2023 | VOLUME 57 | NUMÉRO 1

REVUE JURIDIQUE THÉMIS

de l'Université de Montréal

SOMMAIRE

LES PAGES DU CDACI

LES PAGES DU CRDP

LES ÉDITIONS THÉMIS

Les pages du CRDP

Centre de recherche
en droit public

Réflexion sur l'effectivité de l'obligation de divulgation d'incidents de sécurité en droit québécois

Nicolas Vermeys*

* Professeur titulaire à la Faculté de droit de l'Université de Montréal, directeur du Centre de recherche en droit public et directeur adjoint du Laboratoire de cyberjustice : www.vermeys.com. Courriel : nicolas.vermeys@umontreal.ca.

Plan de la chronique

Introduction

Dans la première édition des pages du Centre de recherche en droit public (CRDP), Vincent Gautrais annonçait une chronique « un peu particulière »[1] du fait qu'elle visait à servir d'introduction au CRDP, son approche et son histoire, « plutôt que de présenter une recherche spécifique »[2]. Au cœur de cette chronique se situait la présentation de l'École de Montréal, soit – pour citer une fois de plus le professeur Gautrais – « ce courant du voir "autrement", du voir "largement" le phénomène normatif »[3].

La présente contribution se veut ainsi, en quelque sorte, une illustration de cette vision, laquelle illustration passe par l'un des concepts phares de l'École de Montréal, soit l'effectivité des normes en général et du droit en particulier[4]. Comme le précise Karim Benyekhlef :

> L'effectivité du droit ne doit pas être confondue avec l'efficacité du droit. L'efficacité renvoie à la capacité d'une loi, d'une norme ou d'une règle à produire les effets que ses auteurs souhaitaient obtenir en la créant. L'effectivité du droit renvoie à une idée plus large, plus étendue et polyvalente et désigne tout type ou forme d'effet qu'une loi peut avoir.[5]

Guy Rocher viendra ainsi associer la notion d'effectivité aux effets « voulus et involontaires, recherchés ou accidentels, directs ou indirects, prévus et inattendus, sociaux, politiques, économiques ou culturels »[6] d'une règle de droit. Il établira par ailleurs une distinction entre une effectivité attendue

---

1 Vincent Gautrais, « Tentative définitionnelle du Centre de recherche en droit public (CRDP) », (2022) 56(2) *R.J.T.U.M.* 361, 365.

2 *Id.*

3 Vincent Gautrais (dir.), *École de Montréal*, Montréal, Éditions Thémis, 2019, quatrième de couverture.

4 Karim Benyekhlef, « Autour de l'École de Montréal », dans V. Gautrais (dir.), *id.*, p. 17, à la p. 29.

5 *Id.* Notons que cette définition se veut ainsi plus englobante que celle que l'on retrouve dans les dictionnaires juridiques où l'effectivité est définie comme étant le « [c]aractère d'une règle de droit qui est appliquée réellement ou qui produit l'effet recherché par le législateur ». Voir : Hubert Reid, *Dictionnaire de droit québécois et canadien*, 5e éd., Montréal, Wilson & Lafleur, 2015, p. 239.

6 Guy Rocher, « L'effectivité », dans Andrée Lajoie, Roderick A. MacDonald, Richard Janda et Guy Rocher (dir.), *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, Montréal, Éditions Thémis, 1998, p. 133, à la p. 136. Également cité dans Dalia Gesualdi-Fecteau et Maxine Visotzky-Charlebois, « La notion d'effectivité du droit », dans Stéphane Bernatchez et Louise Lalonde (dir.), *Approches et fondements*

du droit, soit « celle qui anime et structure le processus de la production du droit »[7] et une effectivité du droit observée, laquelle « se conduit à l'aide d'études empiriques des comportements de ceux à qui les normes étaient destinées »[8].

Ce long détour conceptuel nous ramène à notre point de départ et à la thématique de la présente chronique : l'effectivité de l'obligation de divulgation d'incidents de sécurité en droit québécois. En effet, avec la hausse progressive des attaques informatiques et autres incidents pouvant compromettre la sécurité des données détenues notamment par les entreprises et organismes publics au fil des ans[9], plusieurs législateurs à travers le monde ont opté pour l'adoption de dispositions législatives contraignant les représentants desdites entités à divulguer la survenance de tels incidents[10] ; le tout afin de permettre aux individus pouvant en subir préjudice de prendre les précautions nécessaires (l'effectivité attendue). Le Québec, s'inspirant notamment de l'approche européenne[11], a récemment emboîté le pas pour inclure une telle obligation dans ses divers textes de loi relatifs à la protection des renseignements personnels[12]. Mais qu'en est-il de l'effectivité observée de cette nouvelle obligation ?

