La protection des données personnelles comparée entre la Suisse et le Québec.

Philippe BONVIN*, Novembre 2024

Les lois sur la protection des données personnelles ont été récemment actualisées en Suisse et au Québec à la suite de l'introduction du Règlement Général sur la Protection des Données (RGPD) dans l'Union européenne. Dans ce contexte, il est intéressant de comparer la perception différente de notion de protection de données personnelles dans ces deux systèmes juridiques, d'autant plus que le Québec vit dans un système hybride de *common law* du Canada et de droit romano-civiliste.

Cet article discute de la protection des données à caractère personnel en tant que droit fondamental puis aborde la question de la définition de donnée personnelle ; il montre les différences des personnes et organismes soumis à des obligations légales de protection ; il met également en lumière les différentes normes et dispositions requises pour assurer une saine gestion des systèmes de traitement et une protection adéquate des données personnelles ainsi qu'exposent les outils juridiques mis à disposition pour assurer l'application des dispositions précitées. L'influence du RGPD sur les législations suisses et québécoises est également discutée.

Mots-clés : Protection des données personnelles – LPD Suisse – Loi 25 Québec – RGPD Union Européenne – LPRPDE Canada

Table des matières

Table des abréviations

al.	Alinéa
aLPD	LF du 19 juin 1992 sur la protection des données
art.	article(s)
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
CC	Code civil Suisse du 10 décembre 1907 (RO 24 245)
ch.	Chapitre
CAD	Dollar canadien
CAI	Commission d'accès à l'information
C.c.Q.	Code civil du Québec
CEDH	Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (RS 0.101)
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
consid.	Considérant
CPC	Code de procédure civile du 19 décembre 2008 (RS 272)
CSC	Cour Suprême du Canada
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS 101)
DPO	Data Protection Officer
€	Euros
éd.	Édition
édit.	éditeur(s)
etc.	et cætera
FF	Feuille fédérale
HIPPA	Health Insurance Portability and Accountability Act
ISO	International Organization for Standardization
LCDP	Loi canadienne sur les droits de la personne (L.R.C. (1985), ch. H-6)
LCPRP	Loi sur la protection des renseignements personnels (L.R.C. (1985), ch. P-21)
LF	Loi fédérale
LPrD	Loi [vaudoise] sur la protection des données personnelles
LPRPDE	Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch. 5)
LPRPSP	Loi sur la protection des renseignements personnels dans le secteur privé (ch. P-39.1)
LRens	LF du 25 septembre 2015 sur le renseignement (RS 121)
LTF	Loi du 17 juin 2005 sur le Tribunal fédéral (RS 173.110)
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
LSCPT	LF du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (RS 780.1)
n$^{o(s)}$	numéro(s)
NIST	National Institute of Standards and Technology
nLPD	LF du 25 septembre 2020 sur la protection des données (RS 235.1)
p.	page(s)
pp.	Pages
par.	Paragraphe
RGPD	Règlement général sur la protection des données (Règlement (UE) 2016/679)

RS	Recueil systématique du droit fédéral
RLRQ	Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
SP	NIST Special Publication
ss	suivant(e)s
SCR	Canada Supreme Court Reports
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral suisse
trad.	Traduction
UE	Union Européenne

I. Introduction

Les récentes avancées technologiques permettant le traitement automatisé et de masse d'informations ont poussé les législateurs à renforcer ces dernières années le principe de protection des données personnelles dans le secteur privé. Le *Règlement général sur la protection des données* (RGPD) au sein de l'Union Européenne a été le premier règlement dit de deuxième génération en 2018, suivi par l'introduction simultanée en 2023 de la révision de la *Loi sur la protection des données* (nLPD) en Suisse et de la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi 25) au Québec. Le Canada n'a pas récemment introduit de révision de sa *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) mais y travaille dans ses *Projet de loi C-11* et *Projet de loi C-27*.

La comparaison de ces législations permet de mettre en lumière les approches différentes des législateurs dans des États fédéraux tels que le Canada et la Suisse ainsi que les différences de perception culturelle de la notion du droit à la vie privée. En effet, il est difficile d'aborder le sujet de la protection des renseignements personnels sans analyser la notion du droit à la vie privée étant donné que l'un découle de l'autre. La définition de la notion de « vie privée » est exprimée de différentes manières dans la *Charte des droits et libertés de la personne* [du Québec] (Charte québécoise) à l'art. 5 et dans le *Code civil du Québec* (C.c.Q) aux art. 35 et 36, dans la *Charte canadienne des droits et libertés* (Charte canadienne) aux art. 8 et subsidiairement 7, dans la *Constitution fédérale de la Confédération suisse* (Cst) à l'art. 13 et dans la *Convention européenne des droits de l'Homme* (CEDH) à l'art. 8. En illustration de la différence de l'importance portée à ce droit, le droit à la vie privée est très clairement exprimé dans la CEDH et à l'inverse beaucoup plus flou dans la *Charte canadienne*. La *Cour Suprême du Canada* (CSC) a déduit dans plusieurs arrêts[1] des articles de la *Charte canadienne* susmentionnés un droit de protection « des renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels »[2] et encore en 2024, a dû préciser qu'il existe une « *attente raisonnable au respect de la vie privée en droit canadien »*[3].

Le Québec fonctionne dans un système particulier dit bi-juridique, de droit civil pour le droit privé provincial et de *common law* pour le droit public tant provincial que fédéral et pénal fédéral. Cette particularité influence la manière dont les tribunaux vont interpréter les situations et rendre des décisions car même en droit civil, les méthodes de *common law* sont considérées[4]. Faire figurer le droit au respect de la vie privée dans la *Charte québécoise* lui accorde une protection dite quasi-constitutionnelle, qu'il n'est pas possible d'y déroger[5].

Au Canada particulièrement, le principe de la protection des données personnelles est fortement couplé avec le principe du droit d'accès à l'information détenue par l'administration publique[6]. Ce principe a été créé à la suite de l'introduction du traitement informatisé des renseignements personnels par l'État canadien. La philosophie de l'époque était de se protéger du gouvernement plus que des entreprises privées, principe maintenant renversé[7]. Par conséquent, le gouvernement canadien a commencé par légiférer dans le secteur public avec la *Loi canadienne*

[1] R. c. Tessling, [2004] 3 R.C.S. 432, 2004 CSC 67 et R. c. Plant, [1993] 3 R.C.S. 281, 2004 CSC 67, R. v. Spencer, 2014 CSC 43 (CanLII), [2014] 2 SCR 212, et encore R. c. Bykovets, 2024 CSC 6 notamment
[2] R. c. Plant, note 2
[3] R. c. Bykovets, 2024 CSC 6
[4] GERVAIS, SÉGUIN
[5] DU PERRON, par. 3-2
[6] COMEAU, p. 10
[7] MOYSE, p. 24

sur les droits de la personne (LCDP) en 1977 puis avec la *Loi sur la protection des renseignements personnels* (LCPRP) introduite en 1982. Le secteur privé n'étant pas concerné par ces lois, la LPRPDE qui règlemente le secteur privé arrivera seulement en l'an 2000. Le Québec a suivi avec la création de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ) en 1982. En Suisse, le principe de la transparence dans l'administration publique fédérale est apparu après le principe de protection des renseignements personnels avec la création de la *Loi fédérale sur le principe de la transparence dans l'administration* (LTrans) en 2004. Par ailleurs, *le Message relatif à la loi fédérale sur la transparence de l'administration* (Message LTrans) mentionne explicitement le Canada comme exemple de base de législation et y cite la liaison entre le principe de protection des données et le principe du droit d'accès à l'information en droit canadien. On remarque d'emblée que ces deux concepts ne sont pas mis en rapport en droit Suisse, contrairement au droit canadien.

L'Union Européenne a introduit la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (Convention 108) en 1981, que la Suisse a ratifié en 1998 et complété par un protocole additionnel (le STE 181) en 2008. Cette convention pose les bases de la protection des données personnelles en Europe et a été modernisée en 2018 (la Convention 108+) que la Suisse a ratifiée en 2023 à la suite de l'introduction de la nLPD. Bien que la Convention 108 étant ouverte aux États tiers, le Canada n'en n'est pas signataire. Toutefois, toutes ces lois sont fondées sur les principes relatifs à l'équité dans le traitement de l'information[8] énoncés par l'OCDE dans ses *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel* (Lignes directrices OCDE) datant de 1980. La Suisse introduit la *Loi fédérale sur la protection des données* (aLPD) en 1992, tandis que le Québec se dote de la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP) en 1994, l'UE emboîte le pas avec l'introduction de la directive 95/46/CE en 1995. Toutes ces lois sont dites de première génération.

La plupart des législations sur la protection des données personnelles dans le secteur privé ayant été introduites il y a plus de 30 ans, il était nécessaire de faire une révision profonde de ces principes. Il convient également de se doter d'un cadre législatif permettant d'assurer la protection de la vie privée tenant compte de l'évolution notre société, de l'augmentation fulgurante de la quantité de données qui sont traitées et des technologies actuelles, le tout en restant technologiquement neutre. Le Conseil Fédéral l'a ainsi bien relevé dans son *Message nLPD*, l'Assemblée nationale du Québec dans son *Journal des débats* ainsi que le Conseil de l'Europe dans son *Rapport 223*. À la lecture des différents débats, rapports et autres considérations émis lors de la révision de ces lois, on comprend que les législateurs ont fait face à d'importants défis pour s'assurer que ces lois restent pertinentes et permettent d'assurer les principes fondamentaux du respect de la vie privée malgré les avancées technologiques rapides.

La synchronicité de l'introduction de ces lois dénote une prise de conscience sociétale sur les menaces grandissantes du droit à la vie privée dans le secteur privé. L'actualisation de ces lois, en revanche, pourrait être discutée sous un autre angle. En effet, le RGPD a été la première révision de ces lois et non pas des moindres car il apporte notamment une dimension extraterritoriale aux mesures de protection visées. L'UE étant le premier partenaire commercial de la Suisse[9] et deuxième partenaire commercial du Québec[10], il était absolument nécessaire

[8] DU PERRON, par. 3-5
[9] Exportations de la Suisse par partenaire commercial
[10] Le commerce extérieur du Québec, p. 38

pour ces législations[11] de continuer à être considérées comme étant reconnues comme offrant une protection adéquate des données[12] par la Commission européenne pour assurer la continuité des échanges commerciaux. Une tentative de révision de la LPRPDE en 2021, sous le nom de *Projet de loi C-11* pour moderniser la législation canadienne en la matière est malheureusement mort-née[13].

C'est pourquoi il est intéressant d'observer comment le Québec et la Suisse ont adapté leurs législations à la suite de l'introduction du RGPD. Il sera également possible d'illustrer par des exemples d'arrêts l'interprétation que les tribunaux de ces différentes juridictions en font en droit privé. Du fait de la nature du droit canadien, il faut de naviguer entre les différentes lois publiques et privées, canadiennes et québécoises pour bien cerner le sujet. Au vu des différents systèmes juridiques en vigueur au Québec, nous nous limiterons uniquement aux éléments de droit privé afin de rester dans une interprétation civiliste de la loi. Ceci exclut d'emblée les organismes publics, étant donné qu'ils sont réglementés par la RLRQ et non pas par la Loi 25. Nous serons également obligés d'illustrer les positions des différents tribunaux avec des jurisprudences prédatant les dernières révisions des lois sur la protection des données personnelles par manque de décisions récentes. Celles-ci posent souvent des principes qui sont encore aujourd'hui valables et cités par la doctrine.

II. Principes généraux des lois sur la protection des données personnelles

A. Dans l'Union Européenne – RGPD

Le RGPD est considéré comme précurseur dans le domaine de la protection des renseignements personnels. C'est la loi qui a servi d'exemple pour établir notamment la nLPD et la Loi 25, les législateurs s'en étant largement inspirés[14]. C'est également la loi la plus connue du grand public car son introduction en 2018 a suscité beaucoup de discussions, mais n'est pas la seule en vigueur dans l'UE. On l'a vu, la Convention 108+ traite également de la protection des renseignements personnels, tout comme la directive 2016/680 aborde cette question dans l'espace Schengen et vient compléter et préciser le RGPD. La Convention 108+ adresse le droit d'accès aux documents officiels dans son préambule, ainsi pour l'UE également, cette notion est proche de la protection des renseignements personnels. Le RGPD a des effets extraterritoriaux étant donné qu'il s'applique à toutes les personnes sur le territoire de l'UE, indépendamment du lieu de traitement[15].

