Université de Montréal

L'efficacité du régime de responsabilité civile comme mesure de contrainte au respect de l'obligation de sécurité des renseignements personnels

par Isabelle Lafont

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de maîtrise en droit (LL.M.)
option droit des technologies de l'information

Novembre 2013

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

L'efficacité du régime de responsabilité civile comme mesure de contrainte au respect de l'obligation de sécurité des renseignements personnels

présenté par
Isabelle Lafont

a été évalué par un jury composé des personnes suivantes :

Nicolas W. Vermeys

Pierre Trudel

Patrice Deslauriers

RÉSUMÉ

Dans un contexte où les renseignements personnels sont aujourd'hui une « devise » commerciale importante, il importe de s'attarder à la responsabilité de leur protection. Les lois encadrant la protection des renseignements personnels imposent notamment aux entreprises du secteur privé une obligation de sécurité. Par contre, elles ne prévoient pas de sanction monétaire en cas de violation. Il faut donc se tourner vers le droit de la responsabilité civile afin de contraindre les entreprises à adopter des mesures de sécurité. Or, le régime de responsabilité civile actuel est mal adapté aux obligations associées à la sécurité des renseignements personnels. Le flou normatif entourant le contenu de l'obligation de sécurité et les difficultés d'exercice du recours rendent peu efficace le régime de responsabilité civile compensatoire. Dans un souci d'améliorer son efficacité, deux propositions méritent d'être considérées, soit : la revalorisation des dommages-intérêts punitifs et l'encadrement statutaire d'une obligation de notification des atteintes à la sécurité des renseignements personnels. Ces deux propositions sanctionnent les violations à l'obligation de sécurité là où le régime de responsabilité civile compensatoire semble échouer. Par contre, elles ne sont elles-mêmes efficaces que si leur exercice respecte les fonctions qui leur sont sous-jacentes. Au final, la responsabilité de la sécurité des renseignements personnels ne repose pas seulement sur un régime responsabilité, mais sur une culture de responsabilité.

Mots clés: responsabilité civile, sécurité informationnelle, mesures de sécurité, protection des renseignements personnels, dommages-intérêts, dommages-intérêts punitifs, obligation de notification

ABSTRACT

In a context where personal information is today a major commercial « currency », it is important to focus on the responsibility of its protection. The laws governing the protection of personal information impose safety requirements, especially to enterprises of the private sector. On the other hand, they do not provide for monetary penalties in the case of violation. One must therefore turn to the law of civil liability in order to force enterprises to adopt security measures. However, the current regime of civil liability is ill-suited to the obligations associated with the security of personal information. The regulatory uncertainty surrounding the contents of the safety requirements and the challenges of exercising an action render the system of compensatory civil liability inefficient. In order to improve its efficiency, two proposals are worth considering, namely: the revaluation of punitive damages, and statutory guidance of an obligation to notify security breaches of personal information. Both proposals sanction violations to the safety requirements where the system of compensatory civil liability seems to fail. On the other hand, these proposals cannot be effective unless their exercise respects the functions underlying them. Finally, the responsibility for the security of personal information does not lie solely on a regime of responsibility, but rather on a culture of accountability.

Key words: civil liability, information security, security safeguards, protection of personal information, damages, punitive damages, breach notification

TABLES DES MATIÈRES

Introduction 1

TITRE I. L'INEFFICACITÉ DU RÉGIME DE RESPONSABILITÉ CIVILE COMPENSATOIRE COMME MESURE DE CONTRAINTE AU RESPECT DE L'OBLIGATION DE SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS 12

Partie A. L'échec de la fonction compensatoire du régime de la responsabilité civile 12

Sous-partie 1. Des difficultés d'exercice relatives au préjudice 13

a) L'inexistence du préjudice subi 13
b) La valeur minime du préjudice 19

Sous-partie 2. Des difficultés d'exercice relatives au lien causal 26

a) La causalité adéquate 26
b) Le partage de responsabilité 31
c) La multiplicité des causes 33

Partie B. L'échec des fonctions préventives et dissuasives incidentes du régime de responsabilité civile 36

Sous-partie 1. Une obligation de sécurité indéfinie 36

a) Les incertitudes de la « raisonnabilité » 37
b) L'augmentation de l'intensité de l'obligation 44
(i) Une obligation de résultat, en théorie 45
(ii) Une obligation de résultat, en pratique 48

Sous-partie 2. Un risque insignifiant.....53

a) Un risque économique insignifiant.....53
b) Un risque « réputationnel » insignifiant.....54
(i) L'insuccès des fonctions préventives et dissuasives de la responsabilité civile.....55
(ii) L'absence d'obligation de notification.....55
(iii) Les individus désintéressés.....58

TITRE II. VERS UN RÉGIME DE RESPONSABILITÉ CIVILE PLUS EFFICACE.....61

Partie A. Les dommages-intérêts punitifs.....61

Sous-partie 1. Les fonctions des dommages-intérêts punitifs.....64

a) La prévention.....65
b) La dissuasion.....67
c) La punition.....69
d) La dénonciation.....69
e) Les autres fonctions.....71

Sous-partie 2. L'exercice du recours dommages-intérêts punitifs dans le cadre d'une atteinte à la sécurité des renseignements personnels.....74

a) Les dispositions législatives fondant l'exercice du recours.....74
b) Les conditions d'ouverture.....80
(i) L'atteinte illicite.....84
(ii) L'atteinte intentionnelle.....86
(iii) Les autres conditions.....91
c) L'évaluation du quantum.....94
(i) La gravité du comportement fautif.....95
(ii) La situation financière du fautif.....96

Partie B. L'obligation de notification 101

Sous-partie 1. Les fonctions de l'obligation de notification 104

a) La mitigation des dommages 105
b) L' « accountability » 109
c) L'adoption de mesures préventives 110
d) Le développement des connaissances 114

Sous-partie 2. Les modalités de l'obligation de notification 116

a) Le débiteur de l'obligation 116
b) Le créancier de l'obligation 120

Sous-partie 3. Les sanctions 125

Conclusion 136

TABLES BIBLIOGRAPHIQUES 140

LISTE DES SIGLES ET ABRÉVIATIONS

ACCJE	Association canadienne des conseillers (ères) juridiques d'entreprises
Akron Intell. Prop. J.	Akron Intellectual Property Journal
B.F.L.R.	Banking & Finance Law Review
Brook. J. Corp. Fin.&Com. L.	Brooklyn Journal of Corporate, Financial and Commercial law
C.A.	Cour d'appel
CAI	Commission d'accès à l'information
CAF	Cour d'appel fédérale
Cal. L. Rev.	California Law Review
CAN/CSA	Association canadienne de normalisation/Canadian Standard Association
Can. J.L. & Tech	Canadian Journal of Law and Technology
C.c.Q.	Code civil du Québec
CF	Cour Fédérale
CISAC	Center for International Security and Cooperation
C.Q.	Cour du Québec
CNIL	Commission Nationale de l'Informatique et des Libertés
C.S.	Cour Supérieure
DCL	Droit civil en ligne
DIC	Disponibilité, Intégrité, Confidentialité
D.T.E.	Droit du travail express
G29	Groupe de travail « Article 29 »
GPS	Global Positioning System
GSM	Global System for Mobile Communications
Hastings L.J.	Hastings Law Journal
Hous. L. Rev.	Houston Law Review
IEEE	Institute of Electrical and Electronic Engineers
J.E.	Jurisprudence express
J.Q.	Jugements du Québec
J. Pol. Anal. Manage.	Journal of Policy Analysis and Management
L.C.	Lois du Canada
L.Q.	Loi du Québec
L.R.C.	Lois révisés du Canada
L.R.Q.	Lois refondus du Québec
LCCJTI	Loi concernant le cadre juridique des technologies de l'information
L.G.D.J.	Librairie Générale de Droit et de Jurisprudence
LPRPDE	Loi sur la protection des renseignements

	personnels et les documents électroniques
LPRPSP	Loi sur la protection des renseignements personnels dans le secteur privé
McGill L.J.	McGill Law Journal
Mich. L. Rev.	Michigan Law Review
Mich. St. J. Int'l L	Michigan State University College of Law Journal of International Law
NPD	Nouveau parti démocratique
OCDE	Organisation de coopération et de développement économiques
OIPC	Office of the Information and Privacy Commissioner
PIAC	Public Interest Advocacy Center
PIPA	Personal Information Protection Act
PCI DSS	PCI Data Security Standard
R. du B.	Revue du Barreau
R.C.S.	Recueil des arrêts de la Cour Suprême
R.D.U.S.	Revue de droit de l'Université de Sherbrooke
R.J.Q.	Revue juridique du Québec
R.J.T.	Revue juridique Thémis
R.L.	Revue Légale
RSI	Responsable de la Sécurité Informationnelle
SBNL	Security Breach Notification Laws
W. New Eng. L.Rev.	Western New England Law Review
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Introduction

Au quotidien, le traitement des renseignements personnels[1] est au cœur de nos activités sociales et commerciales. Dès le moment où nous quittons la maison, que nous utilisions les transports en commun ou la voiture pour nous rendre au travail, le traitement des renseignements personnels est déjà amorcé : géolocalisation par les réseaux GSM, Wifi et GPS, dans la voiture ou le téléphone intelligent. Il en va ainsi pour le reste de la journée : le lunch du midi, payé par carte débit ou crédit à puce; l'achat de biens ou services après le boulot, moyennant la communication de certains renseignements : nom, adresse, numéro de téléphone, adresse courriel, numéro de carte, date expiration, numéro de validation, numéros d'identification, numéro de permis de conduire, etc. Pourquoi ? Mais pour mieux nous servir!

De façon plus ou moins consciente, nous sommes prêts à échanger nos renseignements personnels afin d'obtenir des biens et services, peu importe leur valeur. Cependant, la circulation des renseignements personnels n'a pas que des avantages. Un traitement déficient de ces renseignements peut entraîner des conséquences négatives variées telles le vol d'identité, la fraude bancaire, le refus, la perte ou la diminution de son crédit, la diffamation, l'humiliation, l'embarras et la gêne, la perte d'opportunités, etc.

Nos renseignements personnels ont une valeur évidente pour les entreprises, mais les protègent-elles? Dans un marché commercial compétitif, elles auraient plutôt tendance à

---

[1] D'après Le grand dictionnaire terminologique de l'Office québécois de la langue française, les termes « renseignements personnels » sont définis comme étant des « renseignements portant sur un individu et permettant d'établir son identité », en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8398805 (consulté le 8 octobre 2012). L'article 2 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5 (« **LPRPDE** ») définit le « renseignement personnel » comme étant : « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail ». L'article 2 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1 (« **LPRPSP** ») définit l'expression comme suit : « est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier ». Nous ne traiterons pas, pour les fins de notre propos, de la définition ni de l'opportunité de réviser la définition de « renseignement personnel ». À ce sujet, nous référons le lecteur à cet ouvrage : Éloise GRATTON, **Understanding Personal Information: Managing Privacy Risks**, Markham, Ont., LexisNexis, 2013. Nous utiliserons la définition de l'article 2 de la LPRPSP pour nos fins.

choisir la libre circulation de renseignements plutôt que leur sécurité[2]. Or, tel que l'a souligné Jennifer Stoddart, Commissaire à la protection de la vie privée du Canada, les entreprises doivent intégrer la sécurité dans l'élaboration de chacun de leurs produits et services :

> « Les renseignements personnels sont devenus une devise importante dans l'économie actuelle. Les gens sont prêts à échanger une certaine quantité d'information pour obtenir les produits et les services qu'ils désirent. Mais cet échange doit être mesuré et juste. »[3]

La protection des renseignements personnels devient donc un enjeu important dans la poursuite des activités économiques et sociales de notre société. Avant d'échanger nos renseignements personnels, ne devrions-nous pas nous attarder à leur protection?

Cette question est étudiée sérieusement au moins depuis 1980, année au cours de laquelle l'Organisation de Coopération et de Développement Économique (« OCDE ») a énoncé huit (8) principes directeurs qui exercent encore aujourd'hui une influence majeure dans le domaine. Ces principes encadrent le traitement des renseignements personnels par les organisations, soit par : (1) la limitation de leur collecte, (2) la spécification de leurs finalités, (3) la transparence, (4) la participation des individus, (5) la responsabilité, (6) la limitation de leur utilisation, (7) la qualité des données collectées et (8) les garanties de sécurité[4].

---

[2] Kevin J. SOO HOO, « How much is enough? A Risk-Management Approach to Computer Security », (2000) *CISAC* 13, 3, en ligne: http://iis-db.stanford.edu/pubs/11900/soohoo.pdf (dernières modifications: août 2001)

[3] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Discours : Sécurité et protection de la vie privée : protéger l'information dans un monde transparent*, 1er juin 2011, Jennifer Stoddart, p.5, en ligne : http://www.priv.gc.ca/media/sp-d/2011/sp-d_20110601_f.asp (consulté le 7 juillet 2012). Voir aussi : Christian E. GIDEON, « A new approach to Data Security Breaches», (2009) 7 *Can. J.L. & Tech.* 149, 165 : « Arising from the relationship between a bank and its customer is a responsibility on the part of the bank to safeguard its clients' personal information. Failure to do this might give rise to an action for breach of fiduciary duty. The customer has a right to expect that personal information divulged in confidence, in a business or similar transaction, will be guarded with the utmost care. In addition, looking at the issue from a control standpoint, the organization in custody of the personal information is in the best position to protect such information from unauthorized access. »

[4] ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE (« OCDE »), *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontaliers des données à caractère personnel*, 23

Tous ces principes, interdépendants, visent à assurer la protection des renseignements personnels par les organisations. L'absence de l'un d'entre eux affaiblit l'atteinte de cette finalité qu'est la protection des renseignements personnels. Pourtant, pour les raisons exposées ci-après, l'un d'eux nous semble plus important que les autres : les garanties de sécurité. D'une part, il s'agit une exigence essentielle. En effet, même si la collecte des renseignements est limitée, que les renseignements ne sont utilisés qu'à une fin particulière et que l'individu concerné a consenti à leur collecte, de façon libre et éclairée, ses renseignements ne seront pas protégés si quiconque peut y accéder sans autorisation. D'autre part, le principe des garanties de sécurité est une exigence englobante. Elle implique de considérer tous les autres principes dans un contexte organisationnel. La protection des renseignements personnels ne sera assurée que si leur traitement est encadré par les organisations, de leur collecte à leur destruction, par des politiques et des procédures de sécurité qui considèrent chacun des autres principes. De fait, en 2002, la publication des *Lignes directrices de l'OCDE régissant la sécurité des systèmes et des réseaux d'information* a confirmé que la sécurité n'était pas qu'un principe incident, mais un principe essentiel dans tout environnement fonctionnant en réseau[5]. Ces Lignes directrices visent à développer une véritable « culture de la sécurité »[6].

En quoi consiste ce principe de sécurité ? La sécurité des renseignements personnels s'inscrit dans le concept plus englobant de la « sécurité informationnelle ». Cette dernière consiste en la « protection des ressources informationnelles d'une organisation, face à des risques identifiés, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la

---

septembre 1980, en ligne : http://www.oecd.org/fr/internet/economiedelinternet/lignesdirectricesdelocdesurlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm (consulté le 8 octobre 2012)

[5] OCDE, Lignes directrices de l'O.C.D.E. régissant la sécurité des systèmes et réseaux d'information- Vers une culture de la sécurité, 25 juillet 2002, en ligne :http://www.oecd.org/sti/interneteconomy/15582260.pdf (consulté le 8 octobre 2012)

[6] *Id*. Ces *Lignes directrices* énoncent neuf grands principes, soit : (1) la sensibilisation de toutes les parties prenantes (les gouvernements, les entreprises, les autres organisations et les individus)[6], (2) leur responsabilité, (3) leur réactivité aux incidents de sécurité, (4) leur éthique, (5) la démocratie, (6) l'évaluation des risques, (7) la conception et la mise en œuvre de la sécurité par les parties prenantes, (8) la gestion de la sécurité, et (9) la réévaluation de la sécurité des systèmes.

confidentialité, l'intégrité et la disponibilité de l'information traitée » (soulignements ajoutés)[7].

La sécurité informationnelle implique de protéger ces trois composantes de l'information (disponibilité, intégrité et confidentialité), collectivement connues sous le vocable « triade DIC »[8]. Brièvement, la protection de la confidentialité de l'information implique que seules les personnes autorisées y ont accès[9]. La protection de l'intégrité de l'information implique que l'information est complète et qu'elle n'est pas altérée[10]. Enfin, la protection de la disponibilité de l'information implique que l'information est accessible lorsque nécessaire, pour les personnes qui y ont un droit d'accès[11].

Cette protection s'opère en utilisant des mesures de sécurité, également désignées par le vocable « contre-mesures ». Celles-ci constituent l'ensemble des mesures qui visent à prévenir, détecter, dissuader, empêcher ou retarder l'exploitation des vulnérabilités dans un système de sécurité et, le cas échéant, d'y répondre, de corriger le dommage et de récupérer l'information[12]. Ces mesures sont de nature administrative (politiques et procédures), physique et environnementale (clôtures, portes, serrures, caméras de surveillance, etc.) et informatique (mot de passe, anti-virus, protocole SSL, coupe-feu, chiffrement, etc.). Idéalement, ces mesures sont cumulatives dans un environnement donné[13]. Elles visent à protéger les renseignements personnels contre différents types d'atteintes, par exemple contre certaines interventions humaines non autorisées[14].

---

[7] Voir Nicolas W. VERMEYS, *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010, p. 4 citant l'OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, préc., note 1

[8] K. SOO HOO, préc., note 2. Voir aussi : N. W. VERMEYS, préc., note 7, p. 24-33, pour une explication détaillée de ces caractéristiques. Certains auteurs ajoutent d'autres composantes à l'information, telle l'authenticité, l'authentification, la non-répudiation, la fiabilité, etc. Ces ajouts soulèvent d'autres questions : ces composantes sont-elles des propriétés à part entière, sont-elles inhérentes à la triade ou qualifient-elles la triade? Le législateur québécois a choisi de s'en tenir aux composantes de la triade (voir l'art. 26 de la *Loi concernant le cadre juridique des technologies de l'information*, LRQ, c C-1.1 (« **LCCJTI** »)). À notre avis, l'objectif de la sécurité informationnelle étant de tendre vers un idéal de confiance, il y aurait lieu d'interpréter les composantes de la triade largement afin d'assurer le plus haut degré de confiance possible.

[9] N. W. VERMEYS, préc., note 7, p. 23-33

[10] *Id.*

[11] *Id.*

[12] Éric LACHAPELLE et René ST-GERMAIN, « Protection des actifs informationnels », dans Abdelhaq ELBEKKALI, *Gouvernance, audit et sécurité des TI*, Brossard, CCH, 2008, p. 315 et suiv.

[13] Vincent GAUTRAIS, « Les aspects relatifs à la sécurité », dans Éric LABBÉ, Daniel POULIN, François JACQUOT et Jean-François BOURQUE (dir.), *Le Guide juridique du commerçant électronique*, Montréal,

Les principes précités, énoncés par l'OCDE, ont donné naissance au cadre législatif de la sécurité informationnelle que nous connaissons aujourd'hui. Au Québec, les entreprises du secteur privé ont l'obligation légale de prendre des mesures de sécurité raisonnables afin de protéger les renseignements personnels qu'elles traitent. Cette obligation découle d'abord de certaines dispositions des lois, tant fédérales que provinciales, relatives à la protection des renseignements personnels.

