait de répondre à une demande en matière de mobilité des données ne devrait pas prévaloir sur le besoin impérieux de l'organisation divulgatrice de conserver les renseignements personnels, par exemple,

[69] V. GAUTRAIS et P. TRUDEL, préc., note 7.

> pour respecter ses obligations contractuelles ou réaliser autrement la finalité pour laquelle les renseignements personnels ont été recueillis. Bien entendu, si cette fin n'est plus pertinente ou si un individu a exercé le nouveau droit prévu par le projet de loi C-11 de demander à l'organisation de retirer ses renseignements personnels, la situation serait alors tout autre.[70]

Au-delà des défis, l'interopérabilité des données offre un certain nombre d'avantages. Elle accroît l'agilité des systèmes, ce qui permet de s'adapter plus rapidement aux nouvelles demandes et aux changements technologiques. Elle améliore également la qualité des données en réduisant les erreurs dues aux doublons ou aux incompatibilités. En outre, l'interopérabilité des données favorise l'innovation, car la collaboration entre différents systèmes peut déboucher sur des idées et des solutions créatives.

Cela soulève une discussion importante liée à la viabilité même de la portabilité car, malgré ses nobles objectifs, son efficacité dépend essentiellement de la résolution du problème de l'interopérabilité entre le responsable du traitement qui enverra les données et la personne concernée ou le nouveau responsable du traitement qui les recevra. C'est pourquoi les lignes directrices sur le droit à la portabilité des données[71] attestent que, sans normes conduisant à l'interopérabilité, le droit à la portabilité est destiné à rester plus une déclaration de principe qu'un instrument réel et efficace d'autodétermination individuelle dans l'environnement numérique.

Par conséquent, le premier défi à relever pour comprendre le droit à la portabilité concerne ses hypothèses techniques. La difficulté de la question tient au fait que le RGPD semble vouloir imposer aux responsables du traitement l'obligation de développer ce que certains spécialistes ont défini comme un module d'exportation-importation, c'est-à-dire un logiciel capable d'exporter des données d'un service et de les importer dans un second service. Toutefois, il ressort clairement du considérant 68 que le droit du titulaire ne crée pas d'obligation pour les

[70] D. FABIANO et J. UZAN-NAULIN, préc., note 56.

[71] *ARTICLE29 - Guidelines on the right to « data portability » (wp242rev.01)*, en ligne : <https://ec.europa.eu/newsroom/article29/items/611233> (consulté le 28 juillet 2023).

responsables du traitement d'adopter ou de maintenir des systèmes de traitement techniquement compatibles.

On ne voit donc pas comment le droit à la portabilité peut être exercé si les deux systèmes - celui qui envoie les données et celui qui les reçoit - ne sont pas compatibles. La difficulté est d'autant plus grande que la multiplicité des données - qui vont des données biométriques aux goûts et aux rythmes cardiaques, entre autres - dont la variation permet de multiples alternatives d'enregistrement et de structuration.

C'est pourquoi les lignes directrices sur le droit à la portabilité des données concluent que les expressions relatives à la manière dont les données devraient être envoyées dans le cadre de l'exercice du droit à la portabilité sont, en fait, de simples spécifications de moyens par rapport auxquels le résultat souhaité est l'interopérabilité. Toutefois, sans savoir ce qui peut réellement être mis à la charge des responsables du traitement, il est difficile de délimiter le champ d'application du droit.

Selon ce principe, les exigences imposées aux responsables du traitement pour répondre aux demandes des personnes concernées doivent être raisonnables et pertinentes, et il y a même des discussions sur le droit du responsable du traitement de s'opposer à la portabilité ou même de facturer la réalisation du droit lorsque la demande implique des mesures qui sont manifestement excessives ou disproportionnées.

En conclusion, l'interopérabilité des données est un concept fondamental dans le monde moderne des technologies de l'information. Elle joue un rôle essentiel dans l'intégration de systèmes hétérogènes, en favorisant l'échange efficace et significatif d'informations. Bien qu'elle présente des défis, tels que la disparité des formats et les problèmes sémantiques, les avantages de l'interopérabilité des données sont considérables. L'adoption de normes ouvertes et la sensibilisation à l'importance de l'interopérabilité sont des étapes cruciales pour garantir une intégration réussie des systèmes et maximiser la valeur des données dans le paysage contemporain.