Le 8 décembre 2022 paraissait, dans le journal *La Presse*, un article intitulé « Une trentaine d'entreprises ont déclaré des fuites en deux

du droit, Montréal, Éditions Thémis, 2020, p. 327, à la p. 335 ; et dans K. Benyekhlef, préc., note 4, à la p. 29.

7 K. Benyekhlef, *id.*

8 *Id.*, à la page 30 se référant à G. Rocher, préc., note 6, à la p. 138.

9 Cyberedge Group, « 2021 Cyberthreat Defense Report », 2021, p. 7, en ligne : <https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf>.

10 Voir Practical Law Data Privacy & Cybersecurity, « Global Data Breach Notification Laws Chart : Overview », *Thomson Reuters*, 2022, en ligne : <https://uk.practicallaw.thomsonreuters.com/w-016-6863?transitionType=Default&contextData=(sc.Default)>.

11 *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)*, J.O.U.E L 119 (4 mai 2016), art. 33 et 34, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679> (ci-après « Règlement général sur la protection des données »).

12 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, L.Q. 2021, c. 25. Cette loi est mieux connue sous l'appellation de « projet de loi 64 ».

mois »[13]. Sans prétendre que l'on puisse ici parler d'étude empirique, les données recueillies par Hugo Joncas, le journaliste ayant signé l'article, permettent tout de même de poser quelques constats quant à l'obligation de divulgation d'incidents de sécurité en droit québécois. Ce texte servira donc, en quelque sorte, d'assise à notre réflexion visant à cartographier l'obligation de divulgation d'incidents de sécurité en droit québécois (1) et à élaborer certaines hypothèses quant à son effectivité (2). Notons par ailleurs que, bien que cette obligation s'applique tant aux organismes publics que privés, notre analyse se concentrera sur sa perception au sein de l'entreprise privée.

I. L'émergence de l'obligation de divulgation d'incidents de sécurité en droit québécois

Tel que son nom l'indique, l'obligation de divulgation d'incidents de sécurité (*data breach notification*) découle de dispositions législatives obligeant tant les organismes publics que privés à divulguer publiquement tout incident de sécurité[14] ayant potentiellement compromis la sécurité[15] de données[16] qu'ils détiennent[17]. De telles obligations ont d'abord fait leur

13 Hugo Joncas, « Une trentaine d'entreprises ont déclaré des fuites en deux mois », *La Presse*, 8 décembre 2022, en ligne : <https://www.lapresse.ca/affaires/2022-12-08/protection-des-renseignements-personnels/une-trentaine-d-entreprises-ont-declare-des-fuites-en-deux-mois.php> (consulté le 14 avril 2023).

14 Par incident de sécurité, nous référons à « [u]n incident lié à la sécurité de l'information [qui] découle d'un (ou plusieurs) événement indésirable ou inattendu et présentant une probabilité de compromettre la confidentialité, l'intégrité ou la disponibilité de l'information ». Voir : Chambre des notaires du Québec, « Cadre de sécurité des actifs informationnels », 8 septembre 2016, p. 17, en ligne : <https://www.cnq.org/wp-content/uploads/2020/10/928825-cadre-secur-actifs-inform.pdf> (consulté le 14 avril 2023).

15 Comme nous le verrons ci-après, une majorité de lois viseront uniquement les incidents affectant l'une des composantes de la sécurité, c'est-à-dire la confidentialité, au dépend des deux autres (l'intégrité et la disponibilité). Voir : Nicolas Vermeys, « Why Class Action Suits for Security Breaches Need to Look Beyond Privacy Concerns », dans Ignacio N. Cofone (dir.), *Class Actions in Privacy Law*, Londres, Routledge, 2020, p. 81, à la p. 89.

16 Notons, comme nous l'aborderons ci-après, qu'une majorité de textes législatifs limitent leur portée aux seuls renseignements personnels.

17 National Conference of State Legislatures, « Security Breach Notification Laws », 17 janvier 2022, en ligne : <https://www.ncsl.org/research/telecommunications-and-

apparition aux États-Unis[18], puis en Europe, dès le début des années 2000[19]. Au Canada, c'est en Alberta que l'obligation de divulgation d'incidents de sécurité fera d'abord son entrée dans le corpus législatif avec l'ajout de l'article 34.1[20] à la *Personal Information Protection Act*[21] de cette province. Neuf ans plus tard, ce sera au tout du législateur fédéral d'emboîter le pas et d'ajouter une disposition au même effet[22] à la *Loi sur la protection des renseignements personnels et les documents électroniques*[23].