En ce qui concerne la législation fédérale, précisons que les principes de 1980 énoncés par l'OCDE ont inspiré l'Annexe 1 de la *Loi* [fédérale] *sur la protection des renseignements personnels et documents électroniques* (« **LPRPDE** »)[15]. Par ailleurs, soulignons l'article 4.7 du *Code type sur la protection des renseignements personnels* (« Code type ») [16] lequel prévoit que les « organisations » doivent protéger « les renseignements personnels […] au moyen de mesures de sécurité correspondant à leur degré de sensibilité » (soulignements ajoutés). Ces mesures doivent protéger les renseignements personnels contre :

> « la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés. » [17] (soulignements ajoutés)

Même si elles n'y sont pas spécifiquement nommées, le libellé de l'article 4.7 du Code décrit les comportements associés à chacune des trois composantes de la triade DIC. Par exemple, la perte de renseignements personnels compromet leur accessibilité et, potentiellement, leur confidentialité.

2001, p. 75-82, en ligne : http://www.jurisint.org/pub/05/fr/guide_chap3.pdf (consulté le 19 janvier 2011); N. W. VERMEYS, préc., note 7, p. 42 et 43

[14] Les mesures de sécurité peuvent également viser à réduire les risques d'autres types de menaces, telles que des menaces naturelles, techniques, physiques, environnementales et sanitaires et opérationnelles. Voir : N. W. VERMEYS, préc., note 7, p. 39

[15] LPRPDE, *préc*., note 1

[16] *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, annexe A à la *Loi sur la protection des renseignements personnels et les documents électroniques,* L.C. 2000, c. 5, art. 4.7 (« Code Type »)

[17] *Id.*, art. 4.7.1

En ce qui concerne la législation provinciale, soulignons l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (« **LPRPSP** »)[18], lequel prévoit que :

> « Toute personne qui exploite une entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. »[19] (soulignements ajoutés)

Les entreprises doivent également s'assurer que les renseignements qu'elles traitent sont à jour et exacts[20], ce qui implique d'en préserver l'intégrité. Elles doivent également s'assurer que les renseignements peuvent être consultés par les personnes autorisées, ce qui implique d'en protéger la confidentialité et la disponibilité[21].

Précisions que la LPRPSP est considérée « essentiellement similaire » à la LPRPDE[22]. Cela signifie que le mécanisme de protection des renseignements personnels de la loi québécoise est conforme et équivalent à celui de la LPRPDE et aux dix principes de l'Annexe 1 de la LPRPDE. Ainsi, les entreprises assujetties à la LPRPSP sont exemptées de l'application de la LPRPDE quant au traitement des renseignements personnels au Québec. La LPRPDE continue toutefois de s'appliquer aux entreprises fédérales œuvrant au Québec de même qu'au traitement des renseignements personnels à l'extérieur du Québec[23]. Pour les fins de notre propos, nous référerons à ces deux lois de temps en autres indistinctement afin d'étudier, au sens large, l'obligation de sécurité des renseignements personnels.

---

[18] LPRPSP, *préc.*, note 1
[19] LPRPSP, art. 10
[20] LPRPSP, art. 11
[21] LPRPSP, art. 27
[22] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE (**«COMMISSARIAT»**), *Rapport au Parlement relativement aux lois provinciales essentiellement similaires*, juin 2003, en ligne : http://www.priv.gc.ca/leg_c/legislation/leg-rp_030611_f.asp (consulté le 8 octobre 2012)
[23] COMMISSARIAT, « Renseignements juridiques associés à la LPRPDE », *Loi provinciales essentiellement similaires à la loi fédérale*, en ligne : http://29717.vws.primus.ca/legislation/ss_index_f.cfm (consulté le 8 octobre 2012)

Enfin, l'obligation légale des entreprises de prendre des mesures de sécurité raisonnables afin de protéger les renseignements personnels découle également de certaines dispositions de la LCCJTI [24]. En effet, l'article 25 LCCJTI prévoit, dans le contexte de la conservation de renseignements confidentiels[25], que :

> « La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.
>
> Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue par la loi relativement à la conservation du document.» [26] (Soulignements ajoutés)

Par ailleurs, l'article 26 LCCJTI prévoit que :

> « Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance.
>
> Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même

[24] LCCJTI, préc., note 8
[25] La protection des renseignements confidentiels inclut normalement la protection des renseignements personnels. Voir : N. W. VERMEYS, préc., note 7, p. 28-31
[26] LCCJTI, art.25

assurer le respect de toute autre obligation prévue par la loi relativement à la conservation du document. » (soulignements ajoutés)

Enfin, mentionnons que l'article 19 LCCJTI prévoit l'obligation, pour la personne qui conserve un document, d'en préserver l'intégralité, l'accessibilité et l'intelligibilité. Par ailleurs, l'article 34 LCCJTI prévoit que la confidentialité des renseignements doit être protégée lors de leur transmission.

Ces dispositions constituent le cadre législatif dans lequel l'obligation de sécurité informationnelle et, plus particulièrement, l'obligation de sécurité des renseignements personnels existe, s'interprète et s'exerce. Il impose aux entreprises d'adopter des mesures de sécurité « raisonnables »[27], « propres à »[28] protéger les renseignements personnels qu'elles traitent, compte tenu de différents facteurs, notamment « de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support »[29]. Or, pour que cette obligation soit efficace, encore faut-il que sa violation puisse être sanctionnée.

Le régime de responsabilité civile se présente comme une des mesures juridiques afin de contraindre les entreprises à assurer la sécurité des renseignements personnels qu'elles traitent. Il prévoit une sanction monétaire en cas de violation entraînant un dommage. Les entreprises peuvent être contraintes à protéger les renseignements personnels par d'autres mesures juridiques, telles les sanctions pénales[30]. Ces dernières sont davantage punitives, c'est-à-dire qu'elles visent à punir la personne qui porte atteinte aux trois composantes de l'information précitées. Nous ne traiterons, pour les fins de la présente étude, que du régime de responsabilité civile.

Traditionnellement, le régime de responsabilité civile vise à indemniser la victime d'une atteinte et, incidemment, à prévenir et dissuader les atteintes futures à la sécurité des

[27] LPRPSP, art. 10
[28] LPRPSP, art. 10; LCCJTI, art. 25
[29] Code type, préc., note 16, art. 4.7.2; LPRPSP, art. 10
[30] Par exemple, certaines dispositions du Code criminel visent directement les crimes informatiques tels l'utilisation non autorisée d'un ordinateur (art. 342.1 C.cr.) ou le méfait concernant des données (art.430 (1.1) C.cr.).

renseignements personnels[31]. Il s'agit de compenser la victime de la perte subie ou du gain manqué[32]. Le caractère compensatoire des dommages-intérêts vise à remettre la victime dans la situation où elle était avant de subir son préjudice. La réparation doit être compensatoire, intégrale et définitive[33]. C'est par sa fonction compensatoire que le régime de responsabilité civile accomplit ses autres fonctions, c'est-à-dire la prévention et la dissuasion de comportements socialement répréhensibles[34].

En étant responsable du dommage qu'elle cause à autrui, une entreprise évitera de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des renseignements qu'elle traite, en prenant des mesures de sécurité raisonnables afin de les protéger. Dans le cas contraire, si elle omet d'adopter des mesures de sécurité raisonnables, elle pourrait bien être tenue responsable du préjudice subi. L'utilisation du conditionnel est ici volontaire et d'importance. En effet, pour que la responsabilité civile d'une entreprise soit engagée, encore faut-il que la victime de l'atteinte prouve, selon la balance des probabilités[35], trois conditions cumulatives et essentielles[36], à savoir : l'existence d'une faute, d'un dommage et d'un lien causalité entre la faute et le dommage[37]. En pratique, nous verrons que la preuve de ces trois conditions n'est pas triviale dans le contexte de la sécurité des renseignements personnels traités par les entreprises privées.

Les ouvrages au sujet de la responsabilité civile des entreprises en matière de sécurité informationnelle sont rares. Au Québec, le professeur Nicolas W. Vermeys, professeur à la Faculté de droit de l'Université de Montréal, a étudié la responsabilité civile du responsable de la sécurité informationnelle (« RSI ») dans son ouvrage intitulé « Responsabilité civile et sécurité informationnelle ». Plus particulièrement, le professeur Vermeys s'est intéressé aux dispositions législatives et aux principes jurisprudentiels et

---

[31] Au sujet des fonctions de la responsabilité civile, voir : Ejan MACKAAY et Stéphane ROUSSEAU, *Analyse économique du droit*, 2e éd., Montréal, Éditions Thémis, 2008, par. 1161-1175. Pour une définition des fonctions préventives et dissuasives, voir *infra*, p.65-68

[32] C.c.Q., art. 1611

[33] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, *La responsabilité civile, Volume I- Principes généraux*, 7e édition, Cowansville, Éditions Yvon Blais, 2007, no 1-359, p. 362

[34] *Id.*, no 1-12, p.7 et 8

[35] C.c.Q., art. 2804

[36] Abstraction est faite, pour les fins du présent texte, de la condition préliminaire qu'est la faculté de discernement. Nous présumons que cette exigence est remplie pour la quasi-totalité des personnes ayant accès à l'information. Voir: J.-L. BAUDOUIN et P. DESLAURIERS, préc., note 33

[37] C.c.Q., art. 1457.

coutumiers qui constituent le cadre juridique dans lequel l'obligation de sécurité informationnelle existe, s'interprète et s'exerce.

Au-delà du cadre juridique, dans un contexte où les individus commencent à ressentir un « certain malaise » à l'égard des pratiques des entreprises en matière de sécurité des renseignements personnels[38], la question de l'efficacité du régime de responsabilité civile comme mesure de contrainte juridique se pose avec acuité.

Le présent texte se veut donc une continuité de la réflexion amorcée par le professeur Vermeys, en proposant d'analyser l'efficacité du régime de responsabilité civile au regard de ses difficultés d'exercice, dans le contexte de la sécurité des renseignements personnels.

Dans la première partie de ce texte, nous chercherons à évaluer l'efficacité du régime, tant de la perspective de la victime que de celle de l'entreprise eut égard aux fonctions et aux conditions du régime. Dans le premier cas, nous étudierons le traitement jurisprudentiel relatif ou applicable (par analogie) aux atteintes à la sécurité des renseignements personnels. Nous verrons que les victimes rencontrent certaines difficultés dans l'exercice de leur recours. Ces dernières réduisent l'efficacité de la fonction compensatoire du régime. Ceci nous amènera à considérer l'efficacité du régime à l'égard des entreprises. Nous étudierons l'obligation de sécurité des entreprises eut égard à la fonction préventive du régime. En effet, le contenu de l'obligation nous semble étroitement lié à l'efficacité du régime. Nous verrons que le caractère actuellement indéfini de l'obligation de sécurité incite peu les entreprises à adopter des mesures de sécurité raisonnables afin de protéger les renseignements personnels qu'elles traitent. Par

[38] Selon une étude récente, deux tiers des Canadiens sont relativement préoccupés par la protection de leur vie privée : Phoenix Strategic Perspectives, *Rapport final, Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée*, janvier 2013, en ligne : http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_f.pdf (consulté le 27 août 2013); MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, Benoît DUPONT, *Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec*, Septembre 2008, p. 23, en ligne : http://www.benoitdupont.net/sites/www.benoitdupont.net/files/vol_identite%20MSP_0.pdf (consulté le 6 juillet 2012) : selon cette étude, seulement 22% des consommateurs ont confiance dans le contrôle de la cybercriminalité des entreprises offrant des biens et services; COMMISSARIAT, *Donner aux petites entreprises les moyens de protéger les renseignements personnels de leurs clients contre les menaces en ligne de plus en plus nombreuses et le scepticisme croissant des consommateurs*, Communiqué, 18 octobre 2011, p. 1, en ligne : http://www.priv.gc.ca/media/nr-c/2011/nr-c111018_f.cfm (consulté le 9 novembre 2011)

ailleurs, les difficultés rencontrées par les victimes ont également une incidence sur l'efficacité du régime à l'égard des entreprises, en ce qu'il ne peut accomplir ses fonctions préventives et dissuasives incidentes.

Dans la seconde partie de ce texte, nous étudierons différentes pistes de solution afin de bonifier le régime de responsabilité civile et en rétablir les fonctions préventives et dissuasives. Dans un premier temps, nous étudierons la possibilité d'améliorer l'efficacité du régime de responsabilité civile en favorisant le recours en dommages-intérêts punitifs. Cependant, nous constaterons que le recours en dommages-intérêts punitifs ne suffit pas à lui seul à augmenter l'efficacité du régime. Par conséquent, nous étudierons, dans un deuxième temps, l'obligation de notification des atteintes à la sécurité des renseignements en droit québécois. En effet, certaines juridictions, dont la nôtre, militent en faveur de l'introduction et l'encadrement statutaires de cette obligation dans les lois encadrant la protection des renseignements personnels. Or, cet encadrement est délicat et ne doit pas restreindre, plus que nécessaire, la libre circulation des renseignements laquelle est essentielle à la poursuite de nos activités sociales et commerciales. Au final, nous constaterons que la protection des renseignements personnels passe d'abord par un exercice équilibré des efforts préventifs que doivent faire tant les individus que les entreprises.

TITRE I L'inefficacité du régime de responsabilité civile compensatoire comme mesure de contrainte au respect de l'obligation de sécurité des renseignements personnels

Nous avons mentionné, en introduction, que les entreprises ont l'obligation légale d'adopter des mesures de sécurité raisonnables afin de protéger les renseignements personnels qu'elles traitent[39]. Au regard du régime de responsabilité civile comme mesure de contrainte juridique, cette obligation sera inefficace si l'entreprise débitrice de l'obligation « a la possibilité d'échapper à la responsabilité pour le dommage causé ou risque d'être insensible aux signaux que comporte cette responsabilité »[40].

Nous étudierons, dans la première partie de ce titre, les difficultés rencontrées par les victimes dans l'exercice de leur recours en responsabilité civile. Nous arborderons, dans la deuxième partie de ce titre, l'obligation de sécurité des entreprises. Nous constaterons que tant le caractère encore indéfini de l'obligation que les difficultés d'exercice du recours ont un impact sur l'efficacité du régime.

Ce constat nous amènera à conclure que la fonction essentiellement compensatoire du régime de responsabilité civile est inefficace et ne permet pas d'accomplir ses fonctions incidentes, soit préventives et dissuasives, nécessaires au respect de l'obligation de sécurité des renseignements personnels.

<u>Partie A</u> L'échec de la fonction compensatoire de la responsabilité civile

Nous verrons dans la présente partie que l'exercice du recours en responsabilité civile, dans le contexte de la sécurité des renseignements personnels, est pavé de difficultés quant à la preuve du préjudice et du lien de causalité. Les chances de succès du recours

---

[39] *Supra*, p. 5-8
[40] E. MACKAAY et S. ROUSSEAU, préc., note 31, p.351

et, par conséquent, l'intérêt des victimes à l'exercer afin de protéger leurs renseignements personnels s'en trouvent mitigés.

Sous-partie 1 Des difficultés d'exercice relatives au préjudice

Nos recherches nous ont permis d'identifier deux types de difficultés relatives à la preuve du préjudice lesquelles limitent l'intérêt de la victime à s'en prévaloir. D'une part, l'existence du préjudice est difficile à établir. D'autre part, lorsqu'il existe, le montant des dommages-intérêts octroyés en réparation du préjudice est peu élevé. Au final, l'atteinte à la sécurité des renseignements personnels de la victime (le dommage) existe, mais ne génère pas ou peu d'indemnisation en dommages-intérêts.

(a) L'inexistence du préjudice subi

En matière de sécurité des renseignements personnels, en dépit de l'existence d'une faute ayant entraîné un dommage, il est fréquent que la victime d'une atteinte n'en subisse aucun préjudice indemnisable.

Prenons un exemple pour illustrer notre propos: un employé d'une banque laisse un ordinateur portable contentant des renseignements personnels sur le siège arrière de sa voiture, stationnée à l'extérieur sans surveillance. La voiture n'est pas verrouillée. Aucun code ne restreint l'accès au contenu de l'ordinateur. Les données de l'ordinateur ne sont pas encryptées. Un voleur s'empare de l'ordinateur. Cependant, ce qui intéresse le voleur n'est pas le contenu de l'ordinateur, mais seulement l'ordinateur. Il n'utilise pas les données et les efface. La police ne retrace jamais le voleur ni l'ordinateur. La banque informe ses clients de l'incident.

Dans cette hypothèse, les renseignements personnels des clients de la banque et leur droit à la vie privée ont certes fait l'objet d'une atteinte. La confidentialité de leurs

renseignements a été compromise. Cependant, considérant que l'information a été effacée et n'a pas été utilisée, les clients de la banque n'en subissent et n'en subiront aucune conséquence, c'est-à-dire aucun préjudice. Sans préjudice, il n'y a pas de condamnation à des dommages-intérêts contre quiconque, ni pour le voleur (par ailleurs inconnu), ni pour l'employé fautif de la banque qui a laissé l'ordinateur portable dans sa voiture, ni pour la banque elle-même. La victime ne recevra aucune réparation parce qu'il n'y a pas de préjudice à réparer.

Certaines victimes argumenteront, ne sachant quelles sont les intentions du voleur ni ce qu'il est advenu de l'ordinateur portable, qu'elles ont dû entreprendre des démarches et qu'elles ont perdu du temps afin de mitiger leur préjudice, soit : en avisant leur(s) banques(s); en surveillant sans cesse leurs relevés de crédit afin de détecter quelque fraude que ce soit; en modifiant même leurs numéros de comptes bancaires; et en changeant leurs numéros d'identification personnel (NIP). Elles témoigneront également qu'elles ont perdu du sommeil et qu'elles vivent avec la hantise que leurs renseignements personnels puissent être utilisés à mauvais escient. Elles témoigneront qu'elles se sentent humiliées et vulnérables. Elles soumettront que tous ces inconvénients constituent un préjudice certain et indemnisable. Est-ce vraiment le cas?

Aux États-Unis, où le corpus jurisprudentiel dans le contexte d'atteintes à la sécurité des renseignements personnels est plus abondant et historiquement plus avancé qu'au Québec, les tribunaux américains ont généralement adopté une approche selon laquelle la simple crainte d'un préjudice futur ne peut faire l'objet d'une réclamation indemnisable en dommages-intérêts[41]. Dans le contexte où la victime d'une atteinte à la sécurité de ses renseignements n'a pas encore fait l'objet d'un vol d'identité ou d'une fraude, mais est seulement préoccupée par ce risque, les tribunaux américains ont tendance à considérer qu'aucun préjudice n'a encore, dans les faits, été subi. Le préjudice réclamé par la

[41] *Bell* v. *Michigan Council 25AFSCME*, 2005 Mich. App lexis 353 (Mich. Ct. App. 2005); *Stollenwerk* v. *Tri-West Healthcare Alliance*, No. Civ. 03-0185, 2005, WL 2465906 (D. Ariz. 2006) (« ***Stollenwerk*** »); *Forbes v. Wells Fargo,* 420 F. Supp. 2d 1018 (D. Minn. March 16, 2006) (« ***Forbes*** »); *Guin* v. *Brazos Higher Education Service Corp., Inc.*, No. Civ. 05-668, 2006 WL 288483 (D. Minn. 2006) (« ***Guin*** »*); Giordano* v. *Wachovia Sec.,* LLC, 2006 U.S. Dist. LEXIS 52266 (D.N.J. 2006)*; Bell* v. *Acxiom Corp.,* 2006 U.S. Dist. LEXIS 72477 (E.D. Ark. 2006)*; Randolph* v. *ING Life Insurance and Annuity Co.*, No. Civ. 06-1228 (D.D.C. 2007) (« ***Randolph*** »); *Melancon* v. *La. Office Student Fin. Assistance*, 567 F. Supp. 2d 873 (E.D. La. 2008); *Hammond* v. *The Bank of New York Mello Corp.*, 2010 U.S. Dist. LEXIS 71996; et *Resnick* v. *AvMed*., 2011 U.S. Dist. LEXIS 36686 (S.D. Fla. 2011)

victime est considéré comme futur et incertain. Dès lors, les réclamations, pour « monitoring costs » et autres inconvénients liés à la crainte du risque sont rejetées. Par exemple, dans la décision Forbes[42], la Cour de district du Minnesota souligne que:

> « The Plaintiffs' injuries are solely a result of a perceived risk of future harm. Plaintiffs have shown no present injury or reasonably certain future injury to support damages for any alleged increased risk of harm. For these reasons, Plaintiffs have failed to establish the essential element of damages[43]». (soulignements ajoutés)

Cependant, d'autres décisions américaines[44] laissent entendre qu'il pourrait en être autrement s'il était prouvé que les renseignements personnels de la victime (et non seulement ses renseignements en général) étaient ciblés par le voleur. Dans la décision *Guin*, par exemple, la Cour indique: « [...] in this case, Guin has failed to present evidence that his personal data was targeted or accessed by the individuals who bulgarized Wright's home in September 2004 » (soulignements ajoutés)[45]. Le préjudice pourrait présenter, dans ce contexte, un caractère futur suffisamment certain pour être indemnisable. Mentionnons qu'il sera difficile, voire impossible, pour la victime qui ignore l'identité même du fautif de première ligne de faire la preuve de ses intentions.