3.5 L’atténuation des risques

Il se pose une discussion importante liée à la faisabilité de la portabilité elle-même car, malgré ses nobles finalités, son efficacité dépend essentiellement de la résolution du problème d'interopérabilité entre le responsable du traitement qui enverra les données et le propriétaire ou le nouveau responsable du traitement qui les recevra.

Nous savons que « toute entreprise ou organisation, peu import sa taille et son chiffre d’affaires, se doit d’effectuer une analyse des risques qu’elle fait courir à l’information qu’elle détient »[72].

Dans le cas de la portabilité, on parle de partage de données entre deux entreprises différentes, donc cette analyse de risque doit impliquer toutes les personnes impliquées.

L'action de l'organisme de réglementation est nécessaire pour assurer un maintien adéquat de la protection, en évitant une fragilité croissante au cours du processus qui sera adopté pour la migration des données personnelles.

En imaginant le processus de migration entre des entreprises qui utilisent des systèmes et des moyens de stockage différents (contrairement à ce qui se faisait avec l'*open banking* au Brésil par exemple), une grande fragilité peut être présente lors de la modification du logiciel qui permet la communication.

Cela peut se produire soit du côté de l'entreprise qui envoie, soit de celui qui reçoit les données, car leurs mesures de sécurité peuvent ne pas inclure le logiciel source ou final, selon le cas.

Un autre aspect est que le consentement, moteur de la portabilité, doit être préservé comme un droit du consommateur et non comme un instrument de manipulation, où le consommateur sera amené à accorder ce consentement à n'importe quelle entreprise.

[72] Nicolas VERMEYS, *Responsabilité civile et sécurité informationnelle*, Cowansville (Québec), Éditions Yvon Blais, 2010.

Le consentement est toujours lié à la finalité de la collecte des données. À propos du consentement :

> Au départ, le consentement est basé sur la prémisse selon laquelle l'usager est en mesure de « contrôler » les informations le concernant; cette « fameuse » notion de contrôle qui fut déjà le concept clé dans notre analyse sur la qualification des opérations vue dans la partie. Au regard du sacro-saint principe d'autonomie de la volonté, conformément à son étymologie grecque (« auto » pour « soi-même » et « nomos » pour la « loi »), c'est donc par le consentement que l'individu autorise la circulation des renseignements personnels. Ainsi, l'on considère implicitement que la protection passe par l'immobilisation, mais que la circulation des informations peut néanmoins être faite dès lors que la personne y consent; comme si ce dernier acceptait d'être moins bien protégé, ce qui n'apparaît pas tout à fait logique[73].

> Comme nous l'avons évoqué précédemment, le consentement constitue la pierre d'assise du droit à la protection des renseignements personnels, puisque c'est ce mécanisme qui permet aux individus d'exercer un certain contrôle sur ce que les entreprises peuvent faire et ne pas faire avec leurs renseignements[74].

Le maintien du libre consentement est essentiel pour respecter la protection des données. On sait que le consentement est l'un des principes de base de pratiquement toutes les lois qui traitent des données personnelles, que ce soit au Canada ou à l'étranger, et il doit être libre.

Le critère « libre » renvoie à un choix réel du titulaire. L'octroi du consentement doit être un véritable choix, sur lequel le titulaire a le plein contrôle. Si le titulaire n'a pas de véritable choix, se sent obligé de consentir ou subit des conséquences négatives en cas de non-consentement, cela ne sera pas valable.

Lorsqu'on parle de portabilité, le consentement devient une exigence, étant donné qu'il ne s'agit pas simplement de consentir à collecter des données dans un but au sein de l'entreprise ou de l'organisation.

Il s'agit également d'un ordre de la personne concernée de les transmettre à des tiers. Pour ces raisons, le consentement prévu à l'art. 72 de la *Loi sur la protection de la vie privée des*

[73] V. GAUTRAIS et P. TRUDEL, préc., note 7.

[74] Simon DU PERRON, *Droit à la vie privée, mégadonnées et intelligence artificielle: cadre juridique en matière de protection des renseignements personnels*, Montréal, LexisNexis, 2022.

consommateurs (Projet de Loi C-27) doit contenir des exigences spécifiques, afin de protéger le consommateur contre une éventuelle demande d'une autre société de transfert de données d'ouvrir un compte, par exemple.