Au Québec, il faudra attendre l'adoption, en 2021, de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[24] pour qu'une obligation de divulgation d'incidents de sécurité soit ajoutée à la *Loi sur la protection des renseignements personnels dans le secteur privé*[25] (ci-après la « LPRPSP ») et le 22 septembre 2022 pour que cette obligation entre en vigueur[26]. Ainsi, tel que prévu au nouvel article 3.5 de la LPRPSP :

information-technology/security-breach-notification-laws.aspx> (consulté le 14 avril 2023).

18 Benoît Dupont et Benoît Gagnon, « La sécurité précaire des données personnelles en Amérique du Nord. Une analyse des statistiques disponibles », *Chaire de recherche du Canada en sécurité, identité et technologie*, 2008, p. 12, en ligne : <http://benoitdupont.openum.ca/files/sites/31/2015/07/securiteprecaire.pdf> (consulté le 14 avril 2023).

19 Voir Nicolas Vermeys, « Fostering Trust and Confidence in Electronic Commerce : Will the EUCanada Comprehensive Economic and Trade Agreement Really Effect Change ? » (2015) 20-2 *Lex Electronica* 63, 82.

20 Le premier alinéa de cette disposition se lit ainsi : « An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. »

21 *Personal Information Protection Act,* S.A. 2003, c. P-6.5.

22 Il s'agit de l'article 10.1 de la Loi, dont le premier alinéa prévoit que : « L'organisation déclare au commissaire toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu. »

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

24 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels,* préc., note 12.

25 *Loi sur la protection des renseignements personnels dans le secteur privé,* RLRQ, c. P-39.1.

26 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, préc., note 12, art. 175.

> 3.5. Une personne qui exploite une entreprise et qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.
>
> Si l'incident présente un risque qu'un préjudice sérieux soit causé, elle doit, avec diligence, aviser la Commission d'accès à l'information instituée par l'article 103 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1). Elle doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Elle peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication.
>
> Malgré le deuxième alinéa, une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.
>
> Un règlement du gouvernement peut déterminer le contenu et les modalités des avis prévus au présent article.

L'article 3.6 de la même loi vient préciser que la notion d'« incident de confidentialité » peut référer à un accès, une utilisation ou une communication non autorisé par la loi à un renseignement personnel, ou encore la perte ou toute autre atteinte audit renseignement. Quant au risque « qu'un préjudice sérieux soit causé », celui-ci devra être établi en fonction de « la sensibilité du renseignement concerné », des « conséquences appréhendées de son utilisation » et de « la probabilité qu'il soit utilisé à des fins préjudiciables »[27].

Avant de nous attarder à l'effectivité de ces dispositions – réflexion qui se veut limitée dans sa portée vu le peu de données disponibles pour l'instant –, nous nous permettons deux observations importantes.

---

[27] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 25, art. 3.7.

D'abord, le législateur québécois, à l'instar de ses homologues fédéral[28] et européen[29], a opté pour une obligation de divulgation double, c'est-à-dire que l'avis doit à la fois être transmis aux victimes potentielles de l'incident ainsi qu'à un organisme public chargé de l'application de la Loi, en l'occurrence : la Commission d'accès à l'information.

Le fait d'aviser directement les victimes potentielles semble – à première vue – parfaitement cohérent pour atteindre l'effectivité attendue. D'une part, cette approche a l'avantage de favoriser la transparence à l'égard des clients de l'entreprise visée et les habiliter ainsi à prendre les précautions nécessaires en cas d'incident. D'autre part, elle permet à l'entreprise de limiter sa responsabilité puisque, est-il utile de le rappeler, « [l]a personne qui est tenue de réparer un préjudice ne répond pas de l'aggravation de ce préjudice que la victime pouvait éviter »[30]. Ainsi, un avis direct et rapide permettra potentiellement à la victime d'annuler ses cartes de crédit, de changer ses mots de passe, etc., avant qu'elle ne subisse de préjudice.

Toutefois, une multiplication des avis auprès de victimes potentielles viendra également limiter l'effectivité de l'obligation puisqu'elle risque d'exposer ces individus au phénomène que nous qualifierons de lassitude à l'égard des avis d'incidents de sécurité (*breach notification fatigue*) :

> Indeed, there is growing evidence that a new type of negative externality and sub-optimal outcome has emerged from the systemic consequences of mandatory breach notification requirements – notification fatigue. In the beginning, when they were novel, breach notification letters had a significant effect on raising awareness and stimulating corrective behaviour on the part of both organizations and individuals. Over time, however, while the number of notification letters has continued to grow (In 2008 Maryland residents received over 200 such breach notifications!), the marginal utility and value of notification letters has levelled off and perhaps diminished as people become inured to receiving them and less concerned. As the number of notifications continues to increase over time (and the aggregate costs of notification), public reactions and concerns may well plateau and taper off (if they have not already done so). The social and economic benefits of mandatory notification may be subject to the law of diminishing returns. More is not always better. Can there be

---

28 *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 23, art. 10.1(1) et (3).