Plus récemment, en 2011, dans l'arrêt *Hannaford Brothers Co.* (« **Hannaford** »)[46], la Cour d'appel des États-Unis pour le premier circuit a renversé partiellement le jugement de première instance qui avait refusé la réclamation des demandeurs pour les coûts reliés à leurs démarches afin de mitiger leur préjudice futur. La Cour d'appel souligne :

> « It was foreseeable, on these facts, that customer, knowing that her credit or debit card data had been compromised and that thousand of fraudulent charges have resulted from the same security breach would replace the card to mitigate against misuse of the card data.

---

[42] *Forbes*, préc., note 41
[43] *Id.*, p. 1021
[44] *Stollenwerk, Guin et Randolph*, *préc*., note 41
[45] *Guin*, préc., note 41, p. 15.
[46] *In re Hannaford Bros. Co.*, 2011 WL 5007175 (C.A.1.(Me.))

[...]

> Plaintiff's claims for identity theft insurance and replacement fees involve actual financial losses from credit and debit card misuse. Under Maine contract law, these financial losses are recoverable as mitigation damages so long as they are reasonable.[47]» (soulignements ajoutés)

Par contre, il faut mentionner que les faits de l'arrêt Hannaford se distinguent des autres décisions américaines précitées. En effet, dans l'arrêt Hannaford, les numéros de carte de crédit et de débit avaient effectivement été utilisés et des sommes d'argent avaient frauduleusement été débitées des comptes bancaires des victimes. Dans ce contexte, la Cour d'appel a décidé que les démarches des demandeurs visaient à mitiger un préjudice bien réel plutôt qu'un préjudice hypothétique.

Enfin, mentionnons qu'une autre décision récente nuance également le courant qui s'est développé jusqu'à maintenant. Dans *Claridge* v. *RockYou* (« **Claridge** »), la Cour de district fédérale de Californie a rejeté certaines conclusions d'une requête en rejet, au motif que :

> « at the present pleading stage, plaintiff has suffienciently alleged general basis for harm by alleging that the breach of his PII [Personnaly Identifiable Information] has caused him to lose some ascertainable but unidentified "value " and/or property right inherent to the PII. »[48]

La décision Claridge pourrait bien marquer le début d'une évolution de la notion de « prejudice » dans la jurisprudence américaine et d'un incitatif pour les entreprises à adopter des mesures de sécurité raisonnables[49]. En attendant, elle demeure une décision marginale et les tribunaux américains continuent d'interpréter restrictivement la notion de préjudice. Ainsi, en théorie, la victime sera dans une bien meilleure situation, eut égard

---

[47] *Id.*, p.27-28
[48] *Claridge* v. *RockYou* , 2011 WL 1361588 (N.D. Cal. 2011)
[49] Gary ZHAO, « *Decisions may show trend in data breach cases* », (2011) *Chicago Daily Law Bulletin*, en ligne: http://www.salawus.com/PubsEvents/pubs/Decisions_May_Show_Trend_In_Data_Breach_Cases.pdf (consulté le 1er juillet 2013)

au succès de son recours, si elle attend qu'un ou des événements malencontreux se produisent. En pratique, cette conception est difficilement acceptable.

Au Québec, l'état du droit ne semble pas différent. Rappelons que le Code civil prévoit que les dommages-intérêts compensatoires compensent pour la perte subie[50]. Dans le cas d'un préjudice futur, ce dernier doit être certain et susceptible d'être évalué[51]. Par ailleurs, le seul fait de craindre la réalisation d'un préjudice futur n'est pas suffisant pour établir un préjudice indemnisable[52]. En l'absence de préjudice subi, il n'y aura pas de réparation.

En ce qui concerne le préjudice patrimonial, dans la décision Stacey[53], la Cour du Québec a accordé la somme de 2 000$ au demandeur représentant les frais d'avocats que ce dernier avait dû engager afin de rétablir son statut de crédit auprès de diverses sociétés. Le Tribunal a décidé que les démarches que le demandeur avait dû entreprendre pour rétablir son statut représentaient un « dommage direct » résultant des fautes commises par les défendeurs[54]. Fait à noter, dans cette affaire, l'identité du demandeur avait bel et bien été usurpée. Le demandeur avait eu connaissance de l'usurpation d'identité après qu'une entreprise de financement l'ait appelé pour lui demander la raison pour laquelle ses paiements étaient en retard. La réclamation en réparation du préjudice patrimonial n'était donc pas présentée dans le contexte de la crainte d'une usurpation d'identité future, mais bien à la suite d'une usurpation réelle. Ce raisonnement est conforme à celui de l'arrêt Hannaford, précité. Il est permis de se demander si la décision aurait été différente si Stacey avait su que son identité avait été usurpée, sans toutefois que le tiers usurpateur n'entache comme tel son crédit, soit en acquittant ses paiements à échéance. Aurait-il eu droit à des dommages pour la perte de temps et les coûts nécessaires pour vérifier son crédit, rétablir son identité et faire cesser l'utilisation non autorisée de son nom?

---

[50] C.c.Q., art. 1611 al.1.
[51] C.c.Q., art. 1611 al.2.
[52] *Hotte* c. *Servier*, [2002] R.J.Q. 230 (C.S.), citée récemment dans *F.L.* c. *Astrazeneca Pharmaceuticals LP*, 2010 QCCS 470, par. 92
[53] *Stacey* c. *Sauvé Plymouth Chrysler*, J.E. 2002-1147 (C.Q.), par. 110-112 (« **Stacey** ») Voir : *Unfasung* c. *Assouline*, EYB 2011-1890517 (C.S.) (confirmé en appel, 2013 QCCA 534) (« **Unfasung** »), où des dommages matériels au montant de 5, 373.77$ ont été octroyés à la suite du vol d'identité de la demanderesse par son amie d'enfance.
[54] *Id*.

En ce qui concerne le préjudice extrapatrimonial, dans la décision Wellman[55], le demandeur Wellman et la demanderesse Houde poursuivaient le ministère du Revenu du Québec pour avoir publié, dans une citation à comparaître, sans leur autorisation, leur code permanent et divers numéros correspondant aux folios de leurs comptes bancaires. Ils réclamaient la somme de 325 000$. Le demandeur Wellman prétendait craindre que des personnes mal intentionnées accèdent aux différents comptes bancaires le concernant pour y effectuer des transactions non autorisées. La Cour supérieure a noté que cette éventualité (les transactions non autorisées) ne s'était pas produite. Il n'y avait donc pas lieu d'accorder de dommages-intérêts. Par contre, dans son analyse:

> « Le Tribunal estime que cette seule crainte ne peut être source de dommages étant donné qu'il n'y a aucune preuve que cette crainte ait eu des conséquences sur sa santé physique ou mentale. En effet, aucune preuve ne démontre que M. Wellman ait subi quelque préjudice que ce soit. Le sentiment de crainte, tel qu'exprimé par M. Wellman, ne peut certainement pas être la source de dommages. Pour que ce soit le cas, un tel sentiment doit au moins provoquer un malaise, voire même de l'angoisse qui alors affecte la qualité de vie. Une telle preuve n'apparaît pas du dossier et du témoignage de M. Wellman. »[56] (soulignements ajoutés)

En ce qui concerne la demanderesse, Madame Houde, la Cour a retenu de son témoignage que cette dernière avait été manifestement angoissée, même en l'absence de preuve de nature médicale ou psychologique. La somme 1 000$ a été accordée en compensation pour l'angoisse et l'humiliation souffertes.

Cette décision suggère que l'indemnisation du préjudice extrapatrimonial d'une victime d'une atteinte, même dans le cas de la crainte d'un préjudice futur, est possible si une preuve probante des conséquences de l'atteinte est présentée[57]. Logiquement, le préjudice

---

[55] *Wellman* c. *Ministère de la sécurité du revenu-secrétariat*, REJB 2002-33036 (C.S.) (« **Wellman** »)
[56] *Id.*, par. 42
[57] Voir : *Fortier* c. *Zellers inc. et Hudson's Bay Company*, EYB 2009-153198 (C.S.), par. 29. Dans cette affaire, le demandeur réclamait des dommages-intérêts pour « l'anxiété que lui amène la crainte que ses enfants puissent dans le futur contracter quelque maladie à la suite » de leur contact avec un jouet ayant fait

patrimonial subi par cette victime qui prendra des moyens pour corriger la situation, surveiller son crédit et changer ses mots de passe, devrait aussi être indemnisable. Pourtant, la Cour Supérieure a refusé d'accorder des dommages-intérêts à cet égard. Bien que la décision Wellman ait été rendue dans le contexte d'une divulgation non autorisée par un organisme public, elle ouvre légèrement la porte à une interprétation plus large du préjudice dans un contexte où les conséquences de l'atteinte ne se sont pas encore réalisées.

Ainsi, il découle de la revue jurisprudentielle effectuée ci-dessus que les conséquences patrimoniales et extrapatrimoniales résultant de la crainte de la réalisation d'un préjudice futur ne constituent pas un préjudice indemnisable en droit québécois. C'est seulement si l'atteinte a donné lieu à des conséquences réelles que cette dernière engagera l'octroi de dommages-intérêts. Ce constat signifie que l'exercice du recours en responsabilité civile a peu d'attrait pour la victime d'une atteinte à la sécurité de ses renseignements.

(b) La valeur minime du préjudice

Dans certains cas, la victime d'une atteinte subira effectivement un préjudice immédiat à la suite d'une atteinte à la sécurité de ses renseignements personnels. Cependant, la valeur minime de ce préjudice ne justifiera pas l'octroi de dommages-intérêts ou ne justifiera qu'une faible réparation.

En effet, d'une part, pour exister, le préjudice doit être non seulement réel, mais suffisamment grave. Dans l'arrêt Aubry[58], la Cour suprême du Canada rappelait que la seule violation d'un droit garanti par la Charte québécoise[59] ne saurait emporter une condamnation automatique en dommages-intérêts compensatoires, encore faut-il que le préjudice subi soit établi :

---

l'objet d'un rappel parce qu'il contenait du plomb. La réclamation du demandeur a été déboutée mais la Cour a indiqué qu' « aucun début de preuve n'appuie cette prétention ».

[58] *Aubry* c. *Éditions Vice-Versa Inc.*, [1998] 1 R.C.S. 591 (« **Aubry** »)

[59] *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, art. 49 al.1 (« **Charte québécoise** »)

> « […] l'allocation des dommages et intérêts symboliques n'est pas non plus justifiée quand les tribunaux veulent sanctionner la violation d'un droit subjectif qui produira le plus souvent un préjudice minime. Ceci irait à l'encontre des principes de responsabilité civile. »[60]

De plus, tel que le souligne la Cour Suprême du Canada dans l'arrêt *Mustapha* c. *Culligan du Canada Ltd* :

> « Cela dit, les troubles psychologiques constituant un préjudice personnel doivent être distingués d'une simple contrariété. En droit, un préjudice personnel suppose l'existence d'un traumatisme sérieux ou d'une maladie grave : voir *Hinz c. Berry*, [1970] 2 Q.B. 40 (C.A.), p. 42; *Page c. Smith*, p. 189; Linden et Feldthusen, p. 425-427. Le droit ne reconnaît pas les contrariétés, la répulsion, l'anxiété, l'agitation ou les autres états psychologiques qui restent en deçà d'un préjudice. Je n'entends pas donner ici une définition exhaustive de ce qu'est un préjudice indemnisable, mais seulement dire que le préjudice doit être grave et de longue durée, et qu'il ne doit pas s'agir simplement des désagréments, angoisses et craintes ordinaires que toute personne vivant en société doit régulièrement accepter, fût-ce à contrecœur. À mon sens, c'est cette nécessité d'accepter de telles contrariétés, au lieu de prendre action en responsabilité délictuelle pour obtenir réparation, qu'évoquait la Cour d'appel lorsqu'elle a cité *Vanek c. Great Atlantic & Pacific Co. of Canada* (1999), 48 O.R. (3d) 228 (C.A.) : [TRADUCTION]« [E]t la vie continue » (par. 60).. » Tout bonnement, les contrariétés mineures et passagères n'équivalent pas à un *préjudice* personnel et, de ce fait, ne constituent pas un dommage.»[61] (Soulignements ajoutés)

Plus récemment, en 2012, soulignons que la Cour Supérieure a rejeté une requête pour autorisation d'exercer un recours collectif au motif que la demanderesse n'avait pas prouvé *prima facie* l'existence de son préjudice[62]. Dans cette affaire, la demanderesse poursuivait les Services financiers Daimler-Chrysler au motif que cette dernière avait

---

[60] *Aubry,* préc., note 58, par. 68

[61] *Mustapha* c. *Culligan du Canada Ltd*, [2008] 2 R.C.S. 114 (« **Mustapha** »). Dis autrement : de minimis non curat praetur (le magistrat ne doit pas s'occuper de causes insignifiantes). Mentionnons que l'arrêt Mustapha a été rendu en common law. Cependant, tel que le souligne le juge Lacoursière dans la décision subséquente *Mazzona* c. *DaimlerChrysler Financial Services Canada Inc.*, EYB 2012-203721 (C.S.) (« **Mazzona** »), par. 61: « the Court finds no reason to conclude that the distinction between a compensable damage as opposed to an ordinary "annoyance" of life should not apply in Quebec Law. »

perdu un enregistrement (« tape ») contenant des renseignements personnels. Sur la question de la preuve du préjudice au stade de la requête pour autorisation, la Cour Supérieure a reconnu que la demanderesse avait souffert d'anxiété, mais que cela n'était pas suffisant pour établir l'existence d'un préjudice indemnisable :

> « She did indeed suffer anxiety: she has had to change, minimally some of her habits. However, these inconveniences were negligible, so much so that she never felt the need to take any steps to alleviate her anxiety. The most she did was to keep minimum amount of money in the account from which her lease payments were made and to check, twice a month, rather than once a month, on the Internet, whether her account had been tampered with.
>
> This is not enough to meet the threshold, however, *prima facie*, of the existence of "compensable" damages.»[63] (soulignements ajoutés)

Du côté des dossiers soumis à la LPRPDE, la Cour fédérale a rendu, en 2010, deux décisions rejetant des réclamations en dommages-intérêts à la suite d'une divulgation non autorisée de renseignements personnels, au motif que la divulgation et l'atteinte à la vie privée étaient minimes et ne justifiaient pas l'octroi de dommages-intérêts[64].

D'autre part, lorsque le préjudice existe et est suffisamment grave pour être indemnisé, les montants accordés par les tribunaux pour le réparer sont généralement peu élevés.

En ce qui concerne le préjudice patrimonial, dans le contexte bancaire, par exemple, la victime réclame généralement des dommages-intérêts équivalents à la somme qui a été débitée frauduleusement de son compte. De façon générale, cette somme lui sera remboursée par sa banque, soit volontairement selon les politiques de la banque[65], soit

[63] Mazzona, préc., note 61, par. 57 et 58
[64] *Randall* c. *Nubodys Fitness Center*, 2010 CF 681 («**Randall**»); *Stevens* v. *SNF Maritime Metal Inc*., 2010 CF 1137
[65] Ce type de politique semble toutefois être en déclin, voir : D. HOWARD et K. Prince, *Security 2020 : reduce security risks this decade*, p.260 (2011) : « More banks are pushing back [on consumers] as well. [...] With identity theft, and fraud sharply rising, as well as the costs to deal with them, banks are finding themselves less and less willing to absorb all of these losses.»

dans un contexte judiciaire[66]. Le quantum de cette somme est facile à établir. Sauf exception [67] , il est permis de croire que, prises individuellement, les sommes frauduleusement débitées sont généralement peu élevées[68]. En effet, les victimes ont l'obligation de mitiger leurs dommages et de prendre les mesures nécessaires afin d'arrêter la fraude lorsqu'elles la constatent[69]. Par ailleurs, certaines politiques bancaires prévoient des limites quant au montant d'argent qui peut être débité quotidiennement d'un compte bancaire et font la promotion d'une dénonciation rapide, en cas de perte ou de vol de la carte bancaire du client[70]. Néanmoins, il faut souligner que le potentiel d'un dommage plus grand est bien réel. Tel que le souligne le professeur Marc Lacoursière, le montant des « dommages subis à la suite d'une utilisation non autorisée de la carte de débit peuvent […] dépasser de loin le montant disponible au(x) compte(s) en banque au(x)quel(s) la carte donne accès »[71] , notamment en raison de l'accès à la marge de crédit et à la protection en cas de découvert.

Dans un autre contexte, la Cour du Québec a accordé au demandeur des dommages au montant de 4000$ à la suite de la communication de renseignements erronés par la défenderesse à un tiers[72]. Cette indemnité visait à compenser le demandeur pour les « troubles, soucis, inconvénients et perte de temps reliés à l'erreur de la défenderesse ». La Cour a également accordé la somme de 672.32$ pour les frais d'avocat encourus jusqu'à ce que la défenderesse corrige son dossier[73].

En ce qui concerne le préjudice extrapatrimonial, tel que le rappelait la Cour d'appel du Québec dans l'arrêt Valiquette[74], « le préjudice moral étant, par sa nature, qualitatif et

---

[66] *M'Boutchou* c. *Banque de Montréal*, EYB 2008-150981 (C.S.) (« ***M'Boutchou*** »); *Daméus* c. *Banque Nationale du Canada*, 2004 CanLII 20573 (QC C.Q.) (« ***Daméus*** »); *Soucy* c. *Visa Desjardins*, 2005 CanLII 23556 (QC C.Q.)

[67] Dans l'affaire *M'Boutchou*, préc., note 66, la banque a dû rembourser au demandeur la somme de 60 000$.

[68] MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, *Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec*, préc., note 38

[69] C.c.Q., art. 1479

[70] Voir: Marc LACOURSIÈRE, « Chronique - L'utilisation frauduleuse des cartes de débit », *Repères*, Août 2008, *Droit civil en ligne* (DCL), EYB2008REP733

[71] Marc LACOURSIÈRE, « Propositions de réforme pour une protection des titulaires de cartes de débit victimes de transferts de fonds non autorisés », (2009) *54 McGill L.J.* 91, 115

[72] *Wallack* c. *Services financiers Daimler-Chrysler Canada inc.*, EYB 2011-190650 (C.Q.)

[73] Voir aussi: *Couture* c. *Equifax Canada*, 2001 CanLII 20213 (QCCQ) (« **Couture** »)

[74] *Valiquette* c. *The Gazette*, EYB 1996-65651 (C.A.)

irréparable, son appréciation en termes monétaires est un exercice imprécis et arbitraire et se prête difficilement à une évaluation mathématique »[75].

Dans l'arrêt Aubry, précité, la Cour suprême du Canada mentionnait que des dommages au montant de 2 000$ semblaient élevés[76]. Par ailleurs, dans les cas d'utilisation non autorisée de renseignements personnels, les dommages-intérêts accordés en jurisprudence sont peu élevés et oscillent généralement entre 500$ et 3 000$[77], parfois 5 000$[78]. Dans les cas plus exceptionnels, ils peuvent s'élever jusqu'à 15 000$[79] voire, récemment, 50 000$[80].