La portabilité doit être comprise comme un droit qui facilite la vie du consommateur, stimule le commerce et accélère la migration des données personnelles, mais pas comme un devoir du titulaire d'adopter un nouveau service.

Outre ces risques, avec l'ouverture des offres, apparaîtront certainement plusieurs fausses applications se faisant passer pour des institutions et proposant des propositions apparemment extrêmement compétitives qui ne sont rien d'autre que des arnaques.

Nous vous rappelons que la portabilité est un autre moyen de transmettre/communiquer les données des consommateurs.

Bien que ces étapes soient essentielles dans la vie moderne, plus la communication de données est importante, plus les risques sont créés. Les données personnelles seront plus dispersées, déposées dans plus de bases de données et, par conséquent, plus sensibles aux attaques

Avec ces considérations, peut-on conclure que la régulation seule pourra éviter les plus grands risques de sécurité ?

La réponse est que non seulement la mise en œuvre des réglementations, mais aussi une action active par les personnes concernées.

Conclusion

Le droit à la portabilité des données personnelles découle du droit fondamental à l'autodétermination informative, dans la mesure où elle qui suppose que les données appartiennent à son propriétaire, qui a le contrôle, bien que non absolu, de la façon dont ils doivent être utilisés. Et tandis que l'institut renforce l'autonomie de la personne concernée, il sert également comme un important instrument de développement économique et compétitif.

La portabilité à d'importantes implications en matière de concurrence, car, partant du principe que les données sont les intrants les plus importants de l'économie fondée sur les données, la portabilité peut faciliter le transfert de données à des fins d'entrée. de start-ups sur le marché ou encore pour stimuler la concurrence entre concurrents existants, en évitant que l'accumulation de données par un seul ou certains commerçants ne soit une véritable barrière à l'entrée ou un facteur compromettant la rivalité avec des acteurs plus petits.

Outre les conséquences concurrentielles, le droit à la portabilité peut encore générer plusieurs avantages pour le marché, puisqu'il peut également être utilisé pour échanger des données entre des services complémentaires, facilitant ainsi la vie des parties intéressées.

En effet, l'un des éléments pouvant influencer le choix d'une personne concernée entre différents prestataires est précisément la manière dont ses données sont traitées.

Cela signifie que le client ne peut pas être « enfermé » en raison de moyens bureaucratiques, de frais abusifs et de conséquences telles que la perte de données personnelles.

Ainsi, pour une synthèse aisée du fonctionnement de la portabilité des données, quelques points ont été décrits : garantir la liberté et l'autonomie des données au client ; assurez-vous que les données ne sont pas perdues ; s'assurer que, sur demande, le client réutilise ses données.

Néanmoins, il convient également de rappeler qu'il reste encore des normes à stipuler pour l'interopérabilité des données personnelles.

De cette manière, la portabilité des données personnelles sera pleinement établie, garantissant clairement tous les avantages liés à la manipulation des données personnelles d'un individu donné. Cela profitera à la fois aux clients et aux entreprises.

Le droit à la portabilité des données surgit précisément pour faire face à cette situation et apporter des alternatives pour favoriser la concurrence – stimuler l'entrée et réduire les barrières – et protéger les utilisateurs. Sans portabilité, on risquerait d'accorder plusieurs droits aux individus, sans toutefois leur fournir des outils efficaces pour qu'ils recherchent des services qui respectent leurs droits ou qui ont des politiques qui leur conviennent le mieux.

En effet, l'adoption de la portabilité des données dans le cadre du Projet de loi C-11 lie est justifiée, suivant la tendance inaugurée non seulement dans l'Union européenne, mais aussi dans plusieurs autres juridictions. Ce choix apportera sans aucun doute des avantages non seulement aux particuliers, mais également au marché dans son ensemble.

Nous avons également des préoccupations qui émergent en matière de sécurité dans les opérations de portabilité, qui peuvent être, par exemple : avec la bonne façon de répondre à une demande ; avec le fardeau que la portabilité peut générer pour les petites entreprises ; concernant d'éventuelles normes d'interopérabilité ; avec la protection des secrets commerciaux et industriels ; avec des droits de tiers ; avec des données d'inférence ; entre autres.