29 Règlement général sur la protection des données, art. 33 et 34.

30 *Code civil du Québec*, RLRQ c. CCQ-1991, art. 1479.

> too much notification? A tension exists between too little and too much notification, and with it socially optimal levels of security and privacy protections.[31]

Soit, selon un rapport australien, l'un des remèdes à la lassitude à l'égard des avis d'incidents de sécurité réside dans l'adoption de seuils de risques relativement élevés[32]. Ainsi, le critère du « risque de préjudice sérieux » proposé par le législateur québécois viendra contrer le phénomène de lassitude en réduisant le nombre d'avis reçus par les résidents québécois. Toutefois, comme le démontre l'article paru dans *La Presse* cité en introduction, les entreprises font une analyse asymétrique de ce critère. Par exemple, une pharmacie a considéré qu'« une boîte de médicaments mouillée et désagrégée » constituait un risque de préjudice sérieux parce que le livreur était possiblement à même de « voir les informations sur des clients à qui étaient destinés les médicaments »[33]. Il est à parier que d'autres entreprises n'auraient pas fait la même analyse du niveau de risque généré par un tel incident.

Ainsi, l'approche du législateur albertain – laquelle n'exige qu'un avis au Commissariat à l'information et à la protection de la vie privée de l'Alberta[34] – pourrait favoriser une plus grande effectivité de la norme. En effet, en confiant à un tiers neutre possédant plus souvent qu'autrement une meilleure capacité d'apprécier le risque de préjudice sérieux qu'un gestionnaire d'entreprise le rôle d'établir la pertinence d'aviser les victimes d'un incident, l'on s'assure d'une distribution plus cohérente et homogène des avis : si – et seulement si – le Commissariat considère le risque de préjudice suffisamment sérieux, il peut alors exiger que l'entreprise avise les personnes visées[35].

Notre seconde observation découle du fait que, bien que la présente chronique vise l'obligation de divulgation des incidents de sécurité, le législateur québécois ne semble pas partager cette ambition. En effet, l'article 3.5

---

31 Ann Cavoukian, « A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight », *Information and Privacy Commissioner*, 24 juin 2009, en ligne : <https://www.ipc.on.ca/wp-content/uploads/resources/privacy_externalities.pdf> (consulté le 14 avril 2023).

32 Dennis Gibson et Clive Harfield, « Contradictions and inconsistencies in Australia's mandatory data breach notification laws », (2021) 42 *CLSR* 1, 7.

33 H. Joncas, préc., note 13.

34 *Personal Information Protection Act*, préc., note 21, art. 34.1.

35 *Id.*, art. 37.1.

de la LPRPSP ne vise pas les « incidents de sécurité », mais bien les seuls « incidents de confidentialité ». Or, il est utile de rappeler que l'obligation de sécurité se divise en trois sous-obligations, soit celles d'assurer « la confidentialité[36], l'intégrité[37] et la disponibilité[38] de l'information tout au long de son cycle de vie[39] »[40]. Ainsi, un incident qui viendrait affecter l'intégrité d'une donnée – pensons à la corruption d'un fichier à la suite d'un bogue technique – ne serait pas visé par l'article 3.5 de la Loi. Bref, la portée de l'obligation de divulgation des incidents de sécurité en droit québécois demeure relativement restreinte, d'autant qu'elle ne vise que les renseignements personnels, soit « tout renseignement qui concerne une personne physique et permet de l'identifier »[41], ce qui implique qu'un incident impliquant d'autres types de renseignements sensibles – pensons notamment aux secrets commerciaux – ne devra pas être divulgué[42]. Encore une fois, nous soumettons l'hypothèse que ce choix du législateur aura une incidence potentielle sur l'effectivité de l'obligation de divulgation d'incidents de sécurité, notion que nous analyserons maintenant.

II. L'effectivité de l'obligation de divulgation d'incidents de sécurité en droit québécois

Nous l'avons vu, « l'étude de l'effectivité vise à mieux saisir les effets multiples du droit ainsi qu'à retracer les rationalités des destinataires lors-

36 « [P]ropriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des *processus* non autorisés » : norme ISO/IEC 27000:2018, art. 3.

37 « [P]ropriété d'exactitude et de complétude » : norme ISO/IEC 27000:2018, art. 3.

38 « [P]ropriété d'être accessible et utilisable à la demande par une entité autorisée » : norme ISO/IEC 27000:2018, art. 3.