Au niveau fédéral, les condamnations en dommages-intérêts pour divulgation non autorisée de renseignements personnels ne sont guère plus élevées. À la fin de l'année 2010, dans la décision Nammo[81], la Cour fédérale a accordé 5 000$ en dommages-intérêts au demandeur à la suite de la communication de renseignements personnels erronés à une banque dans le contexte d'une demande de crédit. En se référant à l'arrêt Ward[82] de la Cour suprême du Canada, la Cour fédérale indique que :

> « […] Lorsqu'elle applique le raisonnement de la Cour suprême dans *Ward* aux demandes dont elle est saisie et qui sont présentées en vertu de la Loi, la Cour doit déterminer si les dommages-intérêts sont conformes à

[75] *Id.*, par. 39
[76] *Id.*, par. 72
[77] *Wellman*, préc., note 55; *Daméus*, préc., note 66; *Couture*, préc., note 73 *Lacroix* c. *Bilodeau*, REJB 1998-09843 (C.Q.) (« **Lacroix** »); *Arpin* c. *Bernard Gilles Grenier*, 2004 CanLII 11259 (QC C.Q.); *Bouvrette* c. *Superpages*, 2004 CanLII 42097 (QCCQ); *Cyrenne* c. *Municipalité de St-Samuel*, EYB 2005-89615 (C.Q.); *Routhier* c. *Sous-Ministre du Revenu*, no AZ-50342967 (C.Q.) (« **Routhier** »); Séquing c. Général Motors Acceptance Corporation du Canada ltée, 2007 QCCQ 14509; *Timing Inc.* c. *Idéation Chou inc.*, 2009 QCCQ 6037 ; *Duchamps* c. *Chauvin*, EYB 2010-176107 (C.Q.); *Girao* c. *Zarek Taylor Grossman Hanrahan LLP*, 2011 CF 1070; et *V.B.* c. *M.S.*, 2012 QCCQ 6460
[78] *Stacey*, préc., note 53; St-*Amant* c. *Meubles Morigeau Ltée*, EYB 2006-104823 (C.S.); *Landry* c. *Banque Royale du Canada*, 2011 CF 687; *Tremblay* c. *Labonté Marcoux*, EYB 2011-195952 (C.Q.); *Larente* c. *9140-9599 Québec inc.*, 2011 QCCS 3430
[79] *Stacey*, préc., note 53 ; *J.L.* c. *S.B.*, J.E. 2000-1194 (C.S.); *R.S.* c. *Commission scolaire A*, 2008 QCCQ 13546 ; *A.* c. *B.*, EYB 2009-168118 (C.Q.)
[80] *Unfasung*, préc., note 53: dans cette affaire, une amie d'enfance de la demanderesse avait usurpé son identité pendant plus de deux ans alors qu'elle était hospitalisée pour des traitements contre la leucémie. La Cour a condamné la défenderesse à payer la somme de 55,373.77$ pour le préjudice patrimonial et extrapatrimonial et 40 000$ en dommages-intérêts punitifs.
[81] *Nammo* v. *Transunion of Canada*, 2010 CF 1284 («**Nammo**»)
[82] *Ward* c. *Vancouver (City)*, [2010] 2 R.C.S. 28 («**Ward**»)

> l'objet général de la Loi et aux valeurs qui y sont enchâssées pour décider si des dommages-intérêts doivent être attribués et, dans l'affirmative, décider du montant à accorder. De plus, la fonction de dissuasion permettant de décourager la perpétration d'autres violations et la gravité ou l'énormité de la violation seraient des facteurs à prendre en compte.
>
> […]
>
> [79] À mon avis, le même raisonnement s'applique en l'espèce. Bien que le fait de communiquer des renseignements de crédit erronés ne soit pas comparable à une fouille à nu, il révèle la solvabilité d'une personne à ceux à qui sont transmis les renseignements. Selon moi, il s'agit d'une situation aussi dérangeante, embarrassante et humiliante qu'une brève fouille à nu en règle. J'ai donc décidé que M. Nammo a droit à des dommages-intérêts totalisant 5 000 $, montant représentant entre autres l'humiliation qu'il a subie du fait que TransUnion a violé la Loi. »[83]

La Cour fédérale a jugé que le raisonnement de la Cour suprême du Canada, dans l'arrêt Ward (soit l'octroi d'une réparation « convenable et juste» en vertu du paragraphe 24(1) de la Charte canadienne[84]), était applicable dans l'affaire Nammo vu le caractère quasi-constitutionnel de la LPRPDE. La Cour fédérale semble, dans l'affaire Nammo, vouloir réaffirmer avec plus de fermeté l'importance de respecter les principes de la LPRPDE et lui donner un peu plus de « mordant ». Elle assujettit cependant l'octroi et le montant des dommages-intérêts à la considération de plusieurs facteurs : (a) si l'octroi de dommages-intérêts sert les fins générales de la LPRPDE et favorise le respect des valeurs qu'elle exprime ; (b) s'il convient d'en accorder dans le but de décourager de nouvelles violations; et (c) si la violation est grave[85]. Pour établir si la violation doit être considérée comme grave, la Cour Fédérale considère les critères suivants : (a) son effet sur la santé, le bien-être, ou la situation sociale, professionnelle ou pécuniaire du demandeur ; (b) la conduite du défendeur avant et après la violation; et (c) le point de savoir si le défendeur a tiré profit de ladite violation[86]. Ces facteurs s'apparentent à ceux qui sont considérés lorsque des dommages-intérêts punitifs sont octroyés sous l'article 1621 C.c.Q.

---

[83] *Nammo*, préc., note 81, par.76-79
[84] *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, [annexe B de la *Loi de 1982 sur le Canada*], 1982, c.11 (R.-U.) (« **Charte canadienne** »)
[85] Nammo, préc., note 81, par. 76
[86] Randall, préc., note 64, par. 47

Quoiqu'on puisse s'y référer, mentionnons qu'il faut distinguer les décisions rendues sous la LPRPDE dans les autres provinces canadiennes des décisions rendues en droit québécois. Le recours en dommages-intérêts prévu par la LPRPDE accomplit une fonction non seulement compensatoire, mais également dissuasive et préventive[87]. L'avenir nous dira si la Cour fédérale suivra cette voie et quelles en seront les incidences. Jusqu'à maintenant, les décisions subséquentes à la décision Nammo ont adopté une approche très conservatrice[88].

***

Nous retenons de ce qui précède que la compensation accordée par les tribunaux aux victimes d'une atteinte à la sécurité de leurs renseignements personnels, lorsqu'elle est accordée, est généralement peu élevée. Le fait est que la fonction essentielle de la responsabilité civile est de compenser pour le préjudice subi, sans plus. Or, un minimum d'expérience dans la pratique du droit permet de conclure, vu les coûts reliés à l'exercice d'un recours judiciaire, que les victimes d'atteintes ne sont pas gagnantes même lorsqu'elles ont gain de cause[89]. Ces difficultés relatives à la preuve du préjudice subi ne constituent donc pas un incitatif pour les victimes à exercer le recours en responsabilité civile à leur disposition[90].

[87] Nammo, préc., note 81, par.71-79

[88] Jusqu'à maintenant, les décisions subséquentes à la décision *Nammo* ont accordé des dommages-intérêts inférieurs à 5000$ dans des cas de communications de renseignements personnels non autorisées : *Landry* c. *Banque Royale du Canada*, 2011 CF 687 ; et *Biron* c. *RBC Banque Royale*, 2012 CF 1095. Dans la décision *Townsend* c. *Financière Sun Life*, 2012 CF 550, la réclamation en dommages-intérêts du demandeur a carrément été rejetée, faute d'avoir établi en preuve la mauvaise foi de la défenderesse et le préjudice subi par le demandeur.

[89] À moins qu'elles réduisent leur réclamation à 7000$ et s'adressent à la Cour du Québec, division des petites créances. Une autre possibilité serait d'exercer un recours collectif. Nous n'avons pas étudié la faisabilité de l'exercice d'un tel recours.

[90] D. SOLOVE, *Identity Theft, Privacy and the Architecture of Vulnerability*, 54 *HASTINGS L.J.* 1227, 1231 et 1232 (2002-2003)

Sous-partie 2 Des difficultés d'exercice relatives au lien causal

Ce n'est pas tout de prouver le préjudice subi, encore faut-il que la victime prouve que la faute du défendeur a causé son dommage et le préjudice en découlant. Tel que nous l'exposerons, le caractère ambivalent du lien causal constitue une difficulté additionnelle diminuant les chances de succès et, par conséquent, l'intérêt du recours en responsabilité civile, en matière de sécurité des renseignements personnels.

(a) La causalité adéquate

En droit québécois, les tribunaux ont adopté l'approche de la causalité adéquate, c'est-à-dire celle qui a rendu le dommage objectivement réalisable. Les tribunaux se demanderont: « quels sont les faits qui rendaient objectivement possible la création du préjudice, et dont les conséquences étaient normalement prévisibles pour l'agent ? [91]» Autrement dit, lorsque les faits ayant rendu possible la création du dommage sont liés à la faute, il faut se demander si les conséquences de ce dommage (le préjudice) étaient prévisibles pour l'auteur du comportement fautif. Dans le contexte d'une atteinte à la sécurité des renseignements personnels, la victime doit donc, d'abord, prouver (1) que l'omission de l'entreprise de prendre des mesures de sécurité raisonnables a rendu objectivement réalisable son dommage et, ensuite, (2) que l'entreprise pouvait raisonnablement prévoir le préjudice subi.

Étant donné que la jurisprudence québécoise est peu abondante dans le contexte spécifique de l'obligation de sécurité des renseignements personnels, nous ferons une revue de la jurisprudence québécoise analysant le lien causal dans un contexte plus large, mais similaire, incluant l'obligation de sécurité, que ce soit au niveau contractuel ou

[91] J.-L. BAUDOUIN et P. DESLAURIERS, préc., note 33, n° 1-626, p. 628 et 629 (notons que le « préjudice » renvoi ici à notre notion de « dommage »); Aux États-Unis, voir : Cheryl S. MASSINGGALE et A. Faye BORTHICK, « Risk Allocation for Computer System
Security Breaches: Potential Liability for Providers of Computer Services », (1990) 12 *W. New Eng. L.Rev.* 167, 178 : l'obligation de sécurité ne vaut que pour les incidents qui étaient prévisibles par l'agent.

extracontractuel, afin de cerner les difficultés que la victime peut rencontrer dans la preuve du lien causal.

Dans un premier temps, rappelons que le préjudice pour lequel une réparation est réclamée doit être la conséquence de la faute. Dans la décision *Milunovic c. Transunion Canada inc.*, la Cour du Québec a rejeté la réclamation du demandeur en dommages-intérêts[92]. En effet, le demandeur prétendait que l'inscription erronée à son dossier effectué par la défenderesse avait eu pour conséquence d'entacher son dossier de crédit et qu'il n'avait pas pu bénéficier d'un financement avantageux pour ce motif. La Cour mentionne qu'il appartenait au demandeur de prouver que les diverses demandes de crédit qui lui avaient été refusées résultaient du seul fait que son dossier auprès de la défenderesse contenait des informations erronées[93], ce qu'il n'a pas fait. Plus récemment, dans la décision *Chéry* c. *Banque Royale du Canada*[94], la Cour Supérieure réitérait la nécessité non seulement de prouver le préjudice subi, mais également le lien de causalité. Dans cette affaire, la banque avait avisé madame Chéry de transactions suspectes sur ses comptes bancaires. Madame Chéry a poursuivi la banque pour atteinte à la réputation, atteinte à ses droits garantis et perte d'occasion d'affaires. Ces réclamations ont été rejetées, faute de preuve. Le seul préjudice que Madame Chéry a pu prouver était l'humiliation et les inconvénients. Or, la Cour Supérieure a rejeté ces réclamations, la banque n'ayant pas été trouvée fautive. La Cour a ajouté que même si la banque avait été fautive, Madame Chéry n'avait pas prouvé que les dommages réclamés étaient liés à la faute de la banque[95].

Dans un deuxième temps, soulignons que la notion de prévisibilité prend toute son importance lors de la preuve du lien causal. Dans un arrêt datant de 1978[96], la Cour d'appel du Québec a retenu la responsabilité de l'appelante qui avait manqué à son obligation de sécurité et s'était fait voler les certificats d'actions qui étaient sous sa garde.

---

[92] *Milunovic* c. *Transunion Canada inc.*, EYB 2010-182354 (C.S.) (« **Transunion** »); *Milunovic* c. *Equifax Canada inc.*, EYB 2012-178059 (C.S.); *Chéry* c. *Banque Royale du Canada*, EYB 2012-201866 (C.S.) (« **Chéry** »)
[93] *Transunion*, préc., note 92, par. 25
[94] *Chéry*, préc., note 92. Voir aussi: *Fernandez* c. *Takhar Financial et al.*, 2003 CanLII 3252 (QCCQ)
[95] *Chéry*, préc., note 92, par. 67
[96] *Guardian Trust Co.* c. *Frappier & Holland Inc.*, J.E. 78- 532 (C.A.)

Ces certificats avaient par la suite été forgés par un tiers, pour ensuite être négociés. Il convient de reproduire le passage le plus pertinent de l'arrêt :

> « […] the trust company, by the very nature of its functions, had a duty to take proper care of the certificates which had been given to its care, and the very fact that other companies engaged in similar business took much greater precautions is cogent proof that the theft was a foreseeable risk. […] In my view, the theft and the forgery are so closely related that there is a natural lien between them. The thief knows that the certificate have no particular value unless properly filled in, and he must therefore find someone who is prepared to do so. Indeed, it is a bit like a receiver and a thief; one cannot function without the aid of the other. [...] in the case at bar, the forger was but a further link in a chain of events which started in Appellant's premises and the latter must bear the consequences.»[97] (soulignements ajoutés)

Le raisonnement de cet arrêt a subséquemment été repris dans une décision de la Cour supérieure dans laquelle il a été jugé que la défenderesse avait manqué à son obligation de sécurité malgré l'intervention fautive de son employé dans la chaîne des événements[98]:

> « […] le Tribunal considère que la défenderesse a été négligente et fautive dans la gestion des mesures de sécurité qui devaient nécessairement entourer son travail au bénéfice de la demanderesse. Par la nature même de ses activités, la défenderesse avait le devoir de s'assurer que les services rendus par elles le soient de façon sécuritaire, i.e. d'une manière telle que la demanderesse ne soit pas dépouillée de ses biens. […] cette négligence est si étroitement liée à la disparition des argents de la demanderesse dans la nuit du 1er octobre 1988 « that there is a natural *lien* between them » pour reprendre l'expression du juge Kaufman dans l'arrêt *Guardian Trust Co.* c. *Frappier et Allen Inc.* […] La négligence de la défenderesse, en particulier au niveau du contrôle des clés, et la perte subie par la demanderesse sont intimement liées, l'une n'allant pas sans l'autre. Si la défenderesse avait mis en place des mesures de sécurité adéquates et si elle avait contrôlé en particulier les clés dont elle avait la garde, aucun de ses employés n'aurait pu les utiliser en-dehors de ses heures de travail pour dévaliser l'un ou l'autre des guichets automatique de la demanderesse. […] le geste de l'employé de Pinkerton ne devient plus alors qu'un chaînon

[97] *Id.*, par. 26-32
[98] *Banque Laurentienne du Canada* c. *Pinkerton du Québec Ltée*, EYB 1994-73813 (C.S.)

> dans une suite d'événements ayant trouvé leur origine chez la défenderesse et celle-ci doit en subir les conséquences. »[99] (soulignements ajoutés)

Plus récemment, dans l'arrêt *Quantz*[100], les demandeurs reprochaient à ADT d'avoir tardé à agir à la suite de la réception d'un signal indiquant que la ligne reliant leur système d'alarme au réseau téléphonique avait été coupée, entraînant ainsi le vol et le vandalisme de leur demeure. Au sujet de la causalité, la Cour d'appel a jugé que les « pertes pécuniaires »[101] réclamées par les demandeurs avaient été causées par le défaut d'ADT d'envoyer un garde de sécurité dans un délai de vingt minutes.

Nous pouvons conclure de ce qui précède que la victime doit établir que la survenance de l'événement dommageable et ses conséquences étaient prévisibles, eut égard à la nature des activités de l'entreprise. Dans la décision *Banque Laurentienne*[102], la défenderesse Pinkerton offrait des services de sécurité. La nature de ses activités rendait prévisible l'événement dommageable et ses conséquences.

Si cela va de soi pour une compagnie offrant des services de sécurité, il en va autrement, par exemple, pour un commerce de vente aux détails. Le vol, par un tiers, du registre contenant les noms, adresses et numéros de téléphone des clients est-il prévisible pour le commerçant? Et qu'en est-il de l'utilisation subséquente des noms, adresses et numéros de téléphone? Les répercussions du vol peuvent être aussi variées qu'imprévisibles.

Par exemple, dans la décision *Shoghikian*[103], la compagnie défenderesse a été poursuivie en dommages en raison de la fraude commise par l'une des employés de la demanderesse. En effet, la défenderesse avait donné à une employée de la demanderesse le code d'accès élargi (« administrateur »). Ce code avait été donné sans l'autorisation de la demanderesse, alors en congé de maladie, afin que l'employée puisse fermer l'année financière de l'entreprise. Au retour de la demanderesse au travail, la compagnie défenderesse avait oublié de l'aviser qu'elle avait donné le code à son employée.

---

[99] *Id*., par. 36- 43
[100] *Quantz* c. *ADT Canada Inc.*, REJB 2002-33495 (C.A.)
[101] Selon notre lexique, il est question ici du préjudice patrimonial.
[102] Préc., note 98
[103] *Shoghikian* c. *Axxium Vision Inc.*, EYB 2010-177339 (C.Q.)

Quelques années plus tard, l'employée a volé des fonds de l'entreprise de la demanderesse à l'aide ce même code. La Cour du Québec en est venue à la conclusion que la défenderesse ne pouvait pas prévoir que l'employée agirait ainsi, surtout quelques années plus tard, et que la faute de l'employée était plus grande que celle de la défenderesse. La responsabilité de la défenderesse a donc été écartée. La demanderesse a dû supporter seule la fraude, son employée ayant fait cession de ses biens.

La décision précitée illustre les difficultés liées à la notion de prévisibilité. Tant qu'une victime ne subit pas de conséquences négatives, elle ne subit aucun préjudice. Une fois qu'elle subit le préjudice, le facteur temps peut jouer contre elle. Comment prouver que l'utilisation non autorisée était prévisible? Malheureusement, en pratique, ce scénario est probable : peu d'individus savent qu'ils sont victimes d'une atteinte[104].

Enfin, mentionnons quelques illustrations démontrant d'autres difficultés liées à la notion de prévisibilité. Par exemple, dans l'arrêt *Piertrem*, la Cour d'appel a souligné que l'existence de vols antérieurs rend prévisible un vol subséquent, même en présence de mesures de sécurité[105]. Il existe d'autres situations où il a été jugé que la présence de mesures de sécurité, afin de protéger les biens que l'entreprise a sous sa garde, rend imprévisible le vol. Dans ces situations, la victime supporte seule son préjudice[106]. Par ailleurs, si le vol est l'œuvre de voleurs professionnels, l'entreprise défenderesse n'est pas toujours tenue d'indemniser, même si certaines mesures de sécurité étaient manquantes[107]. Appliquer ce raisonnement à la sécurité des renseignements personnels implique un fardeau de preuve très élevé pour la victime. Elle doit prouver que les mesures de sécurité mises en place par la défenderesse sont nettement insuffisantes, dans des circonstances qui lui sont souvent inconnues, et que cette insuffisance a rendu prévisible son préjudice.