Bien sûr, avec une réglementation appropriée, il serait beaucoup plus facile d'assurer l'interopérabilité sur la base de critères raisonnables et réalisables, ce qui est particulièrement important pour les petites et moyennes entreprises, pour lesquelles un compromis doit être trouvé afin qu'elles puissent satisfaire de manière adéquate les obligations de la loi à travers des outils appropriés et compatibles, notamment d'un point de vue des coûts.

De plus, les enjeux ne se limitent pas au besoin de régulation, mais incluent également le rôle des opérateurs de données personnelles, les entreprises.

La possibilité de responsabilité des agents impliqués dans la communication des données (expéditeur et destinataire) doit être délimitée, en tenant compte des principes essentiels de la protection des données personnelles.

Références bibliographiques

Législation :

ARTICLE29 - Guidelines on the right to « data portability » (wp242rev.01), en ligne : <https://ec.europa.eu/newsroom/article29/items/611233> (consulté le 28 juillet 2023).

Brésil, Resolução Conjunta n° 1 de 4/5/2020, en ligne : <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=1> (consulté le 1 août 2023).

Brésil, Circular n° 4.015 de 4/5/2020, en ligne : <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=4015> (consulté le 1 août 2023).

CE, Règlement (CE) 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), 2016 JO L1191, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX%3A02016R0679-20160504> (consulté le 10 juillet 2023).

Considérant 39 RGPD | GDPR-Text.com, (14 octobre 2019), en ligne : <https://gdpr-text.com/fr/read/recital-39/> (consulté le 1 août 2023).

Considérant 50 RGPD | GDPR-Text.com, (14 octobre 2019), en ligne : <https://gdpr-text.com/fr/read/recital-50/> (consulté le 1 août 2023).

Considérant 68 RGPD | GDPR-Text.com, (14 octobre 2019), en ligne : <https://gdpr-text.com/fr/read/recital-68/> (consulté le 12 juillet 2023).

LC 2000, c 5 | Loi sur la protection des renseignements personnels et les documents électroniques, en ligne : <https://www.canlii.org/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-

5.html?searchUrlHash=AAAAAQAHTFBSUERFIAAAAAAB&resultIndex=1> (consulté le 11 juillet 2023).

LQ 2021, c 25 | Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, en ligne : <https://www.canlii.org/fr/qc/legis/loisa/lq-2021-c-25/derniere/lq-2021-c-25.html?searchUrlHash=AAAAAQBmTG9pIG1vZGVybmlzYW50IGRlcyBkaXNwb3NpdGlvbnMgbMOpZ2lzbGF0aXZlcyBlbiBtYXRpw6hyZSBkZSBwcm90ZWN0aW9uIGRlcyByZW5zZWlnbmVtZW50cyBwZXJzb25uZWxzAAAAAAE&resultIndex=1> (consulté le 13 juillet 2023).

LRC 1985, c P-21 | Loi sur la protection des renseignements personnels, en ligne : <https://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-p-21/derniere/lrc-1985-c-p-21.html> (consulté le 12 juillet 2023).

« Projet de loi émanant du Gouvernement (Chambre des communes) C-11 (43-2) - Première lecture - Loi de 2020 sur la mise en oeuvre de la Charte du numérique - Parlement du Canada », en ligne : <https://www.parl.ca/DocumentViewer/fr/43-2/projet-loi/C-11/premiere-lecture> (consulté le 15 juillet 2023).

Résumé législatif du 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, en ligne : <https://lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/LegislativeSummaries/432C11E> (consulté le 13 juillet 2023).

RLRQ c A-2.1 | Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, en ligne : <https://www.canlii.org/fr/qc/legis/lois/rlrq-c-a-2.1/derniere/rlrq-c-a-2.1.html?searchUrlHash=AAAAAQBpTG9pIHN1ciBs4oCZYWNjw6hzIGF1eCBkb2N1bWVudHMgZGVzIG9yZ2FuaXNtZXMgcHVibGljcyBldCBzdXIgbGEgcHJvdGVjdGlvbiBkZXMgcmVuc2VpZ25lbWVudHMgcGVyc29ubmVsAAAAAAE&resultIndex=1> (consulté le 11 juillet 2023).