39 La notion de cycle de vie renvoie à « l'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisme ». Voir Secrétariat du Conseil du trésor, « Directive gouvernementale sur la sécurité de l'information », Québec, 2021, art. 2, en ligne : <https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/directive_securite_information2021.pdf>. Voir également l'article 6 de la *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1.

40 Secrétariat du Conseil du trésor, *id.*, art. 1.

41 *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 25, art. 2.

42 Voir N. Vermeys, préc., note 15, à la p. 89.

qu'ils ont recours au modèle normatif ou lorsqu'ils le rejettent »[43]. Par « destinataires », il est fait référence en l'occurrence aux représentants des entreprises et organismes visés par l'obligation de divulgation d'incidents de sécurité[44]. Retracer les rationalités de ces individus nous invite à nous éloigner des préceptes sociologiques abordés en introduction pour nous tourner vers l'analyse économique du droit puisque la rationalité constitue – avec la rareté et l'incertitude – l'un des trois piliers de cette approche[45]. Comme l'expliquent Ejan Mackaay *et al.* :

> Placé devant une décision à prendre le [destinataire] fait l'inventaire des résultats désirés (*valeurs* ou *préférences*), identifie les actions pouvant être entreprises dans la poursuite de ceux-ci (*options*), détermine dans quelle mesure chaque action, compte tenu des suites qu'elle provoquera, contribuera aux résultats désirés et à quel coût (*valorisation*) et retient celle qui y contribuera le plus (*choix*).[46]

Les auteurs poursuivent en soulignant que :

> Le modèle du choix rationnel prévoit que les individus décident à la lumière des informations sur les options et leurs conséquences dont ils disposent au moment de la décision. Ils sont censés choisir la meilleure option selon leurs préférences personnelles. Possiblement, ils considèreront plus tard ce choix non optimal à la lumière de nouvelles informations obtenues par la suite. L'observateur externe, se basant sur d'autres valeurs et d'autres informations, peut bien considérer leur choix comme non optimal. Tout cela n'affecte pas, cependant, la rationalité du choix du décideur au moment de la décision.[47]

---

43 D. Gesualdi-Fecteau et M. Visotzky-Charlebois, préc., note 6, à la p. 331.

44 « L'expression "destinataire" désigne l'individu, les groupes, les collectivités, dont l'État, ou les collectifs à qui se destine la norme juridique » : *id.*, à la p. 331.

45 Ejan Mackaay, Stéphane Rousseau, Pierre Larouche et Alain Parent, *Analyse économique du droit*, 3e éd., Montréal, Éditions Thémis, 2021, p. 31. Si le passage d'une approche théorique à l'autre peut surprendre, elle s'explique par le fait que « [l]a conception économique est intéressante d'un autre point de vue. Elle permet d'établir des ponts avec d'autres sciences sociales. Les sociologues Boudon et Opp, par exemple, s'inspirent de visions de l'homme qui rejoignent celle de l'économiste. Opp propose une théorie de l'émergence des normes qui est dans le prolongement de celle de Demsetz : les normes surgissent afin d'internaliser les externalités ». Voir Ejan Mackaay, « La règle juridique observée par le prisme de l'économiste : une histoire stylisée du mouvement de l'analyse économique du droit », (1986) 1 *R.I.D.E.* 43.

46 E. Mackaay *et al.*, *id.*, p. 36.

47 *Id.*, p. 37.

De ce qui précède, il découle que l'individu rationnel confronté à l'obligation de divulguer un incident de sécurité intervenu au sein de son entreprise n'y donnera pas nécessairement suite pour la simple raison que cette obligation est codifiée à l'article 3.5 de la LPRPSP. En effet, « [f]ace à l'obligation de faire (ou de ne pas faire) quelque chose, l'individu met en balance son coût d'opportunité à obtempérer et le risque de sanction auquel il s'expose en contrevenant, compte tenu de la probabilité de détection des infractions et de la sévérité des sanctions »[48].

Qu'en est-il en l'occurrence ?

Tel que nous l'avons soulevé en introduction, selon un article paru dans *La Presse*, une trentaine d'entreprises ont déclaré des incidents de confidentialité à la Commission d'accès à l'information entre le 22 septembre et le 28 novembre 2022, ce qui équivaut en moyenne à approximativement un incident aux deux jours. Or, ces chiffres surprennent puisqu'ils ne s'inscrivent pas dans les tendances nationales. En effet, selon une étude publiée par CyberEdge en 2020, 80,7 % des entreprises canadiennes auraient été victimes d'une attaque informatique durant cette même année[49]. Or, selon l'Institut de la statistique du Québec, la province comptait, en décembre 2020, un total de 879 767 entreprises[50]. Ainsi, en appliquant la moyenne nationale d'incidents de sécurité, il nous est possible d'estimer qu'environ 709 972 entreprises québécoises auraient été victimes de cyberattaques en 2020, ce qui équivaut à une moyenne de plus de 1 945 incidents par jour. Ainsi, à la lumière de ce qui précède, seule une entreprise sur 3 890 aurait respecté son obligation de divulgation des incidents de sécurité depuis l'entrée en vigueur de l'article 3.5 de la LPRPSP. La norme serait donc peu respectée.