---

[104] D. SOLOVE, préc., note 90, 1248 : «Victims are often unaware that their identities have been stolen until long after the identity theft has begun.»
[105] *Les enterprises Piertrem (1989) inc.* c. *Pomerleau Les Bateaux inc.*, EYB 2007-120374 (C.A.), par. 61-62
[106] *Kingsway Transport Ltd.* c. *R.K. Investigations Inc.*, [1996] J.Q. no. 1246 (C.S.)
[107] *Guarantee Company of North America* c. *Phil Larochelle Equipement inc*., EYB 2009-153328 (C.S.)

(b) Le partage de responsabilité

Une autre difficulté pour la victime est le partage de responsabilité avec l'auteur du comportement fautif et même, dans certains cas, l'absence de responsabilité de l'auteur du comportement fautif. Il convient de faire une brève revue jurisprudentielle afin d'illustrer notre propos.

Dans la décision *Place Biermans inc.*[108], les locataires d'un centre commercial ont poursuivi le propriétaire et gardien du centre d'achats ainsi que l'auteur de l'incendie ayant ravagé le centre d'achat. Le propriétaire a été tenu responsable en partie des dommages résultant d'un incendie allumé par un adolescent de quinze ans, en raison de sa négligence dans la surveillance des lieux. La Cour supérieure a indiqué qu'il était prévisible et que le propriétaire ne pouvait ignorer que la présence d'un bidon d'essence situé dans un cabanon, non cadenassé, à la sortie arrière du complexe commercial et, plus particulièrement, à la sortie du billard du complexe, attirerait la curiosité et la convoitise des jeunes qui se rendent précisément là pour consommer des drogues, à l'abri des regards. La négligence du propriétaire rendait prévisible l'incendie, bien qu'elle n'en ait pas été la seule cause ni la plus importante. Cette décision illustre le partage classique de responsabilité entre le fautif de première ligne et d'autres intervenants dans la chaîne de responsabilité. Dans cette affaire, l'auteur de l'incendie a dû assumer une part de responsabilité de 75%. Seul hic : l'auteur de l'incendie avait 15 ans et n'avait pas un sou. Transposé dans le contexte de la sécurité des renseignements personnels, nous pouvons anticiper que la victime qui poursuit l'entreprise qui traite ses renseignements doit s'attendre à ce que la responsabilité soit partagée entre l'entreprise fautive et le fautif de première ligne, souvent insolvable ou introuvable[109]. Au final, il est possible que son dommage ne soit que partiellement compensé.

---

[108] *Place Biermans* c. *C.D.*, [2010] QCCS 4170, confirmé en appel 2013 QCCA 64.

[109] Selon la nature du lien qui unit l'entreprise et la victime, la solidarité de l'article 1526 C.c.Q. pourrait pallier à ce problème. Nous n'avons pas, pour les fins de la présente, analysé la nature du lien, contractuel ou extracontractuel, qui peut exister entre l'entreprise qui traite les renseignements personnels d'un individu et ce dernier.

Dans le contexte spécifique de la fraude bancaire, soulignons que le fardeau de preuve est particulièrement difficile à surmonter, surtout lorsque la fraude résulte de l'utilisation du numéro de la carte bancaire et du NIP de la victime, sans sa participation[110]. Comment expliquer, avec crédibilité, que le numéro de la carte bancaire et le NIP, qui n'ont pas été, à proprement dit, volés, ont été utilisés sans la participation de la victime?

Par chance, les tribunaux semblent sensibilisés à cette difficulté. Dans la décision *Daméus*, la Banque Royale du Canada soutenait que sa cliente, la demanderesse, avait révélé son NIP à son fiancé et avait choisi un NIP correspondant à des informations personnelles. Elle soutenait que la demanderesse était donc la seule responsable de la fraude bancaire. Bien que ces faits fussent vrais, la Cour a toutefois décidé qu'il n'y avait pas de lien causal et a mentionné ce qui suit, à la défense des utilisateurs de cartes bancaires :

> « La mise en place d'un système de sécurité à l'épreuve des fraudeurs en rapport avec l'utilisation de la carte, relève de la Banque. Il serait contraire aux exigences de la bonne foi (art. 6 et 7 C.c.Q.) d'imposer à la détentrice d'une carte d'assumer seule à l'exonération de la Banque toute responsabilité pour des transactions frauduleuses reliées à sa carte, pour lesquelles elle n'a pas contribué ou n'a aucun lien. » [111] (soulignements ajoutés)

Il n'en demeure pas moins que les détenteurs d'une carte bancaire ont tout intérêt à redoubler de vigilance lors de l'utilisation de leur carte et NIP s'ils ne veulent pas supporter seuls les conséquences d'une fraude bancaire[112].

Enfin, mentionnons une décision récente rendue aux États-Unis qui confirme cette mise en garde. Dans l'affaire *Ocean Bank*, la Cour du Maine a jugé que les mesures de sécurité de la banque n'étaient pas optimales, mais que cette dernière n'avait aucune obligation

[110] M. LACOURSIÈRE, préc., note 71, 114 et 115. Voir aussi : *Bessaoud* c. *Caisse Desjardins du Marigot de Laval*, 2002 CanLII 23640 (C.Q.), par. 20 et 21; *Louis* c. *Banque Laurentienne du Canada*, EYB 2007-112380 (C.Q.), dans laquelle le demandeur a été débouté, faute de crédibilité, puisque tout portait à croire qu'il était l'auteur de la fraude.
[111] *Daméus*, préc., note 66, par. 54.
[112] *Laberge* c. *Caisse populaire Desjardins de Cowansville*, [1999] R.L. 503 (C.Q.); *Royal Bank of Canada* v. *Devarenne*, [1998] N.B.J. No 376; *Rosen* v. *CIBC*, [2002] O.J. NO 1103 (S.C.)

légale de prendre les « meilleures » mesures de sécurité[113]. L'entente entre la banque et son client était claire quant à son niveau de sécurité et à sa responsabilité en cas de fraude bancaire. De plus, il avait été mis en preuve que le niveau de sécurité d'Ocean Bank était similaire à celui d'autres banques. Ultimement, c'est la victime qui était responsable de son propre malheur : elle aurait dû mieux sécuriser son compte bancaire[114]. Quoique cette décision ait été rendue dans une autre juridiction, elle illustre la vigilance dont les victimes doivent faire preuve à l'égard de la sécurité de leurs comptes bancaires.

(c) La multiplicité des causes

Du côté de la jurisprudence américaine, plus abondante qu'au Québec dans le contexte spécifique de la sécurité des renseignements personnels, d'autres difficultés relatives à la preuve du lien de causalité émergent. À notre connaissance, ces difficultés n'ont pas encore été abordées devant les tribunaux québécois. Ces difficultés résident dans l'impossibilité, dans certains cas, d'identifier la source de l'atteinte[115]. En effet, plusieurs organisations différentes collectent les mêmes données sur les individus[116]. Comment prouver que le dommage résulte d'une atteinte dans le système de sécurité de l'entreprise défenderesse plutôt que d'une autre entreprise? Par ailleurs, considérant que les données des individus se trouvent éparpillées en plusieurs endroits sur la Toile, il est également probable que le dommage ne résulte pas d'une atteinte dans le système de sécurité de l'entreprise défenderesse, mais plutôt des activités d'un bidouilleur qui aura trouvé les données d'une autre source[117]. Ce n'est donc pas parce que le dommage de la victime coïncide avec une annonce dans les médias selon laquelle sa banque, par exemple, a fait

---

[113] Tracy KITTEN, *ACH Fraud: Judge denies Patco Motion No jury expected to hear about dispute with Ocean Bank*, 9 août 2011, en ligne: http://www.bankinfosecurity.com/ach-fraud-judge-denies-patco-motion-a-3939/op-1 (consulté le 23 décembre 2011) Notons que, dans cette affaire, la victime était une personne morale et non une personne physique.
[114] *Id.*
[115] P.M. SCHWARTZ et E. J. JANGER, *Notification of date security breaches*, 105 *MICH. L. REV.* 913, 928 (2007)
[116] Jennifer A. CHANDLER, «Negligence Liability for Breaches of Data Security», (2008) 23 *BFLR-CAN* 223, 235-238
[117] *Id.*

l'objet d'un vol d'informations qu'il y a un lien causal entre les deux. Il n'est pas suffisant pour la victime d'alléguer que l'atteinte dans le système de sécurité informationnelle d'une entreprise lui a causé un préjudice immédiat. La preuve doit démontrer, selon la balance des probabilités, que le dommage et ses conséquences ont été causés par la faute de l'entreprise, par opposition à toute autre source[118]. Cependant, notons que, dans l'arrêt *Stollenwerk*[119], la Cour d'appel des États-Unis, pour le neuvième circuit, a nuancé cette position. En effet, la Cour d'appel a renversé la décision de première instance qui avait conclu que « [...] to determine that one event caused another merely because the first preceded the second is a classic example of *post hoc ergo propter hoc* ("after this, therefore because of this"), [is a] logical fallacy »[120]. La Cour d'appel a indiqué que la demanderesse n'avait pas à prouver que le vol était la seule cause possible du vol d'identité. Il était suffisant de prouver que le vol était la cause la plus probable : « a substantial factor in bringing about the result »[121]. Cette décision nous semble toutefois un cas isolé. Nous ne pouvons présumer non plus de son application au Québec vu la différence des régimes en place. Toutefois, il sera intéressant de voir comment la jurisprudence québécoise interprètera la notion de la causalité adéquate dans le cas particulier des atteintes à la sécurité informationnelle.

***

Tel que l'illustre la revue des décisions citées dans cette sous-partie, la preuve de la causalité adéquate n'est pas un exercice facile. Cette fameuse notion de « prévisibilité » de l'événement dommageable et de ses conséquences est ambivalente. Nous retenons de ces décisions que la preuve du lien causal peut être difficile dans certaines circonstances, considérant les éléments suivants : l'imprévisibilité pour l'entreprise de la survenance de

[118] C.E. GIDEON, préc., note 3, 170-172. Mentionnons que l'utilisation de la présomption de faits de l'article 2846 C.c.Q. et la solidarité de l'article 1480 C.c.Q. pourrait permettre de solutionner ce problème en droit québécois. Cette possibilité mérite une analyse plus poussée que nous avons écartée pour les fins de la présente.
[119] *Id.*
[120] *Stollenwerk*, préc., note 41, p.10
[121] Cité dans C.E. GIDEON, préc., note 3, 170-172

l'événement dommageable et du préjudice subi par la victime vu la nature de ses activités; l'intervention et le mode d'intervention imprévisibles du fautif de première ligne; l'imprévisibilité de l'usage et de la gravité de l'usage des renseignements personnels; l'existence de mesures de sécurité déjà en place; la connaissance de la victime des mesures de sécurité en place; le délai entre la commission de la faute et la réalisation du préjudice et la difficulté de prouver la source exacte du préjudice. Ces difficultés de preuve diminuent les chances de succès du recours et n'encouragent pas les victimes à intenter le recours en responsabilité civile à leur disposition.

Conclusion de la partie A

Nous avons vu dans cette première partie que, en cas d'atteinte, la victime doit intenter une action en responsabilité civile contre l'entreprise qui porte atteinte à la sécurité de ses renseignements afin de réaffirmer son droit à la protection de ses renseignements personnels et d'obtenir une compensation. Personne d'autre qu'elle n'a un intérêt suffisant pour le faire. Or, l'exercice du recours en dommages-intérêts compensatoires souffre de difficultés sérieuses quant à la preuve du préjudice subi et du lien causal, deux conditions essentielles à l'octroi de dommages-intérêts compensatoires. Plus particulièrement, nous constatons que la seule preuve de l'atteinte (du dommage) ne suffit pas. Cette situation conduit à des effets incongrus. La victime qui subit les conséquences négatives d'une atteinte est dans une meilleure position juridique que celle qui subit une atteinte sans conséquence ou que celle qui entreprend des mesures préventives dans le but d'éviter ces conséquences. Au final, le régime de responsabilité civile laisse la victime d'une « simple » atteinte sans indemnisation. Il n'accomplit pas sa fonction compensatoire puisqu'il n'y a pas de préjudice à réparer. La fonction purement compensatoire du régime est donc incompatible avec une atteinte à la sécurité des renseignements personnels.

Partie B L'échec des fonctions préventives et dissuasives incidentes du régime de responsabilité civile

Nous verrons dans cette partie que le régime de responsabilité civile n'incite pas les entreprises à prendre des mesures de sécurité raisonnables. D'une part, le contenu indéfini de l'obligation de sécurité des renseignements personnels empêche les entreprises de bien cerner l'étendue de leur obligation. Par conséquent, les entreprises peuvent difficilement adopter des mesures de sécurité raisonnables afin prévenir les atteintes à la sécurité des renseignements qu'elles traitent. D'autre part, il découle de la partie précédente que l'échec de la fonction compensatoire de la responsabilité civile en matière de sécurité des renseignements personnels rend impossible l'accomplissement de ses fonctions préventives et dissuasives incidentes à l'égard des entreprises.

Sous-partie 1 Une obligation de sécurité indéfinie

Dans le contexte de notre étude sur l'efficacité du régime, il importe de s'attarder à l'obligation que le régime sanctionne en cas de non-respect. Le contenu de l'obligation de sécurité des entreprises est intimement lié aux fonctions préventives et dissuasives incidentes du régime.

Selon le professeur Vermeys, l'obligation de sécurité informationnelle serait une obligation de moyens renforcée[122]. Résumé très sommairement, il en vient à la conclusion que l'obligation de moyens renforcée se présente comme un juste compromis, considérant que l'obligation de moyens est trop exigeante pour la victime et que l'obligation de résultat est trop contraignante pour l'entreprise[123].

[122] Lire, pour une explication détaillée, N. W. VERMEYS, préc., note 7, p. 88-118
[123] *Id.*

L'obligation de moyens renforcée implique, au plan de la preuve, une présomption de faute[124]. La victime doit démontrer, en premier lieu, qu'une une entreprise a permis une atteinte à la sécurité de ses renseignements personnels laquelle lui a causé un dommage[125]. Elle n'a pas à démontrer si cette atteinte est fautive. Il appartient ensuite à l'entreprise de démontrer, selon la balance des probabilités[126], qu'elle a pris les moyens raisonnables pour éviter une telle atteinte[127]. Si l'entreprise s'acquitte de son fardeau, il reviendra à la victime de le repousser.

L'obligation de moyens renforcée demeure donc une obligation de moyens, mais elle allège le fardeau de preuve de la victime en imposant à l'entreprise de prouver, en premier lieu, que des mesures de sécurité raisonnables étaient en vigueur au moment de l'atteinte. En effet, l'entreprise est dans une meilleure position que la victime pour démontrer les moyens de sécurité en œuvre dans son propre système.

Bien que l'obligation de moyens renforcée soit plus contraignante pour l'entreprise que l'obligation de moyens « ordinaire » au plan de la preuve, il y a lieu de se questionner sur l'efficacité de ce degré d'intensité eut égard aux fonctions préventives et dissuasives de la responsabilité civile.

Dans l'état actuel des connaissances, nous soumettons que le contenu indéfini de l'obligation de sécurité des renseignements personnels permet aux entreprises d'osciller entre le risque qui est socialement acceptable et celui qui ne l'est pas. Dans cette perspective, l'obligation de sécurité de moyens crée plus d'insécurité que de sécurité.

(a) Les incertitudes de la « raisonnabilité »

L'obligation de moyens renforcée implique que l'entreprise doit, au préalable, documenter son système de sécurité afin de pouvoir se défendre contre une action en

[124] *Id.*
[125] *Id.*
[126] C.c.Q., art. 2804
[127] N. W. VERMEYS, préc., note 7, p. 88-118

responsabilité civile[128]. Cette nécessité de documenter, d'ailleurs déjà prévue par certaines dispositions législatives[129], exerce une pression positive sur l'entreprise pour qu'elle adopte, dans les faits, des mesures de sécurité raisonnables. Par contre, l'obligation de moyens renforcée n'a pas pour effet de modifier l'intensité de l'obligation de l'entreprise. Cette dernière demeure tenue de prendre des « moyens raisonnables » pour éviter un préjudice. Or, que signifie « prendre des moyens raisonnables »?

La « raisonnabililité » est une notion floue et variable[130], mais elle n'est pas nouvelle. En droit civil québécois, elle se soulève à chaque fois qu'une personne manque à son devoir de prudence et diligence sous l'article 1457 ou l'article 1458 du Code civil[131]. Pourquoi la « raisonnabilité » serait-elle plus incertaine en matière de sécurité des renseignements personnels que dans d'autres secteurs d'activités?

Dans un premier temps, la subjectivité et la relativité du concept de sécurité rendent incertaine la « raisonnabilité » de l'obligation[132]. D'abord, ce qui représente un danger pour une personne « X » n'en est pas nécessairement un pour une personne « Y ». Par ailleurs, la tolérance au danger ou au risque varie d'une personne à l'autre. Par exemple, une entreprise peut juger qu'une clé de chiffrement de 128 bits est suffisante pour protéger le dossier médical d'un individu alors que ce dernier peut juger qu'une clé de chiffrement de 1028 bits serait nécessaire. Quoique la subjectivité et la relativité du concept existent dans d'autres domaines, elles nous semblent plus aiguës en matière d'atteinte à la sécurité informationnelle compte tenu des considérations suivantes.

La sécurité est un processus relatif qui ne se termine jamais[133]. Le choix des mesures de sécurité varie selon le contexte et doit régulièrement être révisé. Dans le choix des mesures de sécurité raisonnables, le RSI raisonnable doit tenir compte du cadre

---

[128] N. W. VERMEYS, préc., note 7, p.117

[129] LCCJTI, art. 17, art. 34; Code type, préc., note 16, art. 4.2.1, art. 4.5.1 et art. 4.8.2d)

[130] Nicolas W. VERMEYS, Computer "Insecurity" and Viral Attacks: Liability Issues Regarding Unsafe Computer Systems Under Quebec Law, *Lex Electronica*, vol. 9 n°1, Hiver 2004, par. 10; réitéré dans N. W. VERMEYS, préc., note 7, p. 191

[131] Anciennement, sous l'article 1053 et 1065 C.c.B.-C.

[132] N. W. VERMEYS, préc., note 7, p. 67; Thomas J. SMEDINGHOFF, « It's all about trust: the expanding scope of security obligations in global privacy and e-transactions law », 16 MICH. ST. J. INT'L L. 2 (2007-2008), 30-32

[133] *Id.*; N.W. VERMEYS, préc., note 7, p. 74; Bruce SCHNEIER, *Secrets & Lies : Digital Security in a Networked World* (2000), xii

législatif[134] et jurisprudentiel[135]. Le RSI raisonnable doit également tenir compte des normes de son industrie[136]. Les normes de l'industrie réfèrent aux règles de l'art, c'est-à-dire à ces normes développées par l'industrie elle-même ou un organisme étatique[137]. Il s'agit des moyens couramment employés dans un type de situation donnée, de normes minimales[138]. Il faut toutefois rappeler que, le comportement moyen n'est pas pour autant raisonnable. En effet, tel que le soulignait la juge L'Heureux-Dubé dans l'arrêt *Roberge* c. *Bolduc*: « il ne suffit pas, à mon avis, de suivre la pratique professionnelle courante pour échapper à sa responsabilité. Il faut que le caractère raisonnable de cette pratique puisse être démontré. »[139] Enfin, les normes de l'industrie ne doivent pas être confondues avec les standards développés par des organismes de normalisation[140]. À la différence des normes de l'industrie, ce sont des normes d'excellence, disponibles moyennant un paiement pour en obtenir une copie. Le RSI ne sera lié par elles que si elles s'intègrent dans les normes de l'industrie[141]. Dans tous les cas, après avoir consulté les règles énoncées par le cadre législatif, la jurisprudence et les normes de son industrie, le RSI raisonnable sait que la conformité avec aucune d'elles ne lui garantira d'avoir rempli son obligation. Il n'y a pas de « safe harbor » en sécurité informationnelle en droit québécois[142].