RLRQ c P-39.1 | Loi sur la protection des renseignements personnels dans le secteur privé, en ligne : <https://www.canlii.org/fr/qc/legis/lois/rlrq-c-p-39.1/derniere/rlrq-c-p-39.1.html?searchUrlHash=AAAAAQBLIGxvaSBzdXIgbGEgcHJvdGVjdGlvbiBkZXMgcmVuc2VpZ25lbWVudHMgcGVyc29ubmVscyBkYW5zIGxlIHNlY3RldXIgcHJpdsOpAAAAAAE&resultIndex=1> (consulté le 11 juillet 2023).

VOLLMER, N., *Raison 26 EU règlement général sur la protection des données (EU-RGPD)*, 4 avril 2023, en ligne : <https://www.privacy-regulation.eu/fr/r26.htm> (consulté le 15 juillet 2023).

Jurisprudence :

Gordon c. Canada (Santé), 2008 Cour fédérale , en ligne : <https://canlii.ca/t/28x7l> (consulté le 12 juillet 2023).

Doctrine :

BANDA, C. *Enforcing Data Portability in the Context of EU Competition Law and the GDPR*, SSRN Scholarly Paper, Rochester, NY, 13 septembre 2017.

BERNIER, C., « Projet de loi C-11 édictant la Loi sur la protection de la vie privée des consommateurs – Répercussions principales sur le secteur de l'assurance », en ligne : <https://www.dentons.com/fr-ca/insights/articles/2021/january/8/projet-de-loi-c-11-edictant-la-loi-sur-la-protection-de-la-vie-privee-des-consommateurs> (consulté le 23 mars 2023).

CANADA, C. à la protection de la vie privée du, « Troisième principe relatif à l'équité dans le traitement de l'information de la LPRPDE – Consentement » (8 janvier 2018), 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/p_principle/principles/p_consentement/> (consulté le 1 août 2023).

———. *Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la Loi de 2020 sur la mise en œuvre de la Charte du numérique*, 11 mai 2021.

CRAVO, D. C., « The Right of Data Portability in EU's GDPR and Brazil's LGPD », (2022) 50-1 *Revista da Faculdade de Direito da Universidade Federal de Uberlândia* 89-121, DOI : 10.14393/RFADIR-50.1.2022.62778.89-121.

DU PERRON, S., *Droit à la vie privée, mégadonnées et intelligence artificielle: cadre juridique en matière de protection des renseignements personnels*, Montréal, LexisNexis, 2022.

———. « Projet de loi 64 : une réforme à l'Européenne du droit à la protection des renseignements personnels », *Laboratoire de cyberjustice*, en ligne : <https://www.cyberjustice.ca/2020/06/17/projet-de-loi-64-une-reforme-a-leuropeenne-du-droit-a-la-protection-des-renseignements-personnels/> (consulté le 1 août 2023).

EVANS, M., « The data-informed marketing model and its social responsibility », dans *The data-informed marketing model and its social responsibility*, Policy Press, 2005, p. 99-132, DOI : 10.56687/9781847421272-006.

FIDALGO, V. P., « O direito à portabilidade de dados pessoais »,, en ligne : <https://blook.pt/PHfS> (consulté le 15 juillet 2023).

FABIANO, D. et J. UZAN-NAULIN, « Projet de loi C-11 – Mobilité des données : un pas supplémentaire vers le RGPD » (15 décembre 2020), en ligne : <https://www.fasken.com/fr/knowledge/2020/12/15-bill-c-11-data-mobility-another-step-towards-the-gdpr> (consulté le 23 mars 2023).

GANCK, A. D., « The New European Interoperability Framework », *ISA^2 - European Commission* (16 février 2017), en ligne : <http://webserver:8080/isa2/eif_en> (consulté le 28 juillet 2023).

GAUTRAIS, V., « Rapport auprès de la Commission d'accès à l'information (CAI) », *Vincent Gautrais*, en ligne : <https://www.gautrais.com/blogue/2015/12/04/rapport-aupres-de-la-commission-dacces-a-linformation/> (consulté le 12 juillet 2023).

GAUTRAIS, V. et P. TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010, en ligne : <https://www.lccjti.ca/doctrine/gautrais-v-et-trudel-p-circulation-des-renseignements-personnels-et-web-2-0/#ancre1221>.

GOLA, R., « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », (2017) 59-2 *LEGICOM* 29-38, DOI : 10.3917/legi.059.0029.

GRAEF, I. *The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation*, SSRN Scholarly Paper, Rochester, NY, 26 novembre 2020.