---

48 Claude Fluet et Roberto Galbiati, « Lois et normes : les enseignements de l'économie comportementale », (2016) 92 *Actual. Econ.* 191, 193.

49 Cyberedge Group, « Cyberthreat Defense Report 2020 », 2020, p. 7, en ligne : <https://www.imperva.com/resources/resource-library/reports/2020-cyberthreat-defense-report/> (consulté le 14 avril 2023).

50 Institut de la statistique du Québec, « Nombre d'entreprises actives au Québec en décembre 2020 », 19 mai 2021, en ligne : <https://statistique.quebec.ca/fr/document/nombre-entreprises-actives-quebec> (consulté le 14 avril 2023).

Évidemment, notre calcul demeure très approximatif. D'une part, la méthodologie de CyberEdge ne précise pas la taille de l'échantillon[51]. L'entreprise souligne d'ailleurs dans l'édition 2021 de leur même étude que « all results pertaining to individual industries and countries should be viewed as anecdotal as their sample sizes are much smaller »[52]. Ensuite, ces chiffres présument une distribution normale à travers le pays et ignorent le fait que certaines entreprises établies au Québec ne sont pas soumises à l'application de la LPRPSP[53]. Finalement, nos projections présument que toute attaque informatique se traduit en un incident de confidentialité, ce qui n'est pas le cas.

Toutefois, même en rejetant notre analyse, les arguments voulant que le nombre réel d'incidents de sécurité depuis l'entrée en vigueur de l'article 35.1 de la LPRPSP est plus élevé que ce qui a été rapporté à la Commission d'accès à l'information (et donc que le niveau d'effectivité de l'obligation de divulgation est faible) demeurent convaincants. D'abord, les statistiques générées par CyberEdge visent les cyberattaques identifiées et ignorent de ce fait les incidents n'ayant aucun lien avec les systèmes informatiques. Pourtant, ces incidents semblent représenter une proportion non négligeable des cas communiqués à la Commission d'accès à l'information en 2022[54]. Quant aux attaques informatiques, notons que – selon le département de la justice américain – 85 % de celles-ci demeurent indétectées[55]. Cela ne surprend pas dans la mesure où, selon une étude de l'Université du Maryland, un système informatique est attaqué en moyenne une fois à toutes les 39 secondes[56]. Évidemment, une majorité de ces attaques échoue, mais comme un rapport produit par IBM fixe à 277 jours le délai moyen

51 Notons toutefois que, dans l'édition subséquente de l'étude, il est indiqué que 1 200 experts en sécurité représentant 17 pays et 19 industries ont été consultés. Voir : Cyberedge Group, préc., note 9, p. 61.

52 *Id.*

53 Rappelons en effet que cette loi ne s'applique pas aux « entreprises ou secteurs d'activité qui relèvent de la compétence législative du Parlement [du Canada] » : *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 23, art. 2 et 30(1).

54 H. Joncas, préc., note 13.

55 U.S. Department of Justice, « Report of the Attorney General's Cyber Digital Task Force », 2 juillet 2018, en ligne : <https://www.justice.gov/archives/ag/page/file/1076696/download> (consulté le 14 avril 2023).

56 Michel Cukier, « Study : Hackers Attack Every 39 Seconds », *University of Maryland*, 9 février 2007, en ligne : <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds> (consulté le 14 avril 2023).

avant qu'une attaque ne soit détectée et neutralisée[57], cela pourra prendre plusieurs mois avant qu'une entreprise ne soit à même d'évaluer les dommages causés à la suite d'un incident de sécurité précis et, donc, la pertinence d'en aviser la Commission d'accès à l'information.

Finalement, notons que bien que les données utilisées pour notre analyse datent de 2020, les statistiques indiquent une hausse générale des cyberattaques en 2021[58], ce qui devrait se traduire par une hausse des incidents de sécurité et, donc, de confidentialité.

Ainsi, il semble fort probable que le nombre d'incidents déclarés à la Commission d'accès à l'information représente une fraction du nombre réel d'incidents, ce qui nous ramène à nous questionner sur les causes de cette apparente ineffectivité de l'obligation de divulgation des incidents de sécurité. Comme, tel qu'indiqué ci-haut, l'étude de l'effectivité du droit vise notamment à retracer les rationalités des individus lorsqu'ils rejettent un modèle normatif et comme ce rejet sera influencé par la probabilité de détection des infractions et la sévérité des sanctions, la réponse à notre interrogation se trouve potentiellement dans l'analyse de ces deux éléments.