Dans un deuxième temps, et au risque de tomber dans le cliché, la « raisonnabilité » est plus incertaine en matière de sécurité informationnelle à cause de l'évolution rapide des technologies. Cette évolution implique tant l'évolution technologique des menaces que des mesures de sécurité[143]. Dans ce contexte, il devient difficile pour une entreprise d'identifier le comportement raisonnable qu'elle doit adopter. Si bien que ce « n'est que

---

[134] *Supra*, p. 5-8
[135] N.W. VERMEYS, préc., note 7, p.138
[136] *Id*.
[137] N.W. VERMEYS, préc., note 7, p.129
[138] *Id.*
[139] *Roberge* c. *Bolduc*, [1991] 1 R.C.S. 374, p.81. Ce principe a été repris dans la décision américaine *T.J. Hooper* v. *Northern Barge*, 60F 2d 737 (2nd Cir. C.A. 1932)
[140] N.W. VERMEYS, préc., note 7, p.129, l'auteur qualifie ce type de normes d'« industrie des normes ».
[141] *Id*.
[142] N.W. VERMEYS, préc., note 7, p.191-192. Voir T.J. SMEDINGHOFF, préc., note 132, 32-33, et aussi le rapport de la Maison Blanche, lequel recommande l'établissement d'un « safe harbour » par le FTC : THE WHITE HOUSE, *Consumer data privacy in a networked world : a framework for protecting privacy and promoting innovation in the global digital economy*, Washington, February 2012, p. 37, en ligne: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (consulté le 3 janvier 2013) (« **The White House report** »)
[143] *Supra*, p. 4

lorsqu'elles seront concrètes et significatives, et non pas hypothétiques, qu'il conviendra de se pencher sur […] les modifications technologiques susceptibles de rendre insuffisantes les mesures de sécurité prises »[144].

D'une part, dans un contexte où la nature des menaces évolue rapidement, l'entreprise ne sait plus contre quelles menaces elle doit se prémunir[145]. Or, l'obligation de moyens est efficace en autant que l'événement dommageable soit prévisible. La sécurité informationnelle consiste à protéger les ressources informationnelles « face à des risques identifiés »[146]. L'instabilité des risques rend difficile toute évaluation du comportement socialement acceptable. D'autre part, dans un contexte où la « raisonnabilité » des contre-mesures à adopter peut changer dans un court laps de temps, il devient difficile pour une entreprise d'apprécier le contenu de son obligation et de s'y conformer.

L'affaire TJX illustre parfaitement bien notre propos[147]. Lors de la découverte d'une intrusion dans son système de sécurité, à la fin de l'année 2006 et au début de l'année 2007, TJX était en train de transformer son protocole de chiffrement WEP en protocole WPA. Le protocole WPA avait été recommandé par l'Institute of Electrical and Electronic Engineers (« IEEE ») en 2003. Cette migration vers le protocole WPA se faisait dans le cadre de l'implantation de la nouvelle version (version 1.1.) des normes de sécurité sur les données de l'industrie des cartes de paiement, connue sous l'abréviation « PCI DSS »[148]. Cette version était en circulation depuis septembre 2006 et exigeait le protocole de chiffrement WPA[149]. Or, la Commissaire indique, dans ses conclusions, que TJX aurait dû se conformer, avant la fin de l'année 2006, à la version 1.1. des PCI DSS. Selon elle, « TJX utilisait un protocole de chiffrement peu fiable et n'a[vait] pas mis en

---

[144] *Wansink* c. *Telus Communications*, [2007] 4 R.C.F. 375, par. 15
[145] Voir: Michael E. WHITMAN et Herbert J. MATTORD, *Readings and cases in information security: Law and Ethics*, p.192 (2011) : «Internet security threats continue to evolve as hackers attempt to stay ahead of security defences that are being applied at the application and network layers»
[146] OFFICE DE LA LANGUE FRANÇAISE, préc., note 7
[147] COMMISSARIAT, *Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels, TJX Companies Inc./Winners Merchant International L.P.*, en ligne : http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_f.asp (consulté le 8 octobre 2012) (« **TJX** »)
[148] PCI SECURITY STANDARD COUNCIL, en ligne: https://www.pcisecuritystandards.org/security_standards/ (consulté le 8 juillet 2012)
[149] TJX, préc., note 147, par. 87

place une norme de chiffrement plus stricte dans un délai raisonnable »[150]. Les propos de la Commissaire illustrent parfaitement la difficulté de déterminer ce que constitue l'emploi de « moyens raisonnables ». Pourquoi le protocole WEP était-il peu fiable? Il faisait partie des exigences de la version 1.0., laquelle n'a été remplacée qu'en 2006. TJX aurait-elle dû implanter le protocole WPA dès sa sortie en 2003? Et si ce protocole ne s'était pas avéré concluant? Quel aurait dû être le délai raisonnable pour l'implantation de la version 1.1? Et compte tenu de quels facteurs? Qui plus est, nous ne pouvons manquer de souligner que la norme WPA retenue par la Commissaire a été remplacée, peu de temps après la publication de ses conclusions, par la norme WPA2, jugée supérieure[151]. L'évolution rapide des technologies rend donc difficile l'évaluation des mesures de précautions raisonnables à adopter.

Même l'analyse économique du droit, utilisée par certains auteurs afin d'évaluer le comportement socialement acceptable lorsque le droit positif n'y arrive pas[152], est de peu de secours dans un contexte aussi instable. En fait, l'analyse économique du droit propose d'identifier le comportement socialement acceptable en « identifiant le seuil au-delà duquel les précautions destinées à prévenir le dommage ne sont plus nécessaires »[153]. Ce seuil dépend de l'interaction de trois variables : la probabilité d'un événement dommageable (P); la gravité du préjudice qui résulterait de la survenance de cet événement (L); et le fardeau de précautions adéquates pour le prévenir (B)[154]. La probabilité de l'événement dommageable (P) oscille entre la certitude et l'impossibilité. À ces deux extrêmes, inutile de prendre des mesures de précautions. Entre les deux, il s'agit de limiter la probabilité de sa survenance grâce à l'adoption de mesures de précautions. La gravité du préjudice (L) est une variable « variable ». Tel que mentionné précédemment, le préjudice est une notion subjective. Par ailleurs, il doit être prévisible et évitable. Autrement, on ne peut parler de négligence. Enfin, les mesures de précautions

[150] *Id.*, par. 90
[151] N. W. VERMEYS, préc., note 7, p.189
[152] Nicolas W. VERMEYS, *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, thèse de doctorat, Montréal, Faculté de droit, Université de Montréal, 2009, p. 274 (« **N.W. VERMEYS, thèse doctorat** »)
[153] Grégory MAITRE, *La responsabilité civile à l'épreuve de l'analyse économique*, Paris, L.G.D.J., 2005, p.80
[154] N.W. VERMEYS, thèse de doctorat, préc., note 152, p. 265

(B) représentent les moyens mis en place pour éviter la survenance de l'événement dommageable. Sont inclus dans ces moyens les équipements (techniques ou physiques), les éléments non-monétaires (les compromis en matière de fonctionnalité et d'accès de systèmes), les coûts intangibles (le capital réputationnel) et les coûts de remise en état[155]. Considérant ces variables, selon le « calcul de la prévention » élaboré par les tenants de l'analyse économique du droit, une personne est fautive si le coût des mesures de précautions qu'elle a prises est inférieur aux coûts de l'événement dommageable (L) multiplié par la probabilité de sa survenance (P), soit : B<PL.[156] Selon cette formule, si la probabilité de survenance de l'événement dommageable est élevée, alors l'obligation corrélative de prendre des mesures de précautions augmente. L'inverse est aussi vrai.

Ceci étant dit, nous pouvons facilement concevoir que l'évolution rapide des technologies fait fluctuer la probabilité de la survenance de l'événement dommageable et le coût des mesures de précautions dans l'équation précitée. De ce fait, elle influence inévitablement le degré de certitude du calcul[157]. Le seuil de prévention optimale devient donc mouvant sur la courbe graphique créée par l'équation précitée. Par ailleurs, soulignons que, malgré toute la logique de ce test, plusieurs auteurs remettent en cause sa valeur en matière de sécurité informationnelle[158]. En effet, le coût des actifs informationnels à protéger s'évalue difficilement pour une entreprise. L'évaluation de ces coûts est nécessaire afin de déterminer la variable (B), soit le coût des mesures de précautions. Or, la valeur de l'information n'est pas uniforme et dépend de différents facteurs. Il n'y a pas d'évaluation basée sur la juste valeur marchande, la valeur de remplacement ou la valeur à neuf qui tienne. Par ailleurs, la sécurité informationnelle étant une notion relativement nouvelle, les entreprises ne bénéficient pas de données empiriques fiables leur permettant de faire des matrices afin d'évaluer les risques futurs et le coût de ces risques. En l'absence de valeurs fiables à insérer dans l'équation, comment identifier le comportement raisonnable? Ainsi, dans la mesure où les risques sont difficilement

[155] *Id.*, p. 255-257
[156] *Id.*; Voir aussi : E. MACKAAY et S. ROUSSEAU, préc., note 31, p. 332
[157] K. SOO HOO, préc., note 2, 32
[158] M. E. WITHMAN et H. J. MATTORD, préc., note 145, p. 87-89; N.W. VERMEYS, préc., note 7, p.47-67

prévisibles, il est difficile pour l'entreprise de déterminer le seuil de sécurité socialement acceptable.

La conséquence de cette incertitude quant au contenu de l'obligation est l'adoption de pratiques déviantes. Afin d'éviter d'engager sa responsabilité, une entreprise pourra décider d'adopter un comportement irréprochable (« sur-sécurité »)[159]. Ce faisant, elle investira dans des mesures de sécurité excessives, dépassant largement ses besoins et ses ressources en sécurité. Or, en plus d'être inutile, ce comportement n'est pas souhaitable. En effet, tel que le souligne Danielle Keats Citron (« Citron »): « [a] database operator's uncertainty about the contours of due care may prompt it to take too much precaution. Such overcompliance with the law risks inhibiting socially useful data collection »[160]. Ensuite, la multiplication des contre-mesures n'est pas gage d'une plus grande sécurité[161], puisque: « [as] systems continue to get more complex, they will continue to get less secure »[162]. Par ailleurs, la sur-sécurité est économiquement non viable à long terme. Les finances d'une entreprise ne peuvent supporter un investissement sans retour. De plus, s'il est vrai que le coût des accidents diminue en fonction des mesures de précautions, cette diminution n'est pas linéaire[163]. Les mesures de protection de base sont peu coûteuses et éviteront à l'entreprise de subir les atteintes facilement identifiables. Cependant, plus le niveau de sécurité recherché sera élevé, plus coûteuses seront les mesures additionnelles, jusqu'à ce que leur coût devienne prohibitif. Pendant ce temps, le niveau de sécurité, lui, n'augmentera pas de façon équivalente[164]. Le corollaire de cette sur-sécurité est que l'entreprise choisira, tôt ou tard, d'opter pour le strict minimum[165]. En fait, malgré toutes les mesures de précaution qu'une entreprise pourra adopter, il restera toujours un risque. Cette situation correspond à ce que Citron désigne comme étant le

[159] Danielle K. CITRON, « Reservoirs of danger: the evolution of public and private law at the dawn of the information age », (2006) 80 *CAL. L. REV.* 241
[160] *Id.*, 264; K. SOO HOO, préc., note 2, 3
[161] B. SCHNEIER, *Beyond Fear*, p.105 (2003): « [...] security is not just a matter of numerous countermeasures [...] »
[162] *Id.*, p. 90
[163] E. MACKAAY et S. ROUSSEAU, préc., note 31, p. 333
[164] N.W. VERMEYS, thèse doctorat, préc, note 152, p. 259
[165] LACHAPELLE et ST-GERMAIN, préc., note 12, p. 325 : « En l'absence d'un ensemble établi et admis de métriques permettant l'évaluation du retour sur investissement de la sécurité, il y a peu de chose qu'une organisation puisse faire dans ce domaine, si ce n'est appliquer des mesures dans le but d'éviter des incidents ou de minimiser l'impact d'un risque couru. »

risque résiduel de l'obligation de moyens : « no amount of due care will prevent significant amounts of sensitive data from escaping into the hands of cyber-criminals. Such data leaks will constitute predictable residual risks of information reservoirs »[166]. Ce même risque zéro n'existe pas[167], il y aura toujours un risque résiduel sur lequel l'obligation de moyens n'aura pas d'emprise. En ce sens, même si l'entreprise est débitrice de l'obligation, c'est la victime qui supporte les conséquences du risque résiduel. Dans un contexte où il est difficile pour l'entreprise de cerner le contenu de l'obligation de sécurité, le risque résiduel prend une proportion plus grande que normale. Il pourrait être plus avantageux pour l'entreprise de se contenter d'investir dans des mesures de base, moins dispendieuses, et de transférer le risque d'une atteinte plus complexe à prévenir sur la victime. Ainsi, l'incertitude de l'obligation de moyens encourage soit la sur-sécurité, soit la sous-sécurité. Aucune de ces options n'est souhaitable.

Il découle de ce qui précède que la « raisonnabilité » incertaine de l'obligation de moyens, même renforcée, ne favorise pas l'identification et l'adoption de mesures de sécurité afin de prévenir la survenance d'une atteinte. L'effet de l'obligation de moyens, même renforcée, est de faire supporter à l'individu les risques d'atteintes à la sécurité de ses renseignements personnels traités par l'entreprise à la place que ces risques soient assumés par l'entreprise dans le cadre de ses activités. Les fonctions préventives et dissuasives de la responsabilité civile sont donc mal servies par l'obligation de moyens, même renforcée.

(b) L'augmentation de l'intensité de l'obligation

Considérant l'incertitude relative au contenu de l'obligation de moyens, il semble émerger une certaine volonté de responsabiliser davantage les entreprises en augmentant

[166] D.K . CITRON, préc., note 159, 263 et 265
[167] N. W. VERMEYS, préc., note 7, p.110

l'intensité de l'obligation de sécurité informationnelle à une obligation de résultat[168], voire de garantie[169]. Ces deux intensités basent la responsabilité de l'entreprise sur la création du risque par la simple détention des renseignements personnels plutôt que sur sa faute.

Quoique nous soyons d'avis que d'élever l'intensité de l'obligation des entreprises ne soit pas approprié à l'heure actuelle, il convient de s'attarder brièvement aux rationalités sous-jacentes à la théorie du risque en matière de sécurité informationnelle et à son opportunité pratique.

i) Une obligation de résultat, en théorie

En matière de sécurité informationnelle, Citron soutient que le risque d'atteintes créé par le traitement des renseignements personnels militerait en faveur d'une obligation de résultat[170]. Au soutien de son argument, elle compare la création de banques de renseignements personnels par les entreprises à la construction des réservoirs d'eau pendant la Révolution Industrielle. Se basant sur une vieille décision britannique datant de 1868, *Rylands* c. *Fletcher*[171], elle fait une analogie entre la responsabilité de l'entreprise qui traite des renseignements personnels et celle du propriétaire du réservoir d'eau dans l'affaire *Rylands*. Dans cette affaire, le propriétaire avait été jugé responsable du préjudice découlant du déversement de son réservoir d'eau, lequel avait inondé la mine du terrain voisin. Le tribunal a jugé que tout préjudice étant la « conséquence naturelle » du risque créée par un propriétaire, sans égard à la faute du propriétaire ou celle du constructeur, devait être supporté par le propriétaire[172]. Il faut noter que cette décision s'ancre dans un contexte où les industries étaient en pleine croissance et peu

[168] D.K. CITRON, préc., note 159, appuyée par Chris Hoofnagle dans Chris HOOFNAGLE, « Internalizing Identity Theft », (2010) 13 *UCLA Journal of Law and Technology* 1, 29 et suiv.
[169] Julie MORINGIELLO, « Warranting Data Security », (2010) 5 *Brook J. Corp. Fin.&Com. L.* (2010) 72
[170] D.K. CITRON, préc., note 159, 268-269, citant les propos de Oliver Wendel Holmes : « the safest way to secure care is to throw the risk upon the person who decides what precautions shall be taken ».
[171] *Rylands* v. *Fletcher*, (1868) 3 L.R.E. & I. App. 330
[172] D.K.CITRON, préc., note 159, 270, citant *Fletcher* v *Rylands*, (1866) 1 L.R. Exch. 265, 279 : « a person who "brings on his land and collects and keeps there anything likely to do mischief if it escapes" must pay for all the damage that "is the natural consequence of its escape" ».

concernées par les matières dangereuses qu'elles dégageaient ou des situations dangereuses qu'elles créaient. Suivant cette analogie, Citron soutient que la création de « réservoirs » de renseignements personnels créerait un risque de fuites (« leaking databases ») entre les mains de tiers malveillants[173]. Ce risque de fuites serait la « conséquence naturelle » du risque créé par le traitement des renseignements. L'entreprise devrait donc supporter la responsabilité du risque créé, du seul fait qu'elle est à l'origine de la création de ce risque.

L'analogie de Citron souffre cependant d'une lacune majeure : contrairement à l'eau, les renseignements personnels ne créent pas de dommages à des tiers. D'abord, les renseignements personnels ne sont pas une source autonome de dommage. Les renseignements personnels ne se déversent pas, ne fuient pas, ne s'infiltrent pas et n'endommagent pas la propriété d'autrui. Il n'y a pas de « fuite » de renseignements personnels d'une banque au même titre qu'une fuite d'eau d'un réservoir. Une atteinte à la sécurité des renseignements personnels implique, certes, une vulnérabilité dans le système de sécurité de l'entreprise, mais surtout l'intervention d'un tiers. C'est leur utilisation subséquente qui peut être dommageable. Enfin, la victime du dommage est l'individu concerné par les renseignements, et non un tiers. En soi, une banque de renseignements personnels ne crée donc pas un risque latent au même titre que l'eau dans un réservoir.

Par contre, il faut souligner que le propos de Citron dénote une volonté de faire supporter aux entreprises qui traitent les renseignements personnels une responsabilité plus grande que celle qu'elles supportent actuellement. L'intensité d'une obligation plus grande se justifierait par des considérations morales et économiques[174]. D'un point de vue moral, la gravité potentielle du dommage, par sa gravité intrinsèque ou son étendue, militerait en faveur d'une obligation plus grande[175]. Par ailleurs, le bénéfice[176] que retire l'entreprise

[173] *Id.*, 279
[174] D.K. CITRON, préc., note 159
[175] Nous comprenons qu'un préjudice grave peut impliquer de faibles conséquences à grande échelle, de graves conséquences à grande échelle ou les deux.
[176] À ce sujet, voir: M. Maureen MURPHY, « Privacy protection for customer financial information, dans Ryan F. LEWIS et Gary M. HOWARD (*dir.*), *Information Security Laws: An Introduction,* Hauppauge, N.Y., *Nova Science Publishers,* 2012, p. 34: « With modern ability to gather and retain data, financial services businesses have increasingly found ways to take advantage of their large reservoirs of customer

du traitement des renseignements justifierait qu'elle en supporte la responsabilité[177]. L'entreprise devrait donc assumer le coût des mesures de précautions afin de prévenir une atteinte à la sécurité informationnelle. Elle devrait également être responsable du risque qu'elle a mal évalué ou qu'elle a refusé de supporter et être responsable du risque résiduel.