Le *Contrôleur européen de la protection des données* (CEPD) ne traite que les demandes relatives aux instances de l'UE. Il veille également à la bonne application du RGPD et conseille les autorités nationales de vérification (art. 68 et ss RGPD), chargées d'être le point de contact national pour les questions relatives à la protection des renseignements personnels.

Les États membres de l'UE établissent librement une autorité nationale de vérification. Par exemple pour la France, la *Commission nationale de l'informatique et des libertés* (CNIL) prend ce rôle. Celui-ci est délimité à la protection des données personnelles, le droit d'accès à l'information étant traité en France par une autre autorité, la *Commission d'accès aux documents administratifs*.

[11] Message nLPD
[12] Art. 45 al. 3, RGPD
[13] DU PERRON, par. 0-10
[14] Message nLPD et Journal des débats
[15] Art. 3 RGPD et Lignes directrices 3/2018

Le choix d'un règlement directement applicable sans transposition nationale dans les lois des différents États membres de l'UE permet de simplifier et d'unifier les protections offertes et le cadre à suivre. Ceci est une grande avancée car précédemment, chaque pays avait sa loi dérivée de la directive 95/46/CE.

B. En Suisse – LPD

En Suisse, une seule loi couvre tous les domaines de la protection des renseignements personnels, la nLPD. Avant son introduction en 1992, les renseignements personnels étaient considérés comme faisant partie de la sphère privée[16] et bénéficiaient donc déjà d'une certaine protection par l'art. 28 al. 1 CC et par l'art. 13 al. 2 Cst.

La aLPD faisait déjà la différenciation entre le secteur et privé et le secteur public, tout comme le Canada. Elle régulait également la communication de renseignements personnels hors de la Suisse[17]. La Suisse n'a pas mis en place de loi spécifique pour le traitement des données médicales, celles-ci étant couvertes par la LPD.

Une différence notable entre la aLPD et la nLPD est que la notion de données personnelles d'une personne morale n'existe plus[18]. Celles-ci peuvent toutefois toujours se reposer sur l'art. 28 CC pour invoquer une atteinte illicite à leur personnalité.

Tout traitement de données personnelles est considéré comme une atteinte présumée illicite[19], à charge du responsable du traitement de démontrer un motif justificatif prévu à l'art. 31 nLPD. Subsidiairement à la nLPD, un particulier pourra toujours recourir à l'art. 28 CC.

La question de l'application de la aLPD au regard du principe de territorialité a été discuté maintes fois par le TF. L'approche prépondérante est que la LPD s'applique aux faits se déroulant sur le territoire Suisse, indépendamment du domicile ou de la nationalité de la personne concernée[20]. Toutefois, le TF a reconnu[21] une dimension extraterritoriale limitée à l'application de la LPD et ce pour des faits se produisant à l'étranger pour autant qu'ils aient suffisamment d'effets en Suisse. Ceci a maintenant été codifié à l'art. 3 al. 1 nLPD d'une manière telle que certains auteurs y voient une application plus large même que le RGPD[22].

Le rôle de contrôleur de l'application de la LPD est donné au *Préposé fédéral à la protection des données et à la transparence* (PFPDT) à l'art. 4 nLPD. Celui-ci ne peut notamment pas prononcer de sanctions administratives[23] et est également en charge des questions du droit d'accès à l'information basées sur la LTrans.

Les cantons ne peuvent pas agir comme le Québec et remplacer la nLPD par leur propre loi, mais ils peuvent la compléter. Par exemple, le canton de Vaud l'a fait avec sa *Loi sur la protection des données personnelles* (LPrD) dans le domaine administratif.

---

[16] BENHAMOU, COTTIER, par. 1, p. 12
[17] Message aLPD et Consultations projet de loi 64
[18] BENHAMOU, COTTIER, par. 2, p. 13
[19] *Idem*, par. 6, p. 19
[20] *Idem*, par. 6, p. 40
[21] ATF 138 II 346, JdT 2013 I 71, consid. 3.3
[22] BENHAMOU, COTTIER, par. 16, p. 41
[23] Message nLPD

C. Au Canada – LPRPDE

Le principe de protection de la vie privée au Canada est décrit comme étant subjectif et objectif par la jurisprudence. Elle est séparée en trois catégories : la vie privée physique, la vie privée territoriale et la vie privée informationnelle[24]. C'est cette dernière qui est visée par le principe de protection des renseignements personnels.

Au Canada, la notion du droit d'accès à l'information est fortement couplée avec la notion de protection des renseignements personnels. En effet, ces deux thématiques sont souvent mises en commun, comme le montre le rôle du *Commissariat* au niveau fédéral et de la *Commission d'accès à l'information* (CAI) au niveau provincial au Québec.

De plus, le Canada a introduit une différenciation entre le traitement des données personnelles par les institutions publiques (droit administratif) et par les entités privées (droit civil), lesquelles sont régies par des lois différentes. Dans les deux cas, le *Commissariat à la protection de la vie privée du Canada* (Commissaire) est chargé de mener des enquêtes, des vérifications et publie sur les meilleures pratiques de traitement des renseignements personnels[25]. Il publie un rapport annuel[26] pour le gouvernement canadien sur ses prises de décision et de position mais ne remplace toutefois pas la Cour en cas de litige.

La manière dont le système juridique du Canada est conçu permet aux provinces de légiférer sur certains sujets, notamment en matière sur la protection des renseignements personnels. Dans un tel cas, la *LPRPDE* ne s'applique que de manière subsidiaire. Le Québec l'a fait récemment avec la Loi 25 et l'Alberta l'avait également tenté avec sa *Personal Information Protection Act*, invalidée par la CSC en 2013[27].

Certaines provinces canadiennes ont promulgué des lois spécifiques sur la protection des renseignements personnels dans le domaine de la santé. Le principe de traiter les données médicales dans une autre loi est probablement tiré du modèle américain, comme l'ont fait les Etats-Unis dans la loi fédérale HIPPA introduite en 1996. Suivant cette logique, le Québec a fait entrer en vigueur la *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*[28] au 1er juillet 2024.

Selon une interprétation littérale de la loi, la LPRPDE ne s'applique qu'au Canada. À cet effet, une entreprise peut simplement élire un for juridique en dehors du Canada tout en offrant des services au Canada, évitant ainsi l'application de la LPRPDE. Bien que l'interprétation soit correcte, la CSC a déterminé qu'il existe un intérêt prépondérant à écarter une telle clause d'élection de for car les *consommateurs* (définition en droit canadien d'un particulier acceptant un contrat générique avec une société sans droit de négociation individuel[29]) doivent pouvoir contester des droits considérés comme « quasi constitutionnels »[30], tel que la protection des renseignements personnels. Ainsi la LPRPDE peut avoir (mais n'a pas systématiquement) des effets à l'étranger pour autant que cela concerne un *consommateur* canadien.

---

[24] BENYEKHLEF, DÉZIEL, p. 151
[25] Art. 11 LPRPDE
[26] Rapport du Commissariat 2023-2024
[27] Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401, 2013 CSC 62
[28] Loi sur les renseignements de santé et de services sociaux
[29] Loi sur la protection du consommateur
[30] Douez c Facebook, Inc, 2017 CSC 33, CSC

D. Au Québec - Loi 25

Au Québec, la loi fédérale LPRPDE ne s'applique pas car elle est remplacée par la Loi 25. Le *Code civil du Québec* (C.c.Q.) pose les principes généraux de la protection de la vie privée aux articles 35 à 41, que la Loi 25 vient compléter et préciser.

Ainsi, lorsqu'il y a des parties interprovinciales ou internationales en sus du Québec, le C.c.Q et la Loi 25 ne peuvent pas être appliqués et la LPRPDE prévaut. L'absence de portée extraterritoriale de la Loi 25[31] affaiblit considérablement les effets de cette loi, même à l'intérieur du Québec. Ainsi, les entreprises de compétence fédérale[32], notamment les banques, les entreprises de télécommunication, les médias (radiodiffusion, télédiffusion), le service postal, les entreprises de transport (par route, ferroviaire, aérien ou par eau) ne sont pas soumises à la Loi 25 et sont de-facto soumis à la LPRPDE bien qu'elles aient des établissements au Québec. Une entreprise ayant des clients au Québec mais qui n'a ni place d'affaires ni employés au Québec n'est également pas soumise à la Loi 25[33]. Certains organismes privés à but non lucratifs n'exerçant pas une activité économique organisée en sont également exemptés[34], tel que le Conseil de presse du Québec[35] ou l'Association des courtiers et agents immobiliers du Québec[36] par exemple. La fuite massive de données de la banque québécoise Desjardins en 2019[37] a influencé le contenu de la Loi 25, les débats parlementaires en sont la preuve[38]. Toutefois étant une banque, cette institution n'est tout de même pas soumise à la Loi 25.

Les personnes morales n'ont pas droit à la protection de leurs renseignements personnels selon Loi 25 et elles ne peuvent pas non plus se substituer pour leurs employés[39].

Le Québec s'est doté de la *Commission d'accès à l'information* (CAI) qui traite les sujets de demande d'accès à l'information ainsi que de protection des renseignements personnels tant dans le domaine public que privé. La CAI a le rôle de tribunal administratif pour trancher les litiges dans ces domaines[40]. Elle joue également un rôle de surveillance[41] de l'application de la Loi 25 et édite divers règlements notamment sur l'anonymisation des renseignements personnels[42] et les incidents de confidentialité[43].

On constate donc déjà une différence notable entre l'organisation de l'appareil gouvernemental québécois et celui du Canada étant donné que la CAI a un pouvoir judiciaire que le Commissaire ne possède pas.

La Loi 25 détermine le responsable du traitement et donc de la protection des renseignements personnels comme étant « toute personne qui exploite une entreprise ». Ainsi, la responsabilité tombe directement sur une personne physique, passant outre la personne morale, donnant plus

[31] GRANOSIK, GRENIER, SAMSON, par. 1/45 et 1/46, p. 14
[32] Code canadien du travail, parties I, II, III et IV
[33] *X. c. Kroll Background America (Canada),* n° 04 12 88, 16 septembre 2005, H. Grenier.
[34] GRANOSIK, GRENIER, SAMSON, par. 1/19 et 1/20, p. 7
[35] *Conseil de presse du Québec c. Lamoureux-Gaboury*, 2004, AIE-54, EYB 2004-121640, CSC.
[36] *Tannenbaum c. Association des courtiers et agents immobiliers du Québec*, 2004AIE-57, CAI.
[37] Enquête Desjardins
[38] Journal des débats
[39] GRANOSIK, GRENIER, SAMSON, par. 2/75, p. 40
[40] Art. 134 al. 2 RLRQ
[41] Art. 122 al. 1 RLRQ
[42] Décret 783-2024, p. 2847ss
[43] Règlement sur les incidents de confidentialité

d'incitatifs à respecter cette loi. Par ailleurs, du fait de cette définition, sont exclus les organismes à but non lucratif et les personnes physiques traitant des renseignements personnels.

III. Mises en œuvre comparées de protection des données personnelles

A. Notion de donnée personnelle et de donnée sensible

Les données personnelles sont une catégorie particulière des actifs informationnels[44]. Afin qu'une information soit considérée comme personnelle, il faut qu'elle permette d'identifier une personne physique en particulier, directement ou indirectement[45]. Ceci inclut la corrélation d'informations et des moyens raisonnablement susceptibles d'être utilisés pour réidentifier une personne [46].

Un des angles qui doit être considéré est la propriété de ces informations personnelles. Le droit des biens matériels est très développé et explicité dans les différentes lois, mais la notion de bien meuble incorporel l'est beaucoup moins en ce qui a trait aux données. C'est pourquoi certains auteurs défendent que les renseignements personnels doivent être considérés comme un bien informationnel[47], leur conférant ainsi un propriétaire et celui-ci aurait donc des droits à leurs égards. Cette question est d'autant plus pertinente que la CSC a rendu en 1988 dans l'affaire *R. c. Stewart*[48] un arrêt dans lequel elle considère que les données ne sont pas des biens et que par conséquent, elles ne peuvent pas être volées[49]. D'autres auteurs considèrent que pour considérer un renseignement comme un bien et donc ayant une valeur, la confidentialité de ceux-ci est une condition *sine qua none*[50] pour leur assigner une valeur. Ainsi, un renseignement n'ayant aucune valeur ne serait pas un bien, n'appartiendrait à personne et ne serait pas digne de protection. De notre avis, cette interprétation est quelque peu simpliste car un renseignement isolé peut être anodin mais s'il est corrélé à d'autres renseignements tout aussi insignifiants, des informations d'une grande valeur peuvent en être déduites.