A. La probabilité de détection des infractions

Tel que prévu à l'article 3.5 de la LPRPSP, pour être en infraction, une entreprise doit avoir « des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient », considérer que « l'incident présente un risque qu'un préjudice sérieux soit causé » et ne pas en aviser la Commission d'accès à l'information, ainsi que « toute personne dont un renseignement personnel est concerné par l'incident ».

Pour illustrer la principale problématique liée à cette obligation, prenons l'exemple suivant :

> Le 17 janvier 2007, TJX[1] et Visa ont informé le Commissariat à la protection de la vie privée du Canada (CPVP) et le Commissariat à l'information et à la protection de la vie privée de l'Alberta (CIPVP) que le réseau informatique

[57] IBM, « Rapport 2022 sur le coût d'une violation de données », 2022, p. 14, en ligne : <https://www.ibm.com/reports/data-breach> (consulté le 14 avril 2023).

[58] En effet, le pourcentage d'entreprises victimes de cyberattaques réussies serait passé de 80,7 % en 2020 à 86 % en 2021 : Cyberedge Group, préc., note 9, p. 7.

> de TJX avait fait l'objet d'une intrusion touchant les renseignements personnels d'environ 45 millions d'utilisateurs de cartes au Canada, aux États-Unis, à Puerto Rico, au Royaume-Uni et en Irlande.[59]

Dans les faits, l'incident aurait eu lieu à compter de juillet 2005, soit plus de 15 mois avant sa découverte en décembre 2006[60]. Si, tel que nous l'avons vu, le délai moyen avant qu'une attaque ne soit détectée et neutralisée est aujourd'hui de 277 jours[61], cela n'empêche pas que de nombreux commerces n'auront pas de « motifs de croire que s'est produit un incident de confidentialité » avant qu'il ne soit trop tard. En effet, après un aussi long délai, il est fort probable que le « préjudice sérieux » ait déjà été subi, réduisant ainsi la pertinence de l'avis dans l'esprit des destinataires. En autres mots, pourquoi risquer les conséquences réputationnelles et opérationnelles[62] d'une divulgation lorsque les externalités positives associées à celle-ci – la protection des clients contre un risque de préjudice sérieux – deviennent négligeables ? Qui plus est, dans la mesure où la définition même de ce qu'est un risque de préjudice sérieux demeure nébuleuse, la décision de ne pas divulguer un événement découvert plusieurs mois après son avènement peut paraître rationnelle pour certains.

De plus, même si un préjudice sérieux est subi, il s'avèrera souvent particulièrement complexe pour la Commission d'accès à l'information, ou une éventuelle victime, de démontrer que celui-ci est causé par un événement survenu chez une entreprise donnée. En effet, tel que nous l'avons indiqué ailleurs[63], le lien de causalité entre un incident de sécurité et le préjudice causé par un individu est difficile à établir dans la mesure où les renseignements personnels des Québécois sont détenus pas des dizaines (sinon des centaines) d'entreprises, dont plusieurs peuvent faire l'objet d'incidents de sécurité durant une même période. Ainsi, à moins qu'une entreprise ne fasse preuve de parfaite transparence, il sera souvent difficile de prétendre qu'elle est responsable des dommages causés.

---

59 Commissariat à la protection de la vie privée du Canada et Commissariat à l'information et à la protection de la vie privée de l'Alberta, *Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels*, 2007 CanLII 41283 (25 septembre 2007), par. 1.

60 *Id.*, par. 11 et 17.

61 IBM, préc., note 57, p. 14.

62 U.S. Department of Justice, préc., note 55, p. 89.

63 N. Vermeys, préc., note 15, à la p. 94.

Finalement, mentionnons un élément crucial quant à la probabilité de détection des infractions : le sous-financement de la Commission d'accès à l'information. Rappelons que les modifications apportées au cadre juridique applicable à la protection des renseignements personnels au Québec par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* imposent un fardeau important sur les commissaires œuvrant au sein de la Commission. En effet, « [d]evant les nouvelles responsabilités qui lui sont confiées, la Commission doit mettre à jour ses processus, ses outils de travail et la documentation disponible à l'intention des organisations »[64]. Or :

> [L]e budget supplémentaire de 1,5 million de dollars accordé à la Commission pour le prochain exercice financier, soit 25 % du montant qu'elle estimait nécessaire pour la mise en œuvre de cette réforme l'an prochain, n'est pas suffisant. Il ne lui permettra pas d'opérer en temps opportun tous les changements requis par les nouvelles responsabilités qui lui sont confiées et de répondre aux attentes des parlementaires, des organisations et des citoyens.[65]

Une norme ne peut être effective si elle n'est pas appliquée et ne peut être appliquée si l'organisme chargé de son application n'a pas les budgets et les effectifs nécessaires pour ce faire[66], peu importe la sévérité des sanctions, élément que nous aborderons maintenant.