D'un point de vue économique, l'obligation de résultat se présenterait comme une solution afin d'éliminer les risques d'atteintes futures. L'avantage de l'intensité de cette obligation serait d'inciter les entreprises à restreindre le traitement des renseignements personnels à un niveau qu'elles peuvent véritablement contrôler[178], comme c'est le cas, par exemple, de la garantie de qualité ou de sécurité des fabricants[179]. À ce sujet, mentionnons qu'en 2011, une demande d'intenter un recours collectif a été déposée contre Sony en raison d'une faille dans la sécurité des comptes de quelques millions d'utilisateurs du réseau de jeu PlayStation[180]. Dans la foulée de cette affaire, la Commissaire a souligné, à juste titre : « I remain deeply troubled by the large number of major breaches we are seeing. Too many companies are collecting more personal information than they are able to effectively protect[181]».

De plus, en augmentant l'intensité de l'obligation, le fardeau de protection des renseignements personnels serait déplacé vers l'entreprise qui est dans une meilleure position que l'individu pour les protéger[182]. En effet, même si la victime est, ultimement, celle qui subit le préjudice, elle ne peut elle-même assurer la protection des renseignements personnels que l'entreprise traite dans son propre système.

---

information. Not only can they enhance customer service by tailoring services and communications to customer preferences, but they can benefit from sharing that information with affiliated companies and other willing to pay customer lists or targeted marketing compilations.»

[177] D.K. CITRON, préc., note 159, 288; Peter P.C. HAANAPPEL, (1978) 24 *McGill L.J.* 635, 636 : « […] celui qui tire profit d'une certaine activité socio-économique doit prendre le risque que cette activité cause à autrui du dommage pour lequel il sera responsable. »

[178] D.K. CITRON, préc., note 159, 266

[179] C.c.Q., art. 1726 et suiv., 1468, 1469, 1473 et 1474

[180] Cyberpresse, *Vie privée : des sanctions plus sévères pour les entreprises*, en ligne : http://argent.canoe.ca/lca/affaires/canada/archives/2011/05/20110504-174101.html (consulté le 8 octobre 2012)

[181] The Globe and Mail, *Canada's privacy Commissionner wants hefty fines for data breaches*, en ligne: http://www.theglobeandmail.com/technology/canadas-privacy-commissioner-wants-hefty-fines-for-data-breaches/article578748/ (consulté le 16 juillet 2012)

[182] D. K. CITRON, préc., note 159, 284

Économiquement, le coût des mesures de précautions devrait être supporté par la partie qui peut identifier les risques et adopter des contre-mesures.

Enfin, quant à la preuve, soulignons que l'obligation de résultat présenterait pour la victime des avantages indéniables. La victime n'aurait qu'à prouver le fait matériel de l'inexécution, soit une atteinte à l'une des composantes de ses renseignements[183]. L'entreprise ne pourrait renverser la présomption de responsabilité que si elle fait la preuve d'un événement qui lui est extérieur, qui ne lui est pas imputable et qui possède les caractères requis (événement imprévisible et irrésistible)[184]. L'absence de faute ne serait pas suffisante pour exonérer l'entreprise[185]. C'est sur elle que reviendrait le fardeau d'établir la cause de l'atteinte[186], ce qui allègerait le fardeau de la victime quant à la prévisibilité de la survenance de l'événement dommageable (faute) et la source de l'événement dommageable (causalité). Ainsi, l'exercice du recours de la victime en serait facilité.

En théorie, donc, l'augmentation de l'intensité de l'obligation aurait pour effet de déplacer le fardeau de protection des renseignements traités par les entreprises sur elles. Les fonctions préventives et dissuasives du régime de responsabilité en seraient du même coup favorisées.

ii) Une obligation de résultat, en pratique

Jusqu'à maintenant, en droit québécois, le professeur Vermeys est le seul qui ait étudié l'intensité de l'obligation de sécurité[187]. Tel que mentionné précédemment, il est d'avis que l'obligation de sécurité de moyens renforcée est l'intensité qui se révèle des dispositions législatives pertinentes étudiées et qui se présente, en pratique, comme

[183] J.-L. BAUDOUIN et P. DESLAURIERS, préc., note 33, par. 1-1359 – 1-1367
[184] C.c.Q., art. 1470
[185] BAUDOUIN et DESLAURIERS, préc., note 33
[186] *Id*.
[187] N.W.VERMEYS, préc., note 7, p. 95-118

l'intensité la plus appropriée[188]. Or, au regard de notre discussion précédente relative aux écueils de l'obligation de moyens renforcée, il est à propos de s'interroger à nouveau sur l'opportunité d'augmenter l'intensité de l'obligation de sécurité, en tout ou en partie.

En effet, le droit commun actuel foisonne de domaines où le législateur a imposé une obligation de résultat plutôt qu'une obligation de moyens à certains débiteurs pour des prestations spécifiques. Pensons, par exemple, à l'obligation de résultat du transporteur[189], à celle du dépositaire à titre onéreux[190], à celle du propriétaire d'un immeuble en décrépitude[191], à celle du propriétaire d'un animal[192], ou à celle de l'entrepreneur d'un ouvrage[193]. Dans d'autres domaines, même si, en général, le débiteur est assujetti à une obligation de moyens dans le cadre de ses activités, certaines obligations sont de résultat. Pensons, par exemple, à certaines obligations du notaire lorsqu'il agit à titre d'officier public pour la réception des actes[194] ou à celles du médecin pour le matériel et les produits qu'il utilise[195].

Pourquoi l'obligation de sécurité ne serait-elle pas une obligation de résultat ou, à tout le moins, pourquoi certaines facettes de l'obligation de sécurité ne seraient-elles pas assujetties à une obligation de résultat? Par exemple, au même titre que le transporteur, la délivrance d'un courriel d'un émetteur à son destinataire ne devrait-elle pas être une obligation de résultat? La conservation sécuritaire des renseignements personnels par l'entreprise ne devrait-elle pas être assujettie à une obligation de résultat au même titre que celle de dépositaire à titre onéreux[196]?

---

[188] *Id.*
[189] C.c.Q., art. 2034, art. 2037 et art. 2038
[190] C.c.Q., art. 2289
[191] C.c.Q., art. 1467
[192] C.c.Q., art. 1466
[193] C.c.Q., art. 2100
[194] *Loi sur le notariat*, L.R.Q., c. N-3
[195] Suzanne PHILIPS-NOOTENS, Pauline LESAGE-JARJOURA et Robert P. KOURI, « La responsabilité du médecin pour le matériel et les produits qu'il utilise », dans Suzanna PHILIPS-NOOTENS, *Éléments de responsabilité civile médicale- Le droit dans le quotidien de la médecine*, 3e édition, 2007
[196] *Contra* : notons que dans la décision *St-Arnaud* c. *Facebook*, 2011 QCCS 1506, la Cour Supérieure est venue à la conclusion qu'il existe un contrat d'adhésion entre un utilisateur et Facebook, mais que ce contrat n'est pas un contrat de consommation parce que l'accès au site est gratuit. Il semblerait donc que la communication de renseignements personnels pour l'obtention de services soit à titre gratuit.

Récemment, une auteure américaine, Juliet M. Moringiello, a avancé que les commerçants auraient une obligation de sécurité implicite de garantie dans le cadre du processus transactionnel lié à l'achat d'un bien ou d'un service. En effet, considérant que les individus acceptent d'échanger leurs renseignements personnels avec les entreprises, souvent dans le cadre de transactions commerciales, elle a recherché une obligation de sécurité plus élevée dans les termes implicites des contrats de biens ou de services[197]. C'est ce qu'elle appelle la garantie implicite de sécurité. La logique sous-jacente à la garantie implicite de sécurité serait la suivante :

(1) considérant que le commerçant impose au consommateur son architecture pour l'exécution d'une transaction commerciale;
(2) considérant que le commerçant connaît cette architecture et que le consommateur ne la connaît pas et n'a pas de moyen de la négocier; et
(3) considérant que le consommateur accorde sa confiance au commerçant quant à l'exécution d'une telle transaction;

le commerçant garantirait, à tout le moins implicitement au contrat principal, que le processus transactionnel imposée est sécuritaire[198].

Nous comprenons l'intérêt de cette proposition. Dans un contexte où le consommateur n'a pas l'opportunité de négocier avec le commerçant les mesures de sécurité qu'il souhaiterait voir mises en place pour la protection de ses renseignements personnels, ce moyen ferait supporter entièrement la responsabilité au commerçant. Il reviendrait alors au commerçant de diminuer son risque[199], soit : en prenant des mesures de précautions afin de protéger les renseignements personnels qu'il traite; et/ou en prévoyant une entente contractuelle similaire avec ses fournisseurs de services internet; et/ou, en contractant une assurance responsabilité[200].

---

[197] J. M. MORINGIELLO, préc., note 169
[198] *Id.*; Voir aussi : C.E. GIDEON, *préc*., note 3, 184 : « Consumers should not have to bargain with companies over the right to have their personal information kept safe. This ought to be considered a necessary part of doing business when a company seeks confidential customer data as part of its business model. »
[199] S'agissant d'une obligation de garantie, elle ne pourra l'éliminer.
[200] Quant aux ententes contractuelles entre les fournisseurs et aux polices d'assurances, voir *Aldo Group Inc.* c. *Chubb Insurance Company of Canada*, 2013 QCCS 2006. Dans cette affaire, Aldo poursuivait Chubb afin de la forcer à assurer sa défense dans une poursuite entreprise en Ontario par ses fournisseurs de

Mais revenons à notre question de départ : serait-il opportun d'augmenter l'intensité de l'obligation de sécurité à une obligation de résultat, voire de garantie?

Afin de déterminer l'intensité de l'obligation qui serait la plus appropriée, il faut notamment considérer l'aléa du résultat envisagé par les parties[201]. L'aléa est intimement lié à la notion de contrôle: le débiteur est-il en mesure de maîtriser les divers éléments susceptibles d'assurer la réalisation du résultat envisagé?[202] À cet égard, le rôle du créancier de l'obligation de sécurité doit aussi être considéré.

Dans le contexte de la sécurité informationnelle, tel que le souligne le professeur Vermeys, les aléas sont nombreux et leur prévisibilité variable rendant l'atteinte du résultat impossible[203]. Faut-il rappeler que la sécurité est un processus et non un produit[204]? Ajoutons également que le rôle de l'individu n'est pas complètement passif. Quoique la valeur du consentement soit controversée[205], l'individu doit consentir à l'utilisation de ses renseignements. Par ailleurs, même après avoir donné son consentement, il conserve un certain droit de regard sur le traitement de ses renseignements : il peut en demander l'accès, la rectification et même leur retrait[206]. En principe, l'individu n'est pas complètement passif dans le traitement de ses renseignements. Enfin, imposer une obligation de résultat ou de garantie à l'entreprise qui traite les renseignements personnels ne tient pas compte de l'architecture « en couches » (« layers ») d'Internet[207]. Les données voyagent, se fragmentent, se séparent et se recomposent, sans discrimination dans cette architecture décentralisée. Cette dernière est composée de différents intermédiaires, à chaque couche, parfois connus, mais aussi

---

passerelle et de processeur de paiement. Ces derniers alléguaient qu'Aldo avait fait défaut de respecter les principes PCIDSS et qu'elle avait fait défaut de préserver la confidentialité des renseignements personnels de ses clients. Chubb avait refusé d'assurer sa défense. Après avoir examiné les ententes contractuelles entre Aldo et ses fournisseurs de services, la Cour a donné raison à Chubb au motif que les ententes contenaient des admissions de responsabilité auxquelles Chubb n'avait pas consenti.

[201] Paul-André CRÉPEAU, *L'intensité de l'obligation juridique ou des obligations de diligence, de résultat et de garantie*, Cowansville, Yvon Blais, 1989, p.39

[202] *Id.*, 39-43

[203] N.W. VERMEYS, préc., note 7, p. 99-100, 110-111

[204] B. SCHNEIER, préc., note 161

[205] *Infra*, p. 58

[206] Code type, préc., note 16, art. 4.9; LPRPSP, art. 27, art.28, art.30 et art. 35

[207] Lawrence B. SOLUM et Minn CHUNG, «The layers principle: internet architecture and law », *University of San Diego School of law*, juin 2003, en ligne: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416263 (consulté le 26 août 2012)

inconnus de l'entreprise. Si l'entreprise peut, en principe, contrôler son architecture à l'interne, il est utopique de croire qu'elle peut contrôler l'architecture externe qui est nécessaire à ses communications ni même son arrimage.

Ainsi, en principe, et de façon générale, l'obligation de moyens renforcée demeure à notre avis l'intensité la plus appropriée à l'obligation de sécurité informationnelle. Par contre, cette intensité ne doit pas être figée. Nous anticipons qu'elle sera appelée à varier selon le contrôle que l'entreprise peut ou pourra exercer quant à certaines facettes de l'obligation de sécurité, au fur et à mesure de l'évolution de l'état des connaissances. Par ailleurs, plutôt que d'augmenter l'intensité de l'obligation vis-à-vis l'individu concerné, la solution réside peut-être dans la rédaction d'ententes contractuelles entre l'entreprise et ses intermédiaires de services.

***

Pour l'instant, nous retenons de ce qui précède que le cadre juridique encore indéfini de l'obligation de sécurité informationnelle n'offre pas la stabilité propice au développement de mesures de sécurité raisonnables. Ce constat amène certains auteurs à remettre en cause l'intensité de l'obligation de moyens, même renforcée, afin d'inciter davantage les entreprises à prévenir les atteintes eut égard aux risques qu'elles créent. Ce tiraillement est bien illustré par les propos de Nathalie Vézina, énoncés il y a déjà quelques années, au sujet de l'obligation générale de sécurité, sous le Code civil : « [e]n matière de sécurité, la mise en œuvre de la distinction obligation de résultat-obligation de moyens conduit à une situation dont on ne peut se satisfaire en terme d'indemnisation. »[208] Cette remise en question de même que l'évolution possible de l'intensité de l'obligation contribuent à l'instabilité du cadre juridique de l'obligation de sécurité. En conséquence, l'obligation de sécurité ne peut être sanctionnée avec rigueur par le régime de responsabilité civile.

[208] Nathalie VÉZINA, « Le préjudice corporel », (2006) EYB2006DEV1215, citée dans N.W. VERMEYS, préc., note 7, p. 110

Sous-partie 2 Un risque insignifiant

Il découle de nos constatations dans la Partie A que le risque que courent les entreprises si elles n'adoptent pas de mesures de sécurité raisonnables est peu élevé. Cette conclusion nous semble si évidente que nous n'en traiterons que brièvement dans cette sous-partie, pour éviter la redondance. Cette conclusion n'en est pas moins importante.

(a) Un risque économique insignifiant

Il existe une corrélation entre le coût d'investissement d'une entreprise dans des mesures de sécurité préventives et le risque financier qu'elle court sans ces mesures de sécurité[209]. Tel que l'écrivent Paul M. Schwartz et Edward J. Janger :

> «As for data security, one can generally expect companies to invest in it from the perspective of wealth-maximizing entities. In other words, firms will seek to calibrate security expenditures according to the level of legal liability and the financial risk that they bear from leaked information. Data security law also acknowledge, at least as a general matter, the legitimacy of economic constraints. It only requires data safeguards that are reasonable – not ones that are perfect, flawless or otherwise airtight.»[210] (soulignements ajoutés)

Suivant ce raisonnement, si l'entreprise ne risque pas d'être condamnée à réparer le préjudice qu'elle cause, il n'est pas nécessaire qu'elle adopte des mesures de sécurité afin d'éviter le coût de sa responsabilité.

Nous avons constaté, dans la Partie A, qu'il est souvent difficile pour la victime de prouver l'existence d'un préjudice subi et, lorsqu'elle le prouve, le montant des dommages est souvent minime (et sa réclamation rejetée) ou peu élevé. Nous avons également constaté qu'il est difficile pour la victime de prouver que l'événement

[209] *Supra*, p.41-42
[210] P.M. SCHWARTZ et E. J. JANGER, préc., note 115, 928

dommageable et ses conséquences sont prévisibles pour l'entreprise et que son préjudice résulte d'une atteinte particulière dans le système de sécurité de cette entreprise. Dans le contexte où l'exercice, avec succès, du recours en dommages-intérêts compensatoires est difficile et que les condamnations sont peu élevées[211], les fonctions préventives et dissuasives du régime de responsabilité civile à l'égard des entreprises ne peuvent s'accomplir.

(b) Un risque « réputationnel » insignifiant

La communication des renseignements personnels repose sur une relation de confiance entre les entreprises et leurs clients[212]. Afin de créer et maintenir cette confiance, nous serions portés à croire qu'une entreprise adoptera des mesures de sécurité raisonnables pour protéger les renseignements personnels qu'elle traite.

Certes, les entreprises qui possèdent de hauts standards d'intégrité adoptent les mesures nécessaires, non seulement afin de créer et préserver le lien de confiance qui les unit à leurs clients, mais également afin de préserver leur image et leur réputation. Ces entreprises ne sont pas visées par les mesures de contraintes juridiques. Pour les autres, nous soumettons que le régime de responsabilité civile ne crée pas un risque « réputationnel » suffisant vu : (1) l'insuccès des fonctions préventives et dissuasives du régime; (2) l'absence d'obligation de notification du régime et (3) le désintérêt de la clientèle des entreprises.

[211] Il existe par contre des cas où l'entreprise, notamment dans l'industrie bancaire, supportera pour ses clients les coûts d'une atteinte. Dans ce contexte, le dommage supporté peut être très élevé et milite en faveur de l'adoption de bonnes mesures de sécurité. Par exemple, dans la décision *Banque Royale du Canada* c. S. (M.), EYB 2010-172365 (C.S.), les clients de la Banque avait été victimes de fraude pour une somme totale de 345 388$. Plus récemment, dans la décision *Banque Royale du Canada* c. *Dionne*, EYB 2012-207119 (C.S.), la banque a réclamé la somme de 549 332,36$ qui a été fraudé du compte bancaire d'un de ses clients.

[212] Cynthia CHASSIGNEUX, « La confiance, instrument de régulation des environnements électroniques », (2007) 37 *R.D.U.S.* 441; The White House report, préc., note 142

i) L'insuccès des fonctions préventives et dissuasives de la responsabilité civile

Nous avons vu que la menace de poursuite a un effet préventif et dissuasif, c'est-à-dire qu'afin d'éviter de devoir rendre compte de ses actes dans une poursuite judiciaire publique, l'entreprise prendra les moyens nécessaires afin d'adopter un comportement socialement acceptable. Cependant, tel qu'expliqué dans la Partie A, il est difficile pour la victime d'établir que la cause de son dommage provient d'une atteinte dans le système de sécurité d'une entreprise donnée et que le préjudice en découlant était prévisible pour cette entreprise. Cette difficulté, comme nous l'avons déjà souligné, n'encourage pas la victime à exercer son recours en responsabilité civile contre l'entreprise. Conséquemment, l'entreprise n'a pas à défendre ni à expliquer, sur la place publique et dans le cadre de procédures judiciaires, l'insuffisance des moyens qu'elle avait adoptés afin de protéger les renseignements personnels de la victime.

ii) L'absence d'une obligation de notification

À l'heure actuelle, sauf en Alberta, il n'existe pas d'obligation statutaire pour une entreprise d'informer les personnes concernées de la survenance d'une atteinte aux mesures de sécurité ayant trait à leurs renseignements personnels:

> « L'approche qui prévaut actuellement au Canada est collectivement indésirable, car elle empêche les personnes dont les renseignements ont été compromis de prendre des mesures afin de se prémunir contre de possibles tentatives de fraude. En ne rendant pas ces incidents et leurs causes publics, les organisations victimes limitent également la capacité des autres organisations d'améliorer leurs pratiques et de mettre en place des programmes ou des solutions permettant de prévenir leur répétition. » [213]

[213] 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.4, en ligne : http://www.cicc.umontreal.ca/recherche/chercheurs_reguliers/benoit_dupont/chaire_note_recherche1.pdf

Cette absence d'obligation de notification est difficilement explicable et justifiable dans un contexte où l'entreprise a seulement une obligation de moyens, même renforcée, qu'elle exerce un contrôle sur les renseignements personnels qu'elle traite et qu'elle en retire un bénéfice. Par ailleurs, il tombe sous le sens commun qu'une partie, qui a une connaissance supérieure du risque, devrait aviser celle qui n'a pas le bénéfice de cette connaissance[214]. De cette façon, la personne concernée peut prendre des mesures afin de mitiger son préjudice, le cas échéant.