Afin d'illustrer cette problématique, toutes les instances comparées ont dû traiter de la question suivante : est-ce qu'une adresse IP (adresse d'un ordinateur sur Internet) est considérée comme une donnée personnelle ? Le Canada l'a affirmé en 2024*[51],* la CJUE en a fait de même en 2011 et en 2016[52] et le TF l'avait fait en 2010[53]. On constate donc un consensus sur cette question, quelle que soit la juridiction. Cette position est d'autant plus intéressante qu'une adresse IP peut en soit être considérée comme une donnée « banale » mais, corrélée à d'autres informations, elle permet une réidentification d'une personne ou d'un groupe de personnes et doit donc être considérée comme un renseignement personnel[54].

Les données sensibles doivent faire l'objet de mesures particulières de protection dans toutes les juridictions. Le RGPD à l'art. 9 interdit, sauf exceptions, le traitement de données sensibles.

---

[44] DU PERRON, par. 1-25
[45] *Idem*, par. 2-76
[46] BENHAMOU, COTTIER, par. 12, p. 57
[47] DU PERRON, par. 2-12
[48] *R. c. Stewart ,*1988, 1 RCS 963
[49] DU PERRON, par. 2-20
[50] *Idem*, par. 2-68
[51] R. c. Bykovets, 2024 CSC 6
[52] Sté Scarlet Extended c/ Société belge des auteurs, compositeurs et éditeur SCRL, affaire C-70/10, § 51, CJUE, 24 nov. 2011 et Patrick Breyer contre Bundesrepublik Deutschland, affaire C-582/14, CJUE, 19 octobre 2016
[53] ATF 136 II 508, 1C_285/2009 du 8 septembre 2010
[54] DU PERRON, par. 2-78

Celles-ci sont définies au même article. L'art. 12 de la Loi 25 reprend les mêmes définitions sans être aussi exhaustif. Une définition large est donnée : selon la nature de l'information par exemple : information médicale, biométrique, intime ou selon le contexte de son utilisation ou de sa communication. La CAI complète la liste en ajoutant les dimensions raciales, les croyances, les informations financières ainsi que les identifiants uniques[55] par exemple. L'art. 5 let. c nLPD reprend ces mêmes principes sans toutefois les clarifier explicitement.

Les renseignements personnels peuvent être pseudo-anonymisés, c'est-à-dire qu'il existe une table de correspondance qui peut être utilisée pour réidentifier les données pseudo-anonymisées. Il existe donc dans un tel cas un risque de réidentification. En Suisse, la question de savoir si des données pseudo-anonymisées doivent être considérées et protégées comme des données personnelles était soumise à débat. Les deux écoles sont les suivantes : selon l'approche absolue, tant qu'il existe une table de correspondance quelque part, même inaccessible, les données pseudo-anonymisées sont soumises aux lois sur la protection des données personnelles. Selon l'approche relative, tant que le détenteur des données pseudo-anonymisées n'a pas accès à la table de correspondance, les données pseudo-anonymisées ne sont pas soumises aux lois sur la protection des données personnelles. Sous l'aLPD le PFPDT et le TF s'étaient prononcés pour l'approche absolue[56]. Sous le régime de la nLPD, l'approche relative a été retenue[57]. Les autorités de l'UE ont une approche absolue[58], mais pas la jurisprudence de la CJUE qui soutient une approche relative selon les possibilités de réidentification[59]. Au Québec, la Loi 25 a une approche absolue car elle ne parle que de « renseignements dépersonnalisés », lesquels elle protège et reprend essentiellement la même terminologie que la LPRPDE. Cette question est centrale pour les organisations détentrices de renseignements personnels car elle implique un niveau de risque devant être ré-évalué et donc des mesures de protection différentes. De manière générale, une organisation souhaitant valoriser des renseignements personnels doit nécessairement les traiter et donc les détenir sous leur forme originale. Ainsi, ces données, que l'on peut qualifier de primaire, sont évidemment soumises aux normes de protection des données personnelles et tant qu'il existe un risque de réidentification, les données pseudo-anonymisées doivent l'être également[60].

Tous les systèmes juridiques analysés font mention d'une approche du traitement de données personnelles et des mesures de protection des données basée sur les risques[61]. Cette notion subjective est souvent discutée car la perception des risques est radicalement différente selon les entités. Bien que cette approche permette une certaine flexibilité, elle a pour défaut de devoir porter beaucoup d'affaires devant un juge pour déterminer précisément ce qui est considéré comme étant « risqué » ou « peu risqué ». Il a également été démontré que la réidentification des personnes est relativement aisée en corrélant des sources d'informations diverses, présentant peu d'intérêt prises individuellement, mais intéressantes lorsque corrélées entre elles. Ainsi toute donnée doit être considérée comme un potentiel renseignement personnel[62].

A titre d'illustration de la différence de perception des risques, citons l'utilisation de Microsoft 365, un système américain hébergé en Europe, par le Conseil fédéral mais refusé par le PFPDT. Le CEPD a également dû se prononcer sur l'utilisation de Microsoft 365 par la Commission

[55] DU PERRON, par. 2-101
[56] ATF 136 II 508 et BENHAMOU, COTTIER, par. 19, p. 59
[57] Message nLPD, p. 6565 ss.
[58] BENHAMOU, COTTIER, par. 17, p. 59
[59] *CRU c/ Deloitte*, affaire T-557/20, CJUE, 26 avril 2023
[60] DU PERRON, par. 2-85
[61] BENHAMOU, COTTIER, par. 6, p. 13, art. 3.5 Loi 25
[62] DU PERRON, par. 2-88

Européenne[63], laquelle n'était pas en conformité avec le RGPD et s'est donc vu restreindre drastiquement son utilisation. Au Canada, la solution Microsoft 365 est également utilisée par différentes entités gouvernementales dont le Commissaire[64] et le gouvernement du Québec, pour laquelle des analyses de risques ont été menées mais sans positionnement contre l'utilisation d'une telle solution. Lors de l'utilisation de Microsoft 365 ou tout autre système américain de stockage et de traitement de données, la question se pose non seulement sur la manière dont le fournisseur protège les données personnelles, mais également sous l'angle de « l'existence d'un droit d'accès légal en faveur d'une autorité étrangère » ainsi que de « l'existence d'un système de surveillance de masse »[65]. Ainsi, l'utilisation d'une telle solution peut remettre en cause la souveraineté numérique des États.

En sus de la protection des données elle-même, la question de la protection des métadonnées[66] doit également être abordée. Une métadonnée peut contenir autant d'informations utiles que la donnée elle-même. Elle contient entre autres informations autres les informations concernant l'émetteur et le receveur de la communication, l'heure, le lieu de connexion, la durée, les moyens utilisés. Ainsi, la collecte de masse de métadonnées doit être considérée comme étant une activité soumise à la protection des renseignements personnels[67]. Cette position est une évolution bienvenue de la doctrine récente canadienne. Dans les lois de première génération cette question n'était pas abordée, explicitement du moins. La Suisse ne s'est pas positionnée sur cette question.

B. Personnes concernées par le traitement et procédure

Il faut en premier lieu déterminer qui est concerné par ces différentes lois sur la protection des renseignements personnels. Les différentes législations internationales s'accordent sur le fait que ces dispositions de protections ne s'appliquent qu'aux personnes physiques, les personnes morales étant exclues. La Suisse a corrigé sa nLPD dans ce sens, car l'aLPD offrait une protection aux personnes morales mais celle-ci n'a jamais réellement été utilisée[68]. Dans la nouvelle législation Suisse, les personnes morales peuvent toujours faire appel à l'art. 28 CC et à la LTrans pour bénéficier de droits similaires.

La nLPD est applicable également aux personnes physiques faisant un traitement de renseignements personnels, tout comme le RGPD, tandis que la Loi 25 ne s'applique qu'aux entreprises, tout comme la LPRPDE.

La Loi 25, à l'art. 88.0.1 donne un droit d'accès aux renseignements personnels d'une personne décédée à sa succession, aux conjoints ou à un proche parent sauf si la personne concernée avait émis des dispositions contraires. A contrario, la nLPD ne s'applique qu'aux « êtres humains », ce qui exclut de facto les personnes décédées[69]. Aucune disposition ni dans la nLPD ni dans la nOLPD adressent cette situation, contrairement à la aOLPD qui réglait l'accès aux renseignements d'une personne décédée à son art. 1 al. 7. Ainsi, dans un tel cas, aucune protection n'est proposée par la nouvelle législation et cette absence de régulation est critiquée par la doctrine[70]. Le RGPD écarte très clairement son application aux personnes décédées dans

[63] Positionnement du EDPS sur Microsoft 365
[64] Positionnement du Commissariat sur Microsoft 365
[65] FISCHER, PITTET
[66] MOYSE, p. 36
[67] BENYEKHLEF, DÉZIEL, p. 190-191
[68] Message nLPD, p. 6632
[69] BENHAMOU, COTTIER, par. 10, p. 25 et par. 23, p. 60
[70] BENHAMOU, COTTIER, par. 10, p. 24

son considérant 27. Ainsi, ce sont les héritiers qui devraient faire valoir une atteinte à leur personnalité.

Afin d'illustrer une interprétation radicalement différente entre le Canada et la Suisse de la notion de protection, prenons l'exemple d'un employé faisant un usage personnel d'un ordinateur professionnel fourni par son employeur. Il existe un jugement dans ces deux pays pour des faits très similaires : un professeur d'école utilise son ordinateur professionnel pour visionner du contenu à caractère pornographique, se fait dénoncer par le service informatique qui a découvert cet usage et une résiliation de son contrat de travail s'en suit. Le professeur conteste la résiliation devant le tribunal, ce qui nous permet d'observer comment un tel cas est traité.
La CSC dans l'affaire *R. c. Cole* en 2012[71] a déterminé que « l'employé a une *attente raisonnable de vie privée* lorsqu'il est au travail. » et que « les employeurs ne peuvent se fier aux politiques relatives au milieu de travail pour neutraliser entièrement les attentes raisonnables des employés à l'égard de la protection de leur vie privée. ». Ainsi, le service informatique par son accès à l'ordinateur de son employé a violé la *Charte canadienne* en ne respectant pas la protection de la vie privée. Donc les éléments de preuves déposées sont irrecevables car obtenus inconstitutionnellement.
La défense dans l'affaire ATA/836/2020 portée devant la Cour de justice genevoise en 2020, pour des faits similaires à l'affaire *R. c. Cole,* n'a tout simplement pas considéré qu'il pouvait y avoir une violation du droit de protection de la vie privée. La Cour de justice genevoise ne l'a pas non plus relevé. Force est de constater à la suite de la lecture de ces arrêts qu'en Suisse, la notion de vie privée pour un employé faisant usage de moyens de son employeur est moindre qu'au Canada.

En Suisse toujours, les personnes concernées ne font que rarement valoir leurs droits[72] compte tenu de l'aspect rebutant d'une procédure judiciaire. A cet effet, il faut relever que le législateur a voulu simplifier et rendre accessible les procédures dans le cas relatifs à la LPD car celles-ci sont soumis à la procédure simplifiée (art. 243, al. 2 let. d CPC) et aucun frais judiciaire n'est perçu (art. 113 al. 2 let. g CPC).

Au Québec, un juge administratif de la CAI traite les demandes d'examen de mésentente. Un processus de médiation similaire à la procédure de conciliation en Suisse est entamé, rendant ainsi la procédure d'apparence plus accessible[73].

Le RGPD prévoit à son consid. 141 une procédure de réclamation à l'autorité de contrôle nationale de la résidence de la personne concernée (ou au lieu de l'infraction présumée) ainsi qu'un droit de recours juridictionnel basé sur l'art. 8 de la *Charte des droits fondamentaux de l'Union européenne*.

C. Dispositions pour le traitement de données personnelles

Avant de considérer les dispositions de protection, l'angle de la responsabilité doit être abordé. Il faut déterminer qui a la responsabilité des informations personnelles et donc à qui incombe la responsabilité de prendre des dispositions de protection. Cette responsabilité se base sur la

[71] *R. c. Cole*, [2012] 3 R.C.S. 34, CSC
[72] MEIER, METILLE, par. 3, art. 32
[73] Règles de preuve et de procédure de la Commission d'accès à l'information

notion de détention de l'information, soit l'exercice d'un contrôle sur l'information[74]. Ainsi, la responsabilité de protection incombe au contrôleur de l'information.

Les principales dispositions pour le traitement de données personnelles ainsi que les attentes en termes de sécurité lors du traitement ont largement évolué ces dernières années et se retrouvent dans toutes les législations comparées. Les principes fondamentaux suivants, bien que pas exhaustifs, sont d'un intérêt particulier en droit comparé :

1. Licéité du traitement (art. 6 al. 1 nLPD, art. 37 C.c.Q, art. 5 Loi 25, art. 4.4 LPRPDE, art. 5 RGPD)

La nLD fait référence au principe de la bonne foi à son art. 6 al. 1. Celui-ci permet ainsi de jouer le rôle de « clause générale » pour tous les cas qui ne seraient pas explicitement traités par la nLPD[75]. Par ailleurs, l'art. 31 nLPD présente les motifs justificatifs sur lesquels il est possible de traiter des renseignements personnels. Le principe d'intérêt prépondérant est la base sur laquelle se reposent la plupart des traitements.

Le RGPD défini à l'art. 5 al. 1 let. a le principe d'un traitement « licite, loyal et transparent », qui peut comparer au principe de « bonne foi » en droit suisse. Toutefois, ces trois adjectifs couvrent une large portion des principes de base du RGPD : la notion de licite couvre ainsi l'entier du RGPD, la notion de loyale donne une certaine garantie de traitement équilibré entre les intérêts des parties, bien que plus faible que les autres adjectifs, et la notion de transparence impose certaines obligations au détenteur des données personnelles, notamment le droit d'accès, les critères de traitement des renseignements personnels et la conception sécuritaire des systèmes de traitement.[76]

Le LPRPDE reprend ce même principe à l'art. 4.4 où elle fait mention d'un recueil de renseignements personnels « de façon honnête et licite ».

La Loi 25 est plus lacunaire dans cette définition, car elle évoque de collecte « par des moyens licites » à l'art. 5, mais complète l'art. 37 du C.c.Q qui mentionne « un intérêt sérieux et légitime », or cette notion n'est pas définie par la législation[77]. Ainsi, la jurisprudence précise que « le critère de nécessité est rempli si les renseignements ne sont pas superflus, sans objet ni pertinence »[78] et que la collecte doit « répondre à un objectif nécessaire, soit légitime, important, urgent et réel. »[79]

Ces clauses génériques permettent ainsi de couvrir les principes de la protection des données personnelles et de s'assurer que leur traitement se fait dans l'intérêt des personnes concernées.

2. Consentement libre et éclairé (art. 6 al. 7 LPD, art. 12 et ss Loi 25, art. 37 C.c.Q, art. 4 RGPD, art. 4.3 annexe 1 LPRPDE)

[74] DU PERRON, par. 3-12
[75] BENHAMOU, COTTIER, par. 18 art. 6
[76] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, par. 35 et ss, art. 5, p. 270
[77] ROY, art. 37
[78] GRANOSIK, GRENIER, SAMSON, par. 5/5
[79] *Idem*, par. 5/19

L'obtention d'un consentement valable est largement commentée car il est une composante principale du droit à l'autodétermination[80] et sa définition varie selon les législations. Les limitations sur la capacité à le donner de manière éclairée par manque de compréhension des technologies sont grandissantes[81]. De plus, un consentement donné par un individu, en particulier au traitement de ses informations personnelles peut avoir une portée au-delà de sa propre personne car il pourrait avoir des effets sur un groupe de population partageant des caractéristiques communes[82].

Au Canada, le principe du consentement éclairé se retrouve à l'art. 4.3 de l'annexe 1 de la LPRPDE mais les critères évoqués sont généralement des recommandations, comme évoqué à l'art. 5 al. 2 LPRPDE. Ces critères ne sont pas très développés, si ce n'est la mention des principes de consentement préalable, d'information, de limitation au besoin strictement nécessaire et d'attentes raisonnables de la personne notamment. La forme du consentement est évoquée mais toujours de manière lacunaire. Certaines exceptions permettant la collecte, l'utilisation et la transmission de renseignements personnels à l'insu ou sans le consentement de la personne sont définis à l'art. 7 LPRPDE. Le Commissaire a édicté des lignes directrices pour l'obtention d'un consentement valable[83] afin de combler les lacunes de la LPRPDE, développant notamment 7 principes directeurs et reprenant les notions de sensibilité de l'information et d'attente raisonnable des personnes concernées.

Au Québec, l'art. 14 Loi 25 précise que le consentement doit être manifeste, libre, éclairé et donné à des fins spécifiques. Le consentement manifeste doit être évident et indiscutable[84]. Le consentement libre doit être fait sans contrainte ou conséquence négative pour la personne concernée. Le consentement éclairé doit être précis, ce qui implique notamment que la personne concernée doit être informée des types de renseignements collectés et du traitement qui en sera fait, incluant la transmission à des tiers[85]. Le consentement donné à des fins spécifiques ne doit pas être général mais pour chaque usage prévu. Ainsi les termes « des informations jugées nécessaires » et « toute autre information jugée pertinente » ne sont pas suffisamment précis[86]. Par conséquent, le même renseignement utilisé dans plusieurs finalités doit faire l'objet de consentement séparé[87]. La CAI complète ces principes[88] avec plusieurs critères dont celui de nécessité : une évaluation du besoin du renseignement personnel doit être effectuée avant même sa collecte. Le critère de temporalité est également mentionné introduisant la validité du consentement limitée dans le temps. Les autres critères évoqués (distinct, compréhensible, granulaire) peuvent se retrouver dans les principes généraux de la Loi 25.

En Suisse, le consentement est requis à l'al. 7 de l'art. 6 nLPD et décrit comme valable si la volonté de la personne est exprimée librement, clairement et après avoir été dûment informée. Le consentement doit être explicite dans le cadre de données sensibles. Il doit toujours être obtenu avant le traitement des données et est révocable en tout temps[89]. Il n'est pas soumis à une exigence de forme particulière, ainsi il peut être tacite[90] mais le silence, l'inaction ou un

[80] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, par. 6 et 8 art. 4(11), p. 198
[81] *Idem*, par. 9 art. 4(11), p. 199
[82] *Idem*, par. 11 art. 4(11), p. 199
[83] Lignes directives du Commissaire
[84] GRANOSIK, GRENIER, SAMSON, par. 14/1
[85] DU PERRON, par. 3-44
[86] GRANOSIK, GRENIER, SAMSON, par. 14/3
[87] *Idem*, par. 14/1
[88] Lignes directrices 2023-1
[89] MEIER, METILLE, par. 76 et 77, art. 6
[90] Message nLPD, p. 6647

comportement purement passif d'une personne ne peut pas être considéré comme un consentement[91]. Le consentement n'est pas nécessaire lors du traitement de données personnelles par des personnes privées, sauf dans le cas de données sensibles selon l'art. 30 nLPD. Le principe d'un consentement par type de traitement n'est pas repris, ainsi le consentement peut porter sur plusieurs traitements différents[92]. Cette possibilité d'interpréter un consentement implicite, inféré par le comportement de la personne[93], est contraire aux principes évoqués par la Loi 25 et la LPRPDE.

Le RGPD, lui, fait mention à l'art. 4 ch. 11 de « toute manifestation de volonté, libre, spécifique, éclairée et univoque » et stipule également que le consentement peut être donné par « un acte positif clair ». Il est complété par l'art. 7 qui détaille la forme du consentement et le droit au retrait du consentement à tout moment, aussi simplement que lorsqu'il est donné. Ainsi, le consentement n'est pas valable lorsqu'il n'est pas donné librement, c'est-à-dire lorsque la personne n'a pas d'autre choix et subira des conséquences négatives en ne le donnant pas[94] ou lorsqu'il existe une différence notable dans la balance des pouvoirs[95]. Le principe de consentement spécifique permet de donner un consentement granulaire au traitement, ainsi plusieurs traitements séparés sur les mêmes données font l'objet de consentements séparés[96]. Le consentement éclairé est possible uniquement lorsque la personne concernée a reçu toutes les informations essentielles à la compréhension du traitement au moment du consentement[97], garantissant ainsi la prise de décision informée. Le consentement univoque est donné lorsque que toute ambiguïté est levée. Ainsi également dans l'UE, il n'est pas acceptable de considérer une inaction comme un consentement[98]. Certaines situations où il n'est pas nécessaire d'obtenir le consentement sont réservées, par exemple lorsque le traitement est requis par la loi ou lorsqu'il existe un intérêt légitime.

Les 7 principes édictés par le Commissaire sont très développés en regard de ce qui est fait en Suisse, par exemple en développant le principe du consentement dynamique et continu. La Loi 25 est la plus développée d'un point de vue législatif. La nLPD manque encore de maturité sur ce point, notamment parce que les principes de consentement ne sont pas autant développés que dans le RGPD.

3. Minimisation de la collecte et principe de proportionnalité (art. 6 al. 2 nLPD, art. 4.4 LPRPDE, art. 5, art. 5 Loi 25, al. 1 let. c RGPD)

Le principe de proportionnalité a pour but d'éviter la collecte trop large de données personnelles et de s'assurer que le traitement des données est strictement nécessaire.

Il est évoqué dans la nLPD à l'art. 6 al. 2, mais il fait en réalité référence à un droit constitutionnel car la proportionnalité est un principe de l'État de droit[99]. Ce principe peut être décomposé en trois aspects : l'aptitude, la nécessité et la proportionnalité au sens étroit[100]. Le critère de l'aptitude vise à déterminer objectivement le but du traitement. Ainsi, il ne peut pas

[91] MEIER, METILLE, par. 79, art. 6 et BENHAMOU, COTTIER, par. 172, art. 6
[92] Message nLPD, p. 6647
[93] *Idem*, p. 6647.
[94] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, par. 21 art. 4(11), p. 203
[95] *Idem*, par. 23 art. 4(11), p. 204
[96] *Idem*, par. 29 art. 4(11), p. 205
[97] *Idem*, par. 43 art. 4(11), p. 209
[98] *Idem*, par. 60 art. 4(11), p. 214
[99] MEIER, METILLE, par. 27, art. 6
[100] BENHAMOU, COTTIER, par. 24, art. 6

être théorique ou abstrait[101] et doit donc répondre à un besoin effectif[102]. Ensuite, la nécessité du traitement doit être apte à atteindre le but identifié[103] et ses finalités doivent être reconnaissables[104]. Enfin, avec le principe de proportionnalité, on retrouve les principes de collecter des données uniquement les données nécessaires[105]. Une pesée des intérêts doit donc être faite, mettant en balance les intérêts de la personne visée par la collecte et le but visé du traitement pour justifier la collecte[106]. Tous les intérêts, tant publics que privés, doivent être pris en compte et un rapport adéquat entre eux doit exister[107].

Au Canada, on retrouve le principe de proportionnalité à l'art. 4.4 LPRPDE décrit avec l'interdiction de « recueillir des renseignements de façon arbitraire » et de « restreindre tant la quantité que la nature des renseignements recueillis ». Toutefois, certains auteurs critiquent le manque de clarté sur les critères définissant la proportionnalité[108].

Au Québec, ce principe de proportionnalité est défini à l'art. 37 C.c.Q. comme limitant la collecte de renseignements « pertinents à l'objet déclaré » et est complété par l'art. 5 de la Loi 25 en ces termes : « ne doit recueillir que les renseignements nécessaires aux fins déterminées avant la collecte ».

Dans l'UE, le principe de proportionnalité est mentionné à l'art. 5, al. 1 let. c RGPD en utilisant les termes « adéquates, pertinentes et limitées ».

4. Droit de suppression (art. 32 al. 2 nLPD, art. 40 C.c.Q, Loi 25 à l'art. 28.1, art. 17 RGPD)

L'introduction du droit de suppression de ses données personnelles dans le cadre du RGPD a permis d'établir un droit à l'oubli. Celui-ci a été rendu célèbre dans la cause Google Spain[109] dans laquelle la CJUE a obligé le moteur de recherche Google à supprimer des renseignements concernant un individu.

Le droit à l'oubli est repris dans la nLPD à l'art. 32 al. 2, mais celui-ci n'est pas absolu car une pesée des intérêts doit être effectuée[110] pour son application.

Ce droit est également présent dans la Loi 25 à l'art. 28.1, lequel est très développé comparativement à la nLPD. Ce principe n'est pas absolu et doit être modéré selon différents critères longuement discutés lors des débats parlementaires[111] et dans la doctrine[112].

[101] BENHAMOU, COTTIER, par. 27, art. 6
[102] MEIER, METILLE, par. 27, art. 6
[103] BENHAMOU, COTTIER, par. 28, art. 6
[104] MEIER, METILLE, par. 41, art. 6
[105] Message nLPD, p. 6644
[106] MEIER, METILLE, par. 28, art. 6
[107] BENHAMOU, COTTIER, par. 34, art. 6
[108] GRATTON, GUILMAIN, p. 23
[109] Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, arrêt C-131/12, CJUE, 13 mai 2014
[110] MEIER, METILLE, par. 26, art. 32
[111] GRANOSIK, GRENIER, SAMSON, commentaires art. 28.1
[112] GRATTON, GUILMAIN, p. 52

Dans la LPRPDE, une telle disposition n'existe pas en tant que telle, mais le droit de retrait du consentement (art. 4.3.8) pourrait être considéré comme équivalent. Malheureusement, il n'existe pas à notre connaissance de cas ayant traité ce sujet devant la CSC.

5. Droit à la portabilité (art. 28 al. 1 LPD, art. 20 RGPD, art. 3.3 Loi 25)

Le RGPD a été le premier à intégrer le droit à la portabilité des données d'un individu à son art. 20. Les données exportées doivent l'être dans un format structuré et courant, permettant ainsi d'être réimporté dans un autre système. Toutefois, ce droit entraine certains défis technologiques et moraux, tel que celui de ne pas porter atteinte aux droits de protection des renseignements personnels d'autres personnes en exerçant son propre droit à la portabilité[113].

Ce droit est repris dans la Loi 25 aux art. 3.3 et 27 ainsi que dans la LPD à l'art. 28 mais pas dans la LPRPDE, probablement car ce principe n'existait tout simplement pas lorsque cette dernière est entrée en vigueur.

Le RGPD a également été conçu dans l'objectif de favoriser un marché unique dans l'UE[114], ceci pouvant expliquer pourquoi la Suisse l'a repris. Le Canada pourrait faciliter le droit à l'autodétermination de ses citoyens en exigeant une telle portabilité.

Il faut également relever que ce droit n'inclut volontairement pas les données inférées des renseignements personnels afin de protéger le secret d'affaire[115]. Cette question pourrait venir un enjeu central dans les prochaines années avec l'apprentissage automatique de l'intelligence artificielle.

6. Droit à l'information des personnes concernées en cas d'incident (Art. 3.5 Loi 25, art. 10.1-3 LPRPDE, art. 24 nLPD, art. 34 RGPD)

Toutes les régulations s'accordent sur le fait que la notification aux personnes concernées par un incident de sécurité touchant leurs renseignements personnels doit être fait lorsqu'il existe un risque élevé. L'appréciation du risque étant partagée entre le détenteur des renseignements personnels et l'autorité de contrôle, sauf dans le cas de la Loi 25. Une autre exception à la communication est le principe d'effort disproportionné que l'on retrouve dans toutes les lois comparées. Ainsi, tout incident de sécurité de l'information de renseignements personnels ne mène pas forcément à une notification aux personnes concernées.

L'obligation d'annonce a été introduite dans la LPRPDE aux art. 10.1 à 10.3 en 2018 avec la notion d'« au plus tôt possible […] après l'atteinte ». Certains auteurs souhaitent voir l'établissement de critères clairs menant à l'annonce[116].

La Loi 25 fait mention d'un « risque sérieux » à son art. 3.5 pour déclencher la notification avec diligence[117] tant à la CAI et les personnes concernées. Le délai n'était pas précisé, toutefois la notion de diligence invoquée sous-entend le principe de rapidité et de soin[118]. Le législateur a souhaité que seule la CAI soit à même de juger si l'atteinte est de nature à nécessiter une

[113] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, par. 5 art. 20, p. 512
[114] BENHAMOU, COTTIER, par. 1, p. 18
[115] DU PERRON, par. 4-49
[116] GRATTON, GUILMAIN, p. 45
[117] DU PERRON, par. 4-37
[118] GRANOSIK, GRENIER, SAMSON, commentaires art. 3.5

communication aux personnes concernées, retirant ainsi cette prérogative à l'entreprise privée[119], contrairement en droit Suisse.

Le RGPD décrit ce droit à l'art. 34 et intègre la notion de « risque élevé » pour initier une communication « dans les meilleurs délais » par le responsable du traitement. L'autorité de contrôle peut également exiger une communication. La définition des « meilleurs délais » reste vague, mais ce délai doit être établi en coordination avec les autorités, notamment en cas d'enquête judiciaire[120].

La nLPD ne consacre pas un article de loi dédié à l'annonce aux personnes concernées, l'art. 24 traitant de toutes les annonces. L'al. 4 mentionne « lorsque cela est nécessaire à sa protection », donc restreignant encore plus la notion de « risque élevé » évoquée à l'al. 1[121]. La formulation de la loi reste floue sur cette question[122]. Aucun délai n'étant évoqué pour cette communication, certains auteurs estiment qu'il y aura donc un « petit temps » supplémentaire après l'annonce au PFPDT pour la faire[123].

On regrette le filtrage des notifications selon une évaluation arbitraire du risque. Ainsi les personnes concernées ne peuvent pas connaître lors de leur consentement les critères d'évaluation auxquels leurs informations personnelles seront soumises pour initier une communication en cas d'incident. Par ailleurs, une obligation de notification en cas de tout type d'incident pourrait renforcer la sensibilisation du public à ces problématiques et permettre de faire un choix éclairé lorsqu'il s'agit de communiquer leurs renseignements personnels à des tiers. D'ailleurs, l'avant-projet de révision de la LPD allait dans ce sens mais n'a pas été retenu[124]. Certains auteurs pensent que cela aurait pour effet de créer une lassitude chez les personnes concernées compte tenu du nombre de notifications que cela engendrerait[125]. Ainsi, la question est de savoir si l'information du public prime sur la praticité. Il serait par exemple imaginable que le PFPDT publie une liste des entreprises ayant fait l'objet d'un incident, comme le fait la CAI[126]. On appréciera que la Loi 25 ne laisse aucun choix à l'entreprise concernée quant à la pertinence ou non de celle-ci, évitant par la même occasion la prise en compte de l'aspect réputationnel lors de la pesée des intérêts qui peut peser lourd dans la décision finale.

7. Principe de protection dès la conception et sécurité par défaut (art. 7 et 8 LPD, art. 9.1 et 10 Loi 25, art. 25 RGPD)

Les principes de sécurité dès la conception et de la sécurité par défaut peuvent d'un premier abord sembler similaires. La sécurité par défaut, bien qu'étant l'une des composantes de la sécurité dès la conception, a pour objectif d'assurer une certaine protection des données personnelles des utilisateurs sans que ceux-ci aient à s'en soucier. La sécurité dès la conception, principe par ailleurs inventé au Canada au début des années 1990[127], a pour but d'anticiper la divulgation d'informations personnelles en concevant des systèmes de traitement de

[119] GRANOSIK, GRENIER, SAMSON, débats parlementaires art. 3.5
[120] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, par. 8 art. 34, p. 685
[121] MEIER, METILLE, par. 72, art. 24
[122] BENHAMOU, COTTIER, par. 41, art. 24
[123] MEIER, METILLE, par. 78, art. 24
[124] *Idem*, par. 5, art. 24
[125] BENHAMOU, COTTIER, par. 44, art. 24
[126] Rapport sur les incidents déclarés à la CAI en 2023
[127] MEIER, METILLE, par. 1, art. 7

l'information sécuritaires se reposant sur 7 principes : mise en œuvre de mesures proactives et préventives, assurer une protection par défaut, intégrer dans les systèmes et procédures la protection de la vie privée, obtenir un paradigme à somme positive et non à somme nulle lors du traitement des données personnelles, garantir la sécurité de bout en bout et en tout temps, intégrer les principes de transparence et de visibilité et enfin, placer les intérêts des utilisateurs au premier plan en respectant leur vie privée.

Ces 7 principes fondamentaux ont posé la base des législations de 2ème génération sur la protection des données personnelles : absents dans la aLPD, ils sont décrits à l'art. 7 nLPD, à l'art. 25 RGPD et à l'art. 9.1 de la Loi 25. La LPRPDE ne fait aucune mention de ces principes.

Le message nLPD[128] décrit bien les attentes du législateur en la matière et celles-ci sont relativement matures en regard des 7 principes évoqués précédemment.

8. Sécurisation des données (art. 4.7 LPRPDE, art. 32 RGPD, art. 8 nLPD, art. 10 Loi 25)

Les mesures exactes attendues pour sécuriser les informations ne sont jamais clairement définies dans les lois, principalement par volonté d'assurer la continuité de la pertinence des lois malgré les évolutions technologiques. Les principes d'analyse de risques et de niveau de sécurité adéquat relativement à la sensibilité des données se retrouvent dans toutes les lois. Celles-ci se basent généralement sur les cadres de gouvernance en sécurité de l'information tels que le NIST Cyber Security Framework et la norme internationale ISO 27'001:2022. Ces cadres évoquent tous le principe d'analyse et d'évaluation de risques et de mesures de protection appropriées selon les risques. Bien que pas évoqués dans les lois, ils sont cités par la doctrine comme référence[129]. Les mesures de sécurité peuvent être de type organisationnelles, physiques, technologiques ou visant à modifier le comportement des personnes[130].

Les grands principes que l'on retrouve communément sont l'anonymisation (altération irréversible des données personnelles pour les désidentifier) et la pseudo-anonymisation (altération réversible des données personnelles permettant la réidentification). Un exemple de pseudo-anonymisation serait de remplacer les données personnelles par un identifiant unique et aléatoire, permettant supposément le traitement des informations pseudo-anonymisées avec des mesures de sécurité moindres[131]. Une table de correspondance entre les données personnelles et l'identifiant unique est conservée et soumise aux mesures de protection complètes des données personnelles. La classification des informations pseudo-anonymisée est discutée dans les différentes législations.

La LPRPDE oblige à son art. 4.7 de protéger les renseignements personnels « au moyen de mesures de sécurité correspondant à leur degré de sensibilité » contre « la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées ». Des mesures matérielles, administratives et techniques sont également évoquées à l'art. 4.7.3, permettant de faire le lien avec la norme ISO 27001:2022, bien que celle-ci ne soit jamais clairement évoquée. Toutefois, le principe de « dépersonnalisation » n'existe pas dans cette loi et serait plutôt introduit dans le projet de *Loi sur la protection de la vie privée des consommateurs* (Projet de loi C-11).

[128] Message nLPD p. 6648
[129] DU PERRON, par. 4-31
[130] ISO 27001:2022, Annex A
[131] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, art. 32, par. 21

Au Québec, la Loi 25 mentionne à l'art. 10 une obligation de prendre des mesures de sécurité pour assurer la protection des renseignements personnels mais reste très laconique sur le détail, ne faisant qu'indirectement référence à la notion de risque. Heureusement, des décisions de la CAI viennent compléter les requis, en précisant par exemple que la protection doit s'appliquer tout au long du cycle de vie des renseignements personnels[132] et que des contrôles actifs de la sécurité sont requis[133]. Ainsi, la Loi 25 exige la mise en place de moyens de protection renforcés[134]. L'art. 23 de la Loi 25 définit l'anonymisation comme une procédure qui « ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne » mais ne traite pas spécifiquement de la pseudo-anonymisation. Il est complété par le *Règlement sur l'anonymisation des renseignements personnels* traitant spécifiquement de l'anonymisation. Celui-ci fait mention de « risques résiduels de réidentification […] très faibles » à l'art. 7 et d'une réévaluation périodique des risques à l'art. 8. Ainsi, il faut considérer des données pseudo-anonymisée comme des renseignements personnels au titre de la Loi 25. Par ailleurs, les mesures techniques de protection doivent constamment être mises à jour, la responsabilité personnelle des dirigeants pouvant être engagée pour négligence dans le cas contraire[135].

La nLPD parle à l'art. 8 de « mesures organisationnelles et techniques appropriées » pour assurer « une sécurité adéquate des données personnelles par rapport au risque encouru » et que « les mesures doivent permettre d'éviter toute violation de la sécurité des données ». On relèvera le terme « éviter toute violation », ce qui est particulièrement contraignant et difficile à atteindre en sécurité informatique. Par les termes utilisés, la nLPD oblige également à considérer une approche de sécurité de l'information gouvernée par les risques[136]. La OPDo détaille assez précisément les attentes de protection en termes techniques et organisationnels dans son art. 3 et reprend notamment les principes directeurs de sécurité de l'information : intégrité, confidentialité, disponibilité. Il faut également souligner que le principe de disponibilité évoqué à l'art. 3, al. 2, let. d est lié à l'art. 32, al. 1 let. c du RGPD mais qu'il n'est pas retrouvé dans la LPRPDE. Enfin, la nLPD introduit un concept de certification des systèmes de traitement à son art. 13, qui aurait pu être étendu en tant qu'obligation pour les traitements à risques élevés comme le voulait initialement le PFPDT[137]. Malheureusement, ceci n'a pas été retenu et fort est à parier sur le fait que très peu de systèmes se verront certifiés. Le principe de certification des systèmes comme dans le RGPD et la nLPD n'existe pas dans la Loi 25 ni la LPRPDE.

En Suisse, l'adéquation des mesures de protection doivent être évaluées selon huit critères définis à l'art. 1 OPDo. Il faut relever que l'OPDo se concentre principalement sur des mesures de protection à un instant donné, la réévaluation des mesures de protection en continu étant seulement évoqué à l'art. 1 al. 5. La régularité de tests de sécurité « à des intervalles appropriées » est plutôt inférée dans le rapport explicatif lors de la procédure de consultation[138]. Concernant les données pseudo-anonymisées en particulier, celles-ci ne sont pas considérés comme des renseignements personnels et n'ont donc pas besoin de faire l'objet de mesures de protection additionnelles si « le risque de réidentification est nul en pratique » et que « la

[132] GRANOSIK, GRENIER, SAMSON, par. 10/1
[133] *Idem*, par. 10/4
[134] DU PERRON, par. 4-10
[135] *Idem*, par. 4-28
[136] Message nLPD p. 6650
[137] *Idem,* p. 6656
[138] BENHAMOU, COTTIER, par. 16, art. 8 et Rapport explicatif OPDo

réidentification demanderait des opérations excessivement compliquées, longues et coûteuses »[139].

Le RGPD introduit à son art. 32 le principe de mesures de sécurité lors du traitement basées sur une évaluation des risques. Les mesures de sécurité évoquées doivent être intégrées à tous les niveaux et non seulement lors du traitement des informations, ce qui inclut également lors du transfert d'information et de leur stockage[140]. Le RGPD présente les mêmes types de mesures de protection que l'OPDo à l'art. 32 mais ajoute également la notion d'évaluations régulières de l'efficacité des mesures de protection, ce qui est essentiel en sécurité de l'information pour garantir une protection en continu. Dans le cas de données pseudo-anonymisées, le RGPD considère cette mesure pour réduire les risques mais n'exclut pas ces données des mesures de protection des renseignements personnels.[141] En effet, la pseudo-anonymisation ne suffit pas pour exclure tout risque et donc toute autre mesure de protection.

Sur le principe de la pseudo-anonymisation, la Loi 25 et le RGPD sont alignés pour considérer que ces données sont des renseignements personnels et doivent donc faire l'objet de protections adéquates basées sur l'évaluation des risques. La nLPD accorde un peu plus d'ouverture sur ce sujet et l'absence de cette notion dans la LPRPDE démontre une fois de plus la nécessité d'actualiser cette loi.

De manière générale, on aurait préféré que la périodicité de la revue de l'efficacité des mesures de sécurité soit plus clairement imposée, par exemple avec une formulation se rapprochant d'« au moins une fois par exercice financier et dès que le risque évolue ». De notre point de vue, la formulation actuelle n'est pas suffisante pour assurer un degré de sécurité suffisant des renseignements personnels. En effet, la plupart des organisations considèrent ces éléments lors de la réalisation d'un projet traitant de renseignements personnels, mais rarement lors de l'exploitation de la solution livrée par le projet. La norme ISO 27701 pourrait permettre d'unifier sur le plan international les principes de sécurité des renseignements personnels. Ceci serait un avantage notable pour les multinationales.

13. Transfert transfrontalier de renseignements personnels (nLPD art. 16, ch. V RGPD)

Il est impossible de traiter de la protection des renseignements personnels sans évoquer le cas des transferts transfrontaliers de renseignements personnels. Cette situation se produit très fréquemment du fait des technologies actuellement utilisées, notamment l'infonuagique. Cette thématique devrait faire l'objet d'un travail en soi étant donné sa complexité et son ouverture vers d'autres lois internationales qui ne sont pas considérées ici. C'est la raison pour laquelle elle ne sera pas traitée ici. Nous nous contenterons de référer le lecteur aux articles des lois traitant de ce sujet ainsi qu'à la saga « Schrems » dans l'UE avec les décisions Schrems I[142] (invalidation de l'accord « Safe harbor » concernant le transfert de données personnelles de l'UE vers les USA dans le cadre de l'utilisation de Facebook), Schrems I[bis][143](statut de consommateur dans le droit à la protection des données personnelles), Schrems II[144] (invalidation de l'accord « Privacy Shield » pour l'échange de données personnelles entre l'UE et les USA dans le cadre de l'utilisation de Facebook) et Schrems III[145] (suite de l'échange de

[139] MEIER, METILLE, par. 104, art. 8
[140] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, par. 2 art. 32, p. 661
[141] *Idem*, par. 25 art. 32, p. 666
[142] *Maximillian Schrems c. Data Protection Commissioner*, affaire C-362/14, CJUE, 6 octobre 2015
[143] *Maximilian Schrems c. Facebook Ireland Limited*, affaire C-498/16, CJUE, 25 janvier 2018
[144] *Data Protection Commissioner c. Facebook Ireland Ltd and Maximillian Schrems*, affaire C-311/18, CJUE, 16 juillet 2020
[145] *Maximilian Schrems c. Meta Platforms Ireland Limited*, affaire C-446/21, CJUE, 4 octobre 2024

données personnelles entre l'UE et les USA) de la CJUE qui représente bien la complexité de ces enjeux. On saluera par la même occasion la ténacité de M. Schrems et on relèvera que la même cause contre Facebook a également été traitée au Canada[146].

Un exemple représentatif de la problématique typique de protection des renseignements personnels dans un cadre transfrontalier peut être illustré comme qui suit : même si les données personnelles ne sont pas « communiquées » en dehors de l'Union européenne, mais qu'elles pourraient être « accessibles » depuis l'extérieur de l'Union européenne via des lois telles que le CLOUD Act[147] aux USA, quelles sont les protections offertes ?

Comme précédemment évoqué, lors d'un transfert interprovincial ou à l'étranger la Loi 25 ne s'applique pas et est remplacée par la LPRPDE. Certains auteurs défendent, à juste titre, une harmonisation des principes de transfert à l'étranger[148].

D. Délégué à la protection des données, autorités de supervision et sanctions

Les préposés à la protection des données des différents États comparés sont les entités qui agissent comme point de contact pour le public en cas de violation suspectée de la loi, comme conseillers auprès des entreprises et également comme vérificateurs du respect des lois en la matière. La Suisse a le PFPDT, le Québec a la CAI, le Canada le Commissaire, les pays de l'UE ont les autorités nationales de vérification et subsidiairement la CEPD. Tous agissent comme conseillers. Certains auteurs[149] comparent le PFPDT à un commissaire (une seule personne secondée par une équipe), proche du modèle canadien et en contradiction avec le modèle québécois qui a une commission (instance collégiale composée de plusieurs personnes). Toutes ces instances, en sus de leur mission de protection des renseignements personnels, ont celle d'assurer le droit à la transparence et à l'accès aux informations gouvernementale. Historiquement, le Canada l'a conçu ainsi car les deux sujets sont considérés comme liés. En Suisse, cela n'est qu'une question « d'économie budgétaire avant tout » afin de ne pas devoir créer encore une autre entité indépendante[150].

Toutes les lois comparées exigent un *Data Protection Officers* (DPO) que les entreprises doivent mettre en place. Le rôle de DPO est d'être le point de contact tant pour le public qui souhaite faire appliquer ses droits que pour les préposés à la protection des données. Il agit également comme conseiller interne en conformité et parfois comme responsable du traitement. Bien que le concept général soit le même dans toutes les législations comparées, leur rôle diffère grandement. En effet, en Suisse un « conseiller à la protection des données » est optionnel (art. 10 LPD) tandis qu'au Québec, la définition du « responsable de la protection des renseignements personnels » est obligatoire (art. 3.1 Loi 25). Dans l'Union Européenne, le « délégué à la protection des données » est obligatoire lorsque l'entreprise traite de grandes quantités de données personnelles ou sensibles, ou réalise un suivi systématique à grande échelle (art. 37 RGPD). Au Canada, la LPRPDE exige également à son annexe 1 à ce qu'un « responsable des renseignements personnels » soit nommé. Selon toutes ces législations, sauf

---

[146] *Canada (Privacy Commissioner) v. Facebook, Inc*., 2024 FCA 140, Federal Court of Appeal Decisions, 2024-09-09 et *Enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet de Facebook, Inc*., Conclusion no 2019-002, Commissaire, 25 avril 2019

[147] Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 115th United States Congress, 2018

[148] GRATTON, GUILMAIN, p. 59

[149] BENHAMOU, COTTIER, par. 8, p. 49

[150] *Idem*, par. 13, p. 50

en Suisse, le DPO doit réaliser des vérifications et des audits pour s'assurer de la conformité de l'organisation. Le RGPD est le plus strict car il demande à que le DPO soit directement relié à la direction et soit indépendant, concept que l'on ne retrouve pas dans les autres lois. L'indépendance du DPO est recherchée surtout par le RGPD mais peu considérée dans les autres législations comparées. Lors d'une non-conformité, le DPO au sens du RGPD est protégé contre les sanctions internes. Aucune autre loi comparée ne propose une telle protection pour le DPO, sa responsabilité personnelle ne pouvant être engagée qu'en cas de négligence grave.

L'annonce d'une violation de sécurité concernant des données personnelles doit se faire dans les meilleurs délais et au plus dans les 72 heures à l'autorité nationale de vérification désignée selon l'art. 33 al. 1 du RGPD, dans les 24 heures à la CAI selon la Loi 25 et dans les meilleurs délais au PFPDT selon l'art 24 al. 1 LPD. Certains auteurs suisses considèrent que la survenue d'une nouvelle information amenant à ré-évaluer le risque vers le haut lors d'un même évènement nécessitant une annonce ferait courir un nouveau délai[151]. Ceci semble une interprétation à tout le moins hasardeuse étant donné que lors d'incidents de sécurité, des faits nouveaux arrivent même jusqu'à la phase de post-mortem[152]. Dans l'UE, l'approche de « sur-déclaration » en cas d'incident prévaut[153], évitant ainsi des sanctions pour non-déclaration. Les informations minimales à détenir pour déclencher la notification sont le type de données, les circonstances de la brèche et le moment où celle-ci est survenue[154], ces informations pouvant par la suite être complétées mais en respectant le délai des 72 heures[155]. Ainsi, l'ampleur et la compréhension d'un incident doit être complète dans la fenêtre de 72 heures. En Suisse, l'annonce peut également être complétée avec des faits nouveaux, mais aucun délai n'est fixé pour obtenir le portrait complet de l'incident[156].
Le délai de 24 heures a été discuté dans le cadre du RGPD pour être en adéquation avec l'art. 2 par. 2 de la directive 2002/58/EC mais a finalement été fixé à 72 heures comme compromis avec comme contrepartie l'obligation de justification si la notification dépasse ce délai. La nLPD est donc la plus laxiste dans sa définition.

Des formulaires standardisés d'annonce ont été développés dans l'UE. La Suisse précise dans à l'art. 15 de l'OPDo les éléments minimaux à déclarer et a également mis à disposition le *Service en ligne d'annonce de violation de la sécurité des données*[157] dans lequel on relèvera que l'estimation des risques est simplement « Élevé » ou « Pas élevé ». Cette manière d'évaluer le risque va à l'encontre des théories d'analyse de risques qualitatives[158] qui préconisent au moins 5 niveaux de risques tels qu'insignifiant, faible, modéré, élevé, critique. Au Québec, la CAI propose également un formulaire standardisé[159], tout comme le Canada[160].

La sanction en cas de non-déclaration d'incident dans l'UE est de 2% du chiffre d'affaires mondial ou 10 millions d'Euros et la négligence du contrôleur de données est également puni[161]. Au Québec, la Loi 25 reprend les mêmes montants que le RGPD[162]. En Suisse, aucune sanction n'est prévue pour les personnes morales, le projet de loi ayant été amendé pour enlever la

[151] BENHAMOU, COTTIER, par. 24, p. 277
[152] NIST SP800-122, p. 5-4
[153] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, par. 11, p. 678
[154] *Idem*, par. 4, p. 674 et Lignes directrices 01/2021
[155] *Idem*, par. 15, p. 679 et ss.
[156] MEIER, METILLE, par. 19, art. 24
[157] Disponible à l'adresse https://databreach.edoeb.admin.ch/report
[158] ISO 27005:2022, A.1.1.2.3 et NIST Risk Management Framework
[159] Formulaire d'annonce d'incident à la CAI
[160] Formulaire de déclaration d'une atteinte à la LPRPDE
[161] SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT, par. 17, p. 680
[162] Art. 90.12 Loi 25

dimension pénale[163]. Il faut également souligner que le PFPDT ne peut dénoncer que des personnes physiques faisant du traitement dans un cadre privé d'informations personnelles pour refus de déclaration d'incident après une décision du PFPDT[164]. Ceci donne peu de pouvoir coercitif à la nLPD car la grande majorité des risques, tant en termes de volume, de sensibilité et de potentiel d'atteinte se situent dans les entreprises. Dès lors, il ne reste plus qu'aux lésés la responsabilité contractuelle comme moyen de défense en cas d'atteinte des leurs renseignements personnels[165]. Au Canada, il n'est pas non plus prévu de sanctions, toutefois le Commissaire peut dénoncer l'infraction au Procureur général du Canada pour d'éventuelles poursuites[166]. La responsabilité du contrôleur de l'information n'est exclue dans aucune législation lors du recours à des sous-traitants.

Pour sanctionner une atteinte à la protection des données personnelles, trois éléments distincts doivent être considérés : le droit administratif, le droit civil et le droit pénal. En Suisse, le PFPDT ne peut pas prononcer de sanctions administratives, alors qu'au Québec la CAI le peut. Les décisions de la CAI peuvent être contestées devant les tribunaux, mais elles sont directement exécutoires. Tandis qu'en Suisse, le PFPDT ne peut qu'émettre des recommandations et saisir le TAF afin de contraindre l'entité à s'y conformer mais n'a pas de pouvoir de sanction directe. Le Commissariat au Canada ne peut pas non plus directement condamner une entreprise, il doit passer par la Cour, ce qui rend son pouvoir similaire à celui du PFPDT. La CAI a donc plus de pouvoir et d'effet dissuasif que le PFPDT. Cette situation illustre bien la différence de perception du rôle de l'État entre le Québec et la Suisse.

Au regard du droit de la responsabilité contractuelle et extracontractuelle, la notion de dommages-intérêts punitifs est acceptée au Québec (par ex. art. 93 al. 1 Loi 25), mais pas en droit Suisse. Le concept de tort moral est toutefois accepté dans les deux juridictions. La dimension pénale est quant à elle également présente au Québec à l'art. 91 de la Loi 25 mais omis par le RGPD et la LPRPDE. À ce titre, une personne morale coupable pourra être condamnée à une amende comprise entre 15'000$ CAD et 25 millions $CAD ou à une amende correspondant à 4% du chiffre d'affaires mondial si celui-ci est plus élevé. Ce principe est équivalent au RGPD, lequel prévoit des amendes administratives jusqu'à 20 millions € ou à une amende correspondant à 4% du chiffre d'affaires mondial si celui-ci est plus élevé. Au Canada, la LPRPDE prévoir une amende maximale de 100 000 $ CAD à son art. 28, sans prendre en compte le chiffre d'affaires mondial. En Suisse, l'amende est d'un montant maximal de 250'000 CHF et ne prend pas non plus en compte le chiffre d'affaires mondial pour la détermination de celle-ci.

Force est donc de constater que le Québec s'est aligné sur le RGPD pour s'assurer d'une application stricte des moyens de protection des renseignements personnels, tandis que la Suisse et le Canada ne démontrent que très peu d'ambition pour mettre en place des moyens dissuasifs.

IV. Conclusion

Comme nous avons pu le voir, les régulations dans le domaine de la protection des données personnelles évoluent rapidement et les lois en vigueur sont récentes. Par conséquent, il est parfois difficile de trouver des arrêts pouvant comparer les lois actuellement en vigueur. Bien

[163] MEIER, METILLE, art. 24, par. 7
[164] *Idem*, art. 24, par. 15
[165] *Ibid*.
[166] BENYEKHLEF, DÉZIEL, p. 251

que l'origine des législations sur la protection des renseignements personnels au Canada et en Suisse ne trouvent pas leur source dans les mêmes principes, celles-ci convergent toutefois vers une approche relativement commune.

Il est difficile de protéger les renseignements personnels, et même les États rencontrent des difficultés en la matière. Les affaires *Services globaux de relogement Brookfield (BGRS)* dans laquelle le *Commissariat* lui-même a été touché par une fuite de données personnelles[167] et l'affaire *Xplain* en Suisse qui a touché l'*Office fédéral de la police (Fedpol), l'Office fédéral de la douane et de la sécurité des frontières (OFDF) et l'entreprise Xplain* et sur laquelle le PFPDT a eu l'occasion de se prononcer en 2024[168] en sont la preuve.

Il serait pertinent que les lois de protection des renseignements personnels fassent la différentiation entre le traitement de petites quantités de données nécessaires pour le fonctionnement ordinaire des PME et le traitement de masse de données lors de recueils de mégadonnées. Pour être considérées comme mégadonnées, les recueils devraient répondre à trois critères : leur volume, leur variété et leur vélocité[169]. L'intérêt des mégadonnées est que le contrôleur peut en retirer un enrichissement par leur exploitation[170]. Par conséquent, se pose la question des bénéfices issuspar des fruits du traitement de celles-ci. Or malgré l'arrêt de la CSC dans l'affaire *R. c. Stewart*[171] vu en introduction, on comprend que la jurisprudence au Canada a tout de même considéré que les renseignements personnels ont une valeur quantifiable et qu'ils sont donc dignes de protection[172]. La détermination du propriétaire du revenu découlant du traitement de ces mégadonnées doit être considéré comme un vide juridique. Les grandes entreprises privées se sont clairement accaparées ces bénéfices sans en redistribuer les retombées aux propriétaires qui ont permis de constituer ces mégadonnées. Le Code civil du Québec propose une interprétation de ce sujet à ses art. 972 et 973 : la valeur de la matière première doit être remboursée à celui qui l'a fournie[173]. Malheureusement, les données considérées individuellement n'ont que très peu de valeur[174], réduisant ainsi l'indemnisation potentielle. Une approche complémentaire permettant éventuellement d'augmenter tant la valeur et les protections requises serait de considérer les données inférées (déduites) de renseignements personnels comme étant elles-mêmes des renseignements personnels[175]. Cette approche poserait toutefois la question de la propriété de celles-ci.

En sus de la régulation des mégadonnées, la régulation explicite des métadonnées serait également la bienvenue afin de clarifier leur traitement et de reconnaître l'importance de celles-ci. La Suisse pratiquant l'interception légale des télécommunications et la conservation des métadonnées par le biais de la LSCPT, on peut considérer qu'il existe également un vide juridique dans ce domaine prétéritant ainsi les utilisateurs des moyens de télécommunication. Il faut également relever que les lois sur la protection des renseignements personnels ne sont pas les seules à requérir des mesures de sécurité de l'information ainsi que d'annonce des incidents de sécurité. La régulation du domaine de la sécurité de l'information est en pleine évolution : des lois spécifiques à ce sujet viennent d'entrer en vigueur ou sont en passe de le devenir. Ces lois contribueront à renforcer la sécurité de l'information et par conséquent, les

[167] Rapport du Commissariat 2023-2024
[168] Rapport du PFPDT sur l'incident Xplain
[169] DU PERRON, par. 1-28
[170] *Idem*, par. 2-31
[171] *R. c. Stewart* ,1988, 1 RCS 963
[172] DU PERRON, par. 2-27
[173] *Idem*, par. 2-39
[174] *Idem*, par. 2-43
[175] *Idem*, par. 2-99

mesures imposées bénéficieront indirectement à la protection des renseignements personnels. En Suisse, la *Loi sur la sécurité de l'information* (LSI) introduite en 2020 précise de manière détaillée les attentes pour les systèmes d'information considérés comme critiques, complété par les *circulaire 2023/01* et *circulaire 2024/04* de la FINMA visant spécifiquement les établissements financiers ainsi que la *Norme minimale pour les TIC*. Cette dernière est déclinée par secteurs et vise principalement les infrastructures critiques du pays. Dans l'Union Européenne, la directive NIS2[176] visant à assurer un niveau élevé de cybersécurité dans l'ensemble des pays membres a également été adoptée en 2022, laquelle est complétée par le Data Act[177], le Data Governance Act[178] et la réglementation DORA[179] notamment. Au Canada, le *Projet de loi C-26* concernant la cybersécurité vise à poser un cadre de règlementation de la sécurité des infrastructures essentielles et devrait entrer en vigueur prochainement. Au Québec, la *Loi concernant le cadre juridique des technologies de l'information* et la *Loi sur les renseignements de santé et de services sociaux* abordent également ces questions.
Ainsi, l'évolution de la régulation sur l'intelligence artificielle devra emboiter le pas aux régulations sur la protection des renseignements personnels afin d'assurer des moyens appropriés pour protéger les citoyens. Au Canada, le *Projet de loi C-27* traite de cette question et dans l'UE, le *Règlement 2024/1689*[180] en fait de même mais ce n'est pas une volonté politique actuelle en Suisse[181].

Finalement, la protection des renseignements personnels est l'une des facettes de l'enjeu de souveraineté numérique. Tant le Canada que la Suisse sont en retard dans le domaine, tandis que l'UE et le Québec se sont dotés de moyens davantage matures. Le retard canadien s'explique car la LPRPDE actuellement en vigueur date de presque 25 ans et des tentatives d'amélioration sont en cours. Il ne se comprends moins pour la Suisse car la nLPD est récente mais manque tant de précisions que de moyens pour son application stricte afin de faire respecter le droit des citoyens. Par ailleurs, la Loi 25 est considérée comme la plus mature dans le domaine de la protection des renseignements personnels au Canada[182]. Certains détracteurs accuseraient l'UE de pallier le manque d'innovation par de la régulation, mais comme nous avons pu le voir, il n'en n'est rien : le RGPD reste la régulation la plus stricte, forçant les entreprises à innover pour s'adapter et pour respecter un droit fondamental en cours d'érosion. Enfin, aux Etats-Unis, la *California Consumer Privacy Act* (CCPA) est souvent citée comme référence nord-américaine dans le domaine de la protection des renseignements personnels. Comme le mentionnait un parlementaire au Québec, ces régulations visent à imposer un cadre strict aux entreprises du domaine privé, ainsi : « *il faut qu'ils fassent le ménage, puis qu'ils détruisent, puis qu'ils encadrent, puis qu'il y ait des pare-feux* ».