B. La sévérité des sanctions

La sévérité des sanctions associées au non-respect de l'obligation de divulgation des incidents de sécurité est avérée. En effet, l'article 90.12 de la *Loi sur la protection des renseignements personnels dans le secteur privé* prévoit l'imposition d'amendes administratives pouvant atteindre « 50 000 $ dans le cas d'une personne physique et, dans les autres cas, de 10 000 000 $ ou du montant correspondant à 2 % du chiffre d'affaires mondial de l'exer-

---

64 Commission d'accès à l'information du Québec, « Dépôt du Rapport annuel 2021-2022 : Une année marquée par une réforme historique », 9 décembre 2022, en ligne : <https://www.cai.gouv.qc.ca/depot-du-rapport-annuel-2021-2022-une-annee-marquee-par-une-reforme-historique/> (consulté le 14 avril 2023)

65 *Id.*

66 Notons que la Commission compte présentement 9 membres et gère un budget de 8 259 900 $. Voir Commission d'accès à l'information du Québec, « Rapport annuel d'activités et de gestion 2021-2022 », novembre 2022, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RAG_2021-2022.pdf> (consulté le 14 avril 2023).

cice financier précédent si ce dernier montant est plus élevé », alors que l'article 91 de la Loi prévoit des amendes pénales « de 5 000 $ à 100 000 $ dans le cas d'une personne physique et, dans les autres cas, de 15 000 $ à 25 000 000 $ ou du montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé ». Notons toutefois que ces sanctions n'entreront en vigueur qu'en septembre 2023[67]. C'est donc dire que, pour l'instant, ces sanctions sont plutôt hypothétiques. Or, comme la forme des avis d'incidents de confidentialité, telle que dictée par le *Règlement sur les incidents de confidentialité*[68], impose un exercice pouvant exposer certaines informations sensibles sur les pratiques de l'entreprise visée en plus de s'avérer dispendieux et relativement chronophage[69], il n'est pas surprenant que les entreprises soumises à la LPRPSP ne s'empressent pas à publiciser leurs incidents de sécurité et, par le fait même, à subir les conséquences réputationnelles et opérationnelles[70] d'une telle divulgation.

Conclusion

Il nous est difficile de rédiger une conclusion pour la présente chronique puisque, tel que nous l'avons annoncé en introduction, nous nous étions fixé comme objectif l'élaboration d'hypothèses qu'il ne nous sera envisageable de valider qu'après une analyse quantitative plus poussée et dépassant le simple décompte du nombre d'avis d'incidents de confidentialité transmis à la Commission d'accès à l'information sur une courte période. Ainsi, la première de ces hypothèses, à savoir que la faible probabilité de détection des infractions incite les entreprises à ignorer leurs obligations, ne pourra être validée que par une étude empirique. Quant à l'hypothèse voulant que l'absence – pour l'instant – de sanctions nuise

67 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, préc., note 13, art. 175.

68 *Règlement sur les incidents de confidentialité,* (2022) 154 G.O.Q. II 3935.

69 La procédure est disponible sur le site de la Commission d'accès à l'information : <https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/aviser-commission-et-personnes/>. Notons que le formulaire d'« 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 » (en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_FO_avis_incident_confidentialite.pdf>) compte à lui seul 11 pages (consultés le 14 avril 2023).

70 U.S. Department of Justice, préc., note 55, p. 89.

également à l'effectivité de la norme, la réaction des destinataires à l'entrée en vigueur des nouvelles dispositions pénales de la LPRPSP viendra confirmer ou infirmer celle-ci. Dans la même veine, il sera intéressant de documenter si le passage du temps aura une incidence positive sur l'effectivité de l'obligation de divulgation des incidents de sécurité puisque, bien que nous n'y ayons pas fait directement référence dans le cadre de notre analyse, il est également possible que cette obligation demeure inconnue pour une majorité d'entreprises œuvrant en sol québécois d'autant que, est-il utile de le rappeler, cette obligation n'existe que depuis quelques mois. Or, l'effectivité dépendra notamment de « la connaissance dont la norme juridique fait l'objet »[71]...

[71] D. Gesualdi-Fecteau et M. Visotzky-Charlebois, préc., note 6, à la p. 334. Notons que ce passage réfère à l'analyse de l'usage du droit, lequel s'inscrit dans l'étude de l'effectivité : *id.*, p. 362.