Certes, un certain nombre d'entreprises divulgue volontairement une atteinte aux mesures de sécurité, soit parce que certains des individus visés sont dans une juridiction qui l'exige ou soit parce qu'elles sentent qu'une telle divulgation est requise vu l'atteinte[215]. Tant le Commissariat à la protection de la vie privée du Canada (« **Commissariat** ») que la Commission d'accès à l'information (« **CAI** ») encouragent les divulgations volontaires et ont mis à la disposition des entreprises des guides pratiques pour les accompagner lors de la notification[216]. Le Commissariat a également mis en ligne un formulaire dynamique de signalement des atteintes à la vie privée à l'attention des entreprises[217]. Mais, cela n'est pas suffisant: « yet it seems likely that many other incidents go unreported given the lack of legal requirement to do so »[218]. Pour la Commissaire Jennifer Stoddart, cette situation est « inacceptable » et « injuste », particulièrement pour les entreprises qui divulguent volontairement[219].

(consulté le 10 juillet 2012) Voir aussi, aux États-Unis : J. K. WINN, « Are better Security Notification Laws possible? », 24 *Berkley Technology Journal* 33 (2009)

[214][214] T.J. SMEDINGHOFF, *préc.*, note 132, 43

[215] Michael GEIST, cité dans Ron DE JESUS, *Exploring Federal Privacy Breach Notification in Canada*, IAPP, 1er avril 2013, en ligne: https://www.privacyassociation.org/publications/2013_04_01_exploring_federal_privacy_breach_notification_in (consulté le 27 août 2013)

[216] COMMISSARIAT, *La protection de la vie privée au sein de votre entreprise- Guide en matière d'atteinte à la vie privée*, 2008, en ligne : http://www.priv.gc.ca/resource/pb-avp/pb_hb_f.pdf (consulté le 28 août 2013), COMMISSION D'ACCÈS À L'INFORMATION (« **CAI** »), *Aide-mémoire à l'attention des organismes et des entreprises : que faire en cas de perte ou de vol des renseignements personnels?*, avril 2009, en ligne : http://www.cai.gouv.qc.ca/documents/CAI_FI_vol_rens_pers_org-ent.pdf (consulté le 28 août 2013)

[217] COMMISSARIAT, *Rapport d'atteinte à la vie privée*, 2008, en ligne : http://www.priv.gc.ca/resource/pb-avp/pb_form_f.pdf (consulté le 28 août 2013)

[218] M. GEIST, préc., note 215

[219] CBC News, *Canada's privacy laws inadequate for digital age, watchdog says*, 23 mai 2013, en ligne: http://www.cbc.ca/news/technology/story/2013/05/23/technology-privacy-jennifer-stoddart.html (consulté le 27 août 2013)

C'est qu'en l'absence d'une obligation légale, les raisons de garder le silence sont nombreuses : coûts reliés à la notification elle-même, incidence négative sur les activités, la marque de commerce et la réputation de l'entreprise; incidence négative sur ses opérations futures; exercice de procédures judiciaires multiples, dont des recours collectifs potentiellement dommageables pour les finances de l'entreprise; et création de statistiques sur ses pratiques (bonnes ou moins bonnes)[220]. Les coûts reliés à la survenance de ces événements peuvent être suffisamment élevés pour que l'entreprise décide de taire l'incident plutôt que de le divulguer[221]. Ce faisant, personne n'est au courant du problème et la réputation de l'entreprise demeure indemne.

Pour l'instant, une entreprise peut décider de passer sous le silence tout incident menaçant la sécurité des renseignements personnels d'un individu. Or, les organismes chargés de la protection des renseignements personnels militent de plus en plus en faveur de l'adoption statuaire d'une obligation de notification[222]. Quoique nous soyons d'avis que l'obligation de notification est englobée par le droit civil québécois, nous étudierons, sous le Titre II du présent texte, l'opportunité d'encadrer une telle obligation dans les lois visant la protection des renseignements personnels.

[220] C.E. GIDEON, préc., note 3, 151; K. SOO HOO, *préc*., note 2, 9
[221] *Id*.
[222] CAI, *Rapport Quinquennal 2011, Technologies et vie privée, à l'heure des choix de société*, juin 2011, en ligne : http://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf (consulté le 27 août 2013) (voir les recommandations 7 à 9), COMMISSARIAT, *The case for reforming the Personal Information Protection and Electronic Documents Act*, mai 2013, en ligne : http://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.pdf (consulté le 27 août 2013) (voir : pressure point 2)

iii) Les individus désintéressés

Daniel Solove mentionne, dans son article intitulé « *Identity Theft, Privacy and the Architecture of Vulnerability* » que:

> « Placing the onus on individual to protect their privacy [...] can only be effective if individuals have the power to exercise their rights. Enforcement mechanisms that relay upon individual initiative often fail because individuals lack the knowledge, power, and resources to use them.»[223] (soulignements ajoutés)

Pour que le régime de responsabilité civile accomplisse ses fonctions et soit une mesure de contrainte juridique efficace, les individus doivent pouvoir exercer leur recours. C'est principalement sur eux que repose l'efficacité du régime. Malheureusement, le rapport de pouvoir entre les individus qui fournissent leurs renseignements et les entreprises qui les traitent n'est pas équilibré.

Dans un premier temps, les individus sont dans une situation où ils ont perdu le contrôle de leurs renseignements. D'une part, l'individu ne sait pas exactement à quoi il consent. Les clauses de consentement sont généralement rédigées de manière complexe et leur contenu est généralement large, de sorte que le consentement s'en trouve dilué[224]. En consentant à ce que ses renseignements soient collectés, sans même savoir s'ils seront protégés ou non, l'individu en perd le contrôle. D'autre part, bien que l'entreprise soit légalement tenue de mettre en place les mesures de sécurité exigées par un individu[225], ce dernier n'a pas le choix véritable de négocier la protection de ses renseignements. Il est peu réaliste de demander à un consommateur de s'informer des mesures de sécurité en place ou d'en exiger avant d'accepter de contracter avec une entreprise. Le consentement est généralement de type « take it or leave it », peu importe que la clause énonce des modalités de sécurité ou non. Par le consentement, l'individu perd le contrôle de ses

[223] D. SOLOVE, préc., note 90, 1228 et 1236
[224] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et web 2.0*, Montréal, Thémis, 2010, p. 163-200
[225] LCCTJI, art.26

données qui se retrouvent éparpillées. Sans contrôle, le pouvoir de l'individu de protéger ses renseignements personnels est illusoire[226]. Incidemment, l'entreprise ne se sent donc pas obligée de prendre des mesures de sécurité.

Dans un deuxième temps, même dans le cas où la responsabilité de l'entreprise est engagée, il est utopique de penser que l'individu exercera son pouvoir de choisir en tant que consommateur et modifiera ses habitudes à la suite d'une atteinte dans le système de sécurité d'une entreprise donnée[227]. En fait, le consommateur raisonnablement informé sait que la plupart des entreprises, à un moment ou à un autre de leur existence, devront faire face à une brèche dans leur système de sécurité[228]. La menace et le pouvoir du « boycott » ne sont donc pas très significatifs.

Finalement, les victimes n'ont pas nécessairement la volonté de sacrifier temps, argent et énergie dans l'exercice d'un recours en dommages-intérêts compensatoires qui, comme nous l'avons vu dans la première partie de ce texte, est loin d'être gagné d'avance. Qui plus est, les condamnations en dommages sont si peu élevées que, sauf par l'exercice d'un recours collectif, le jeu en vaut rarement la chandelle. La menace de poursuite pour les entreprises n'est donc pas très élevée.

***

[226] D. SOLOVE, préc., note 90, 1234-1236

[227] P.M. SCHWARTZ et E. J. JANGER, préc., note 115, 946-949. *Contra* : Rapport de la commissaire à la protection de la vie privée, 3 septembre 2004, cité dans *Turner* c. *Telus Communications Inc.*, 2005 CF 1601, par. 22 : « D'autre part, la nécessité pour Telus de demeurer concurrentielle a une incidence très concrète sur les employés. Si un tiers accédait à des données concernant la clientèle, la confiance qu'ont les consommateurs dans la capacité de l'entreprise de protéger ses renseignements serait sérieusement ébranlée. Sur le marché actuel où la concurrence va très vite, les consommateurs se tourneraient probablement vers une autre entreprise et pourraient ainsi infliger d'énormes pertes à Telus. » Voir aussi : John P. Hutchins et Renard C. François, « A new frontier : litigation over data breaches », (2009) *The pratical litigator*, p.55, disponible à l'adresse: http://www.troutmansanders.com/files/upload/hutchins-newfrontier.pdf « Ponemon's National Survey on Data breach Notifications, which surveyed more than 1,000 people who had received a notice of personal data security breaches, found that 20 percent had already terminated their relationship with companies that maintained their data. »

[228] *Id.*

Il découle de ce qui précède que les entreprises qui traitent des renseignements personnels ne courent pas un risque économique ou « réputationnel » significatif si elles n'adoptent pas des mesures de sécurité raisonnables afin de les protéger.

Conclusion de la partie B

Nous avons exposé dans cette partie que le flou normatif entourant le contenu et l'intensité de l'obligation de sécurité ne favorise pas l'adoption de mesures préventives. Considérant les difficultés que présente la sanction de l'obligation, le régime de responsabilité civile ne crée pas une contrainte significative afin d'inciter les entreprises à protéger la sécurité des renseignements personnels. Ainsi, l'échec de la fonction compensatoire du régime rend impossible l'accomplissement de ses fonctions préventives et dissuasives nécessaires à l'adoption de mesures de sécurité raisonnables.

***

Nous avons vu sous ce premier titre que l'échange auquel référait la Commissaire n'a pas encore ce caractère « mesuré et juste ». En effet, le régime de responsabilité civile actuel est mal adapté au contexte actuel de la sécurité des renseignements personnels. C'est un modèle réactif et principalement compensatoire. Il est plus intéressant pour l'entreprise de laisser le coût des mesures de précautions à celui ou celle qui subira directement le préjudice (la victime), plutôt que de l'intégrer aux coûts de ses activités. Or, l'entreprise est dans une meilleure position que la victime pour protéger les renseignements personnels qu'elle traite. Il faut donc revisiter le modèle de responsabilité civile afin de rétablir ses fonctions préventives et dissuasives et, ainsi, partager le fardeau de responsabilité plus adéquatement entre les individus et les entreprises.

TITRE II Vers un régime de responsabilité civile plus efficace

Nous avons constaté, sous le Titre I, que le régime de responsabilité civile compensatoire n'incite pas efficacement les entreprises à adopter des mesures de sécurité raisonnables. Devant ce constat, nous envisagerons deux solutions afin de responsabiliser efficacement les entreprises et favoriser l'adoption de mesures de sécurité raisonnables. Nous tenterons d'évaluer de façon prospective l'efficacité de ces deux solutions.

Dans un premier temps, nous revisiterons le régime de responsabilité civile actuel afin de considérer l'octroi de dommages-intérêts punitifs à la victime d'une atteinte à la sécurité de ses renseignements personnels. En effet, nous estimons que l'exercice du recours en dommages-intérêts punitifs pourrait avoir pour effet de favoriser l'exercice du recours en responsabilité civile par les victimes et l'adoption de mesures de sécurité raisonnables. Cependant, nous verrons que cette piste de solution ne serait efficace que dans un nombre limité de circonstances. Par conséquent, nous étudierons, dans un deuxième temps, l'opportunité d'encadrer statutairement une obligation de notification en cas d'atteinte aux mesures de sécurité ayant trait à la protection des renseignements personnels. En étudiant les conditions d'ouverture d'une telle obligation, nous verrons qu'elle serait plus facile à circonscrire pour les entreprises que l'obligation de sécurité en elle-même et, paradoxalement, qu'elle assurerait une fonction préventive.

Partie A Les dommages-intérêts punitifs

Dans le contexte où le recours en dommages-intérêts compensatoires de la responsabilité civile n'accomplit pas les fonctions préventives et dissuasives qui lui sont incidentes, il convient de considérer le recours en dommages-intérêts punitifs. Favoriser l'exercice de ce recours pourrait être une façon de contraindre les entreprises à adopter des mesures de sécurité raisonnables là où le recours compensatoire semble échouer.

Afin de bien comprendre notre propos, un bref rappel historique relatif à l'évolution du recours en dommages-intérêts punitifs dans le régime de responsabilité civile québécois s'impose.

Traditionnellement, la fonction essentiellement réparatrice du régime de responsabilité civile a exclu le recours en dommages-intérêts punitifs du droit de la responsabilité civile québécois[229]. Cette situation a perduré jusqu'au milieu des années '70 où le législateur québécois a introduit ou, devrions-nous dire, réintroduit[230], par le biais du second alinéa de l'article 49 de la Charte québécoise, le recours en « dommages exemplaires ». D'autres lois isolées ont par la suite introduit un recours en « dommages-intérêts punitifs », dont notamment, pour les fins de notre propos, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[231] (« Loi sur l'accès »)[232]. Finalement, avec la réforme du Code civil en 1994, le législateur québécois, en introduisant l'article 1621 sous le paragraphe « de l'exécution par équivalent », a relancé le débat silencieux qui avait cours jusqu'alors : les dommages-intérêts punitifs constituent-ils un redressement autonome et distinct du droit de la responsabilité civile québécois? Il n'en fallait pas plus pour que cette question sème la controverse en doctrine, les purs civilistes rejetant du revers de la main l'introduction en responsabilité civile d'un recours à saveur pénale[233]. Cette controverse a par ailleurs été alimentée, en 1996, par la trilogie des arrêts *Béliveau St-Jacques* c. *Fédération des*

[229] *Chaput* c. *Romain*, [1955] R.C.S. 853

[230] Tout dépendant du point de l'histoire auquel nous débutons l'analyse, nous pourrions utiliser le mot « réintroduit ». En effet, à une certaine époque, la séparation entre la responsabilité civile et la responsabilité pénale n'était pas très nette. Voir : Pauline ROY, *Les dommages exemplaires en droit québécois : instrument de revalorisation de la responsabilité civile*, thèse de doctorat, Montréal, Université de Montréal, 1995, p.16-95

[231] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q. c. A-2.1 (« **Loi sur l'accès** ») Cette loi a été sanctionnée le 1er octobre 1982 puis elle est entrée en vigueur par sections de 1982 à 1986. Notons que le recours en dommages-intérêts punitifs prévu par la *Loi sur la protection du consommateur*, RLRQ c P-40.1, pourrait être d'intérêt pour les fins de notre propos. Cependant, nous avons choisi de l'écarter en raison de l'analyse préliminaire qui doit être faite quant à l'application de la loi en matière de protection des renseignements personnels par les entreprises.

[232] Notons que la *Loi sur la protection du consommateur*, RLRQ, c P-40.1, (« **LPC** ») prévoit également un recours en dommages-intérêts punitifs. Nous avons écarté son étude pour les fins de la présente, notamment vu la décision *St-Arnaud* c. *Facebook*, préc., note 196. L'application de la LPC mérite une réflexion plus poussée.

[233] Pierre PRATTE, « Les dommages punitifs : institution autonome et distincte de la responsabilité civile », (1998) 58 *R. du B.*, 287

employées et employés de services publics inc.[234], *Augustus* c. *Gosset*[235] et *Québec (Curateur public)* c. *Syndicat national des employés de l'Hôpital St-Ferdinand*[236], rendus par la Cour Suprême du Canada. En effet, dans l'arrêt *Béliveau St-Jacques*, les propos du juge Gonthier ont été malencontreusement interprétés comme reconnaissant la subordination du recours en dommages exemplaires au recours compensatoire du droit de la responsabilité civile : «un tel recours ne pourra en effet être que l'accessoire d'un recours principal visant à obtenir compensation du préjudice moral ou matériel.[237] » La position du juge Gonthier a été critiquée, dans le même arrêt, par les juges La Forest l'Heureux-Dubé, dissidents. Pour eux, le recours en dommages-intérêts punitifs avait un caractère « autonome et distinct de la réparation de nature compensatoire.[238]» Cependant, cette autonomie demeurait « restreinte » et toute condamnation était subordonnée à la preuve préalable d'une faute au sens civil du terme[239].

Récemment, cette controverse a été dissipée grandement dans l'arrêt de la Cour Suprême du Canada *De Montigny* c. *Brossard (Succession)*[240] (« **De Montigny** »). Dans cet arrêt, le juge Lebel, rendant les motifs d'une Cour unanime, a reconnu le caractère autonome des dommages exemplaires prévus au second alinéa de l'article 49 de la Charte québécoise :

> « En raison de son statut quasi constitutionnel, ce document, je le rappelle, a préséance, dans l'ordre normatif québécois, sur les règles de droit commun. Nier l'autonomie du droit à des dommages exemplaires conférés par la Charte en imposant à ceux qui l'invoquent le fardeau supplémentaire de démontrer d'abord qu'ils ont le droit d'exercer un recours dont ils ne veulent pas, ou ne peuvent pas, nécessairement se prévaloir viendrait assujettir la mise en œuvre des droits et libertés que protège la Charte aux

[234] *Béliveau St-Jacques* c. *Fédération des employées et employés de services publics inc.,* [1996] 2 R.C.S. 345 (« **Béliveau St-Jacques** »)
[235] *Augustus* c. *Gosset*, [1996] 2 R.C.S. 268
[236] *Québec (Curateur public)* c. *Syndicat national des employés de l'Hôpital St-Ferdinand*, [1996] 3 R.C.S. 211 (« **St-Ferdinand** »)
[237] Béliveau St-Jacques, préc., note 234, par. 127
[238] *Id.*, par. 26
[239] Béliveau St-Jacques, préc., note 234, par. 27
[240] *De Montigny* c. *Brossard (Succession)*, [2010] 3 R.C.S. 64 (« **De Montigny** ») *Contra* : dans l'arrêt subséquent *Bou Malhab* c. *Diffusion Métromédia CMR inc.*, [2011] 1 R.C.S. 214 (« **Bou Malhab** »), la Cour Suprême, ayant refusé d'accorder des dommages-intérêts compensatoires, a estimé inutile qu'elle étudie la possibilité d'accorder des dommages-intérêts punitifs.

règles des recours de droit civil. Rien ne justifie que soit maintenu cet obstacle.[241]» (soulignements ajoutés)

L'arrêt De Montigny nous offre aujourd'hui l'occasion de relire l'art. 49 al. 2 de la Charte québécoise en tenant compte du caractère autonome du recours. Il convient de s'attarder plus en détail à ce recours afin de déterminer si son exercice pourrait avoir pour effet d'accomplir les fonctions préventives et dissuasives auxquelles le recours en responsabilité civile compensatoire semble échouer dans le contexte de la sécurité des renseignements personnels.

À cet égard, afin d'évaluer l'opportunité du recours, nous aborderons dans un premier temps l'étude des fonctions du recours en dommages-intérêts punitifs en relation avec les difficultés d'exercice du recours en dommages-intérêts compensatoires relevées sous le Titre I. Nous constaterons que les fonctions du recours en dommages-intérêts punitifs visent d'abord et avant tout la prévention des comportements qui constituent un écart marqué des normes de comportements socialement acceptables. Conséquemment, nous aborderons, dans un esprit plus pratique, l'exercice du recours en dommages-intérêts punitifs dans le contexte d'une atteinte à la sécurité des renseignements personnels. Nous étudierons les dispositions législatives qui fondent l'exercice du recours, les conditions d'ouverture du recours et l'évaluation du quantum des dommages-intérêts punitifs.

Sous-partie 1 Les fonctions des dommages-intérêts punitifs

Dans l'arrêt De Montigny[242], la Cour Suprême a