[176] Directive 2022/2555
[177] Règlement 2023/2854
[178] Règlement 2022/868
[179] Règlement 2022/2554
[180] Règlement 2024/1689
[181] Avis du Conseil fédéral du 26.04.2023 à la suite de l'interpellation 23.3147 du 14.03.2023 sur la réglementation de l'intelligence artificielle en Suisse par Samuel Bendahan.
[182] DU PERRON, par. 5-17

Bibliographie

Doctrine en Suisse

NICOLAS BÉGUIN, YANIV BENHAMOU, BERTIL COTTIER ET 8 AUTRES, in : Benhamou Yaniv / Cottier Bertil (édit.), LPD : loi fédérale sur la protection des données, 1ère éd., Bâle, 2023. (cité : BÉGUIN, BENHAMOU, COTTIER)

PHILIPPE MEIER, SYLVAIN MÉTILLE ET 19 AUTRES, in : Meier Philippe / Metille Sylvain (édit.), *Commentaire romand, Loi sur la protection des données*, 1ere éd., Lausanne, 2023. (cité : MEIER, MÉTILLE)

Doctrine au Québec

BENYEKHLEF Karim, DÉZIEL Pierre-Luc, *Le droit à la vie privée en droit québécois et canadien*, Montréal (Québec) Canada, Éditions Yvon Blais, 2018. (cité : BENYEKHLEF, DÉZIEL)

COMEAU Paul-André*, Protection des renseignements personnels, Projet et réalité*, École nationale d'administration publique (Québec), Bibliothèque Nationale du Québec, 2009. (cité : COMEAU)

DU PERRON Simon, *Droit à la vie privée, mégadonnées et intelligence artificielle : Cadre juridique en matière de protection des renseignements personnels*, Montréal (Québec) Canada, LexisNexis, 2022. (cité : DU PERRON)

GERVAIS, Marie-Claude et SÉGUIN, Marie-France, Le bijuridisme au Canada et dans le monde : Quelques considérations , Ministère de la Justice du Canada, https://www.justice.gc.ca/fra/pr-rp/sjc-csj/harmonization/hlf-hfl/f2-b2/tdm-toc.html (cité : GERVAIS, SÉGUIN)

GUILMAIN Antoine, GRATTON Éloïse, *The protection of personal information in the private sector in Québec : looking back and thinking forward*, Montréal (Québec) Canada, Éditions Yvon Blais, 2020. (cité : GRATTON, GUILMAIN)

GRANOSIK, Lukasz, GRENIER Kateri-Anne, SAMSON Kenny, *Loi sur la protection des renseignements personnels dans le secteur privé : Législation, Jurisprudence*. 3ème édition annotée, Montréal (Québec) Canada, Éditions Yvon Blais, 2023. (cité : GRANOSIK, GRENIER, SAMSON)

ROY, Alain, Code civil du Québec, Annotations - Commentaires, 9e édition, 2024-2025, Montréal (Québec) Canada, Éditions Yvon Blais, 2024 (cité : ROY)

Doctrine de l'UE

SPIECKER gen. Döhmann Indra, PAPAKONSTANTINOU Vagelis, HORNUNG Gerrit, DE HERT Paul, *General Data Protection Regulation: Article-by-Article Commentary*, Baden-Baden, Nomos, 2024. (cité : SPIECKER, PAPAKONSTANTINOU, HORNUNG, DE HERT)

MOYSE Pierre-Emmanuel, *Le droit au respect de la vie privée : les défis digitaux, une perspective de droit comparé – Canada*, Bruxelles (Belgique), Service de recherche du Parlement européen Unité Bibliothèque de droit comparé, Octobre 2018 (cité : MOYSE)

Sources officielles en Suisse

Circulaire 2023/1 Risques et résilience opérationnels – banques Gestion des risques opérationnels et garantie de la résilience opérationnelle, Berne, FINMA, 7 décembre 2022

Code de procédure civile du 19 décembre 2008, RS 272 (cité : CPC)

Communication FINMA sur la surveillance 04/2024, Gestion des risques opérationnels des directions de fonds et des gestionnaires de fortune collective, Berne, FINMA, 12 juin 2024

Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101 (cité : Cst)

Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, RO 1974 2151, (cité : CEDH)

Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, FF 2017 p. 6565 ss. (cité : nLPD)

Loi fédérale sur la protection des données (LPD) du 19 juin 1992, FF 1992 III 929, p. 929 ss. (cité : aLPD)

Loi fédérale sur le principe de la transparence dans l'administration du 17 décembre 2004, RO 2006 2319 (cité : LTrans)

Loi fédérale sur la sécurité de l'information au sein de la Confédération du 18 décembre 2020, RO 2022 232 (cité : LSI)

Loi [vaudoise] du 11 septembre 2007 sur la protection des données personnelles (LPrD; BLV 172.65) (Cité : LPrD)

Message du Conseil fédéral du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 p. 6565 ss. (cité : Message nLPD)

Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 439 (cité : Message aLPD)

Message relatif à la loi fédérale sur la transparence de l'administration (Loi sur la transparence, LTrans), FF 2003 1807, p. 1815 ss. (cité : Message LTrans)

Ordonnance du 31 août 2022 sur la protection des données (OPDo), RO 2022 568 (cité : OPDo)

Rapport explicatif du 31 août 2022 sur l'ordonnance sur la protection des données (OPDo) in : Département fédéral de justice et police (www.ejpd.admin.ch), Berne 2022, p. « https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/datenschutz/erlaeuterungen-vo-f.pdf.download.pdf/erlaeuterungen-vo-f.pdf » (25 septembre 2024), (cité : Rapport OPDo)

Sources officielles au Québec

Charte des droits et libertés de la personne, ch. C-12, LégisQuébec, 2024 (cité : Charte québécoise)

Code civil du Québec, ch.CCQ-1991, LégisQuébec, 2024 (cité : C.c.Q.)

Consultations particulières et auditions publiques sur le projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels - Vol. 45 N° 96, Journal des débats de la Commission des institutions, Assemblée nationale du Québec, 2020 (cité : Consultations projet de loi 64)

Décret 783-2024 du 1er mai 2024 sur l'anonymisation des renseignements personnels, Gazette officielle du Québec, 2024 (cité : Décret 783-2024)

Journal des débats de la Commission des institutions, Québec, 42-1, vol. 45 n° 113, Assemblée nationale du Québec, 2 février 2021 (cité : Journal des débats)

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ch. A-2.1, LégisQuébec, 2024 (cité : RLRQ)

Loi sur la protection des renseignements personnels dans le secteur privé, ch. P-39.1, LégisQuébec, 2024 (cité : Loi 25)

Loi concernant le cadre juridique des technologies de l'information, ch. C-1.1, LégisQuébec, 2024.

Loi sur les renseignements de santé et de services sociaux, ch. R-22.1, LégisQuébec, 2024

Loi sur la protection du consommateur, ch. p-40.1, LégisQuébec, 2024

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, ch. 25, LégisQuébec, 2021 (cité : Loi 25)

Projet de loi N°64 de l'Assemblée nationale du Québec du 12 juin 2020 modernisant des dispositions législatives en matière de protection des renseignements personnels, Éditeur officiel du Québec, 2021.

Règles de preuve et de procédure de la Commission d'accès à l'information, ch. A-2.1, r. 6, LégisQuébec, 2024.

Règlement sur les incidents de confidentialité, ch. A-2.1, r. 3.1, LégisQuébec, 2024

Règlement sur l'anonymisation des renseignements personnels, ch. A-2.1, r. 0.1, LégisQuébec, 2024

Sources officielles au Canada

Loi canadienne sur les droits de la personne, L.R.C. (1985), ch. H-6, CanLII (citée : LCDP)

Loi sur la protection des renseignements personnels, L.R.C. (1985), ch. P-21, CanLII (citée : LCPRP)

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5, CanLII (citée : LPRPDE)

Code canadien du travail, L.R.C. (1985), ch. L-2, CanLII

Loi sur la protection des renseignements personnels, L.R.C. 1985, ch. P-21, CanLII (citée : LRC)

Partie I de l'annexe B de la Loi de 1982 sur le Canada, ch. 11 (R.-U.), CanLII (citée : Charte canadienne)

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, déposé à la Chambre des communes le 2 décembre 2020, ministère de la Justice du Canada (Cité : Projet de loi C-11)

Projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois, déposé à la Chambre des communes le 14 décembre 2022, ministère de la Justice du Canada (cité : Projet de loi C-26)

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, déposé à la Chambre des communes le 4 novembre 2022, ministère de la Justice du Canada (cité : Projet de loi C-27)

Sources officielles de l'UE

Charte des droits fondamentaux de l'Union européenne, 2012/C 326/02, Journal officiel de l'Union européenne, 26 octobre 2012

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens - n° 108, Conseil de l'Europe, Strasbourg, 28 janvier 1981 (cité : Convention 108)

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel de l'Union européenne, 1995

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, L 119/89, Journal officiel de l'Union européenne, 2016

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE), Journal officiel de l'Union européenne, 2022

Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, Série des traités européens - n° 181, Conseil de l'Europe, Strasbourg (France), 8 novembre 2001 (cité : STE 181)

Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des Traités du Conseil de l'Europe - n° 223, Strasbourg (France), 10 octobre 2018 (cité : Convention 108+)

Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités du Conseil de l'Europe - n° 223, Conseil de l'Europe, Strasbourg, 10 octobre 2018 (Cité : Rapport 223)

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal officiel de l'Union européenne, 2016 (cité : RGPD)

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), Journal officiel de l'Union européenne, 2016 (cité : Règlement 2024/1689)

Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, Éditions OCDE, Paris, 2002 (cité : Lignes directrices OCDE)

Lignes directrices 01/2021 Exemples concernant la notification de violations de données à caractère personnel, European Data Protection Board, Bruxelles (Belgique), 2021

Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités du Conseil de l'Europe - n° 223, Strasbourg (France), 10 octobre 2018 (cité : Rapport 223)

Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), Journal officiel de l'Union européenne, 2022

Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011, Journal officiel de l'Union européenne, 2022 (cité : DORA)

Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données), Journal officiel de l'Union européenne, 2023

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), Journal officiel de l'Union européenne, 2024

Sources officielles des États-Unis d'Amérique

California Consumer Privacy Act (CCPA), § 1798.100 et seq., California Civil Code, 28 juin 2018

Health Insurance Portability and Accountability Act, Public Law 104-191, Congrès des États-Unis, 1996 (cité : HIPPA)

Autres sources

Avis à la commission d'accès à l'information concernant un incident de confidentialité impliquant des renseignements personnels et qui présente un risque de préjudice sérieux, Commission d'accès à l'information du Québec, Québec (Canada), mars 2023, in https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_FO_Incident_Conf.pdf (Cité : Formulaire d'annonce d'incident à la CAI)

Enquête sur la conformité à la LPRPDE de Desjardins suite à l'atteinte aux mesures de sécurité des renseignements personnels entre 2017 et 2019, Conclusions en vertu de la LPRPDE no 2020-005, Commissariat à la protection de la vie privée, Gatineau (Canada), 14 décembre 2020, (cité : Enquête Desjardins)

European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies, European Data Protection Supervisor, Bruxelles (Belgique), 11 mars 2024 (cité: Positionnement du EDPS sur Microsoft 365)

Exportations de la Suisse par partenaire commercial, Administration fédérale des douanes, Berne, 2023, in https://www.bazg.admin.ch/bazg/fr/home/themes/statistique-du-commerce-exterieur-suisse/daten/handelspartner.html

FISCHER Philipp, PITTET Sébastien, Peut-on encore, en Suisse, recourir à des services cloud offerts par Microsoft ?, 16 août 2022, in www.swissprivacy.law/165

Formulaire : Déclaration d'une atteinte à la LPRPDE, Commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée, Gatineau (Canada), in https://www.priv.gc.ca/media/4845/lprpde_pb_form_f.pdf (cité : Formulaire de déclaration d'une atteinte à la LPRPDE)

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122, National Institute of Standards and Technology, 2010, (cité: NIST SP800-122)

Information relative aux incidents de confidentialité déclarés à la Commission Septembre 2022 – décembre 2023, Commission d'accès à l'information du Québec, Québec (Canada), 2024, in https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_Incid_Conf_Decl_2022-09_2023-12.pdf (cité : Rapport sur les incidents déclarés à la CAI en 2023)

ISO/IEC 27001:2022: Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences, International Organization for Standardization, 2022

ISO/IEC 27005:2022 Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information, International Organization for Standardization, 2022

ISO/IEC 27701:2019 Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices, International Organization for Standardization, 2019

Le commerce extérieur du Québec, Le calepin, édition été 2024, p. 38 in https://www.economie.gouv.qc.ca/fileadmin/contenu/publications/etudes_statistiques/echanges_exterieurs/calepin_exterieur.pdf

Lignes directrices 2023-1 – Consentement : critères de validité, Version 1.0, Commission d'accès à l'information du Québec, 31 octobre 2023 (cité : Lignes directrices 2023-1)

Lignes directrices pour l'obtention d'un consentement valable, Commissariat à la protection de la vie privée du Canada, Gatineau, 13 juillet 2021 (cité : Lignes directives du Commissaire)

Norme minimale pour améliorer la résilience informatique, Office fédéral pour l'approvisionnement économique du pays, Berne, mai 2023 (cité : Norme minimale en TIC)

Rapport annuel au Parlement 2023-2024 concernant la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques, Commissariat à la protection de la vie privée du Canada, Gatineau, Octobre 2024. (cité : Rapport du Commissariat 2023-2024)

Résumé de l'évaluation des facteurs relatifs à la vie privée du projet infonuagique Microsoft Office 365, Commissariat à la protection de la vie privée du Canada, Gatineau, 22 juin 2022 (cité : Positionnement du Commissariat sur Microsoft 365)

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, SP 800-37 Rev. 2, National Institute of Standards and Technology Taskforce, 20 décembre 2018 (cité : NIST Risk Management Framework)

Schlussbericht und Empfehlungen vom 25. April 2024 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in Sachen BAZG/Fedpol aufgrund Ransomware-Vorfall, Préposé fédéral à la protection des données et à la transparence, Berne, 25 avril 2024 (cité: Rapport du PFPDT sur l'incident Xplain)