GRAEF, I., J. VERSCHAKELEN et P. VALCKE. *Putting the Right to Data Portability into a Competition Law Perspective*, SSRN Scholarly Paper, Rochester, NY, 2013.

GRATTON, É., E. HENRY, F. JOLI-COEUR, S. DU PERRON, M. JARVIE, J. M. GAUTHIER, A. NAGY, D.-N. EL KHOURY, A. HÉMOND et Ca. LABASI-SAMMARTINO. *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*.

GRATTON, É., E. HENRY, F. JOLI-COEUR, M. JARVIE, D. J. MICHALUK, K. M. STRANGER, A. NAGY et I. PARGHI, « Loi sur la protection de la vie privée des consommateurs du Canada (projet de loi C-27) : incidences sur les entreprises », *BLG*, en ligne : <https://www.blg.com/fr/insights/2020/11/canadas-consumer-privacy-protection-act-impact-for-businesses> (consulté le 23 mars 2023).

GRATTON, E., *Redefining personal information in the context of the Internet*, 2013 Accepted: 2017-12-05T15:28:32Z, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/19676> (consulté le 5 juillet 2023).

MONIZ, G. C., *Anuário da Proteção de Dados: 2018*, Lisboa, Faculdade de Direito, Universidade Nova de Lisboa, 2018.

SALVAS, B., *La protection de la vie privée sur le Web avec P3P : l'arrimage incertain du technique et du juridique | CanLII*, 2001, en ligne : <https://www.canlii.org/fr/doctrine/doc/2003CanLIIDocs491?zoupio-debug#!fragment//(hash:(chunk:(anchorText:''),notesQuery:'',scrollChunk:!n,searchQuery:/13226-current-1,searchSortBy:RELEVANCE,tab:toc))> (consulté le 12 juillet 2023).

SOLOVE, D. J., *The Digital Person: Technology and Privacy in the Information Age*, Rochester, NY, 2004, en ligne : <https://papers.ssrn.com/abstract=2899131> (consulté le 10 juillet 2023).

VERMEYS, N., *Responsabilité civile et sécurité informationnelle*, Cowansville (Québec), Éditions Yvon Blais, 2010.

SATTERFIELD, S., « Working Together to Give People More Control of Their Data », *Meta* (20 juillet 2018), en ligne : <https://about.fb.com/news/2018/07/data-transfer-project/> (consulté le 2 août 2023).

SCASSA, T., « Data Mobility (Portability) in Canada's Bill C-11 », en ligne : <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=338:data-mobility-portability-in-canadas-bill-c-11&Itemid=80> (consulté le 23 mars 2023).

SWIRE, P., « The Portability and Other Required Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations », 2022, DOI : 10.2139/ssrn.3689171.

WITZLEB, N. et J. WAGNER, « When is Personal Data "About" or "Relating to" an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws », (2018) 4-1 *Canadian Journal of Comparative and Contemporary Law* 293.

WONG, J. et T. HENDERSON, « How Portable is Portable? Exercising the GDPR's Right to Data Portability », dans *Proceedings of the 2018 ACM International Joint Conference and 2018*

International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers, coll. UbiComp '18, New York, NY, USA, Association for Computing Machinery, 2018, p. 911-920, DOI : 10.1145/3267305.3274152.

ZOLYNSKI, C. et M. LE ROY, « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », (2017) 59-2 *LEGICOM* 105-113, DOI : 10.3917/legi.059.0105.

« 1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board », en ligne : <https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_fr> (consulté le 2 août 2023).

« À quoi correspondent les données à caractère personnel? », en ligne : <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_fr> (consulté le 11 juillet 2023).

« Data Transfer Initiative », en ligne : <https://dtinit.org/> (consulté le 2 août 2023).

« Portabilité des données | CPA Canada », en ligne : <https://www.cpacanada.ca/fr/interet-public/politiques-publiques-relations-gouvernements/politiques-publiques-representation/gouvernance-donnees/portabilite-donnees> (consulté le 2 août 2023).

« Présentation des concepts-clés liés aux renseignements personnels », *Gouvernement du Québec*, en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/concepts> (consulté le 17 juillet 2023).

« With Profile Transfer, Keep Your Netflix Experience a Constant Even in Times of Change », *About Netflix*, en ligne : <https://about.netflix.com/en/news/profile-transfer-keeps-netflix-experience-constant> (consulté le 13 juillet 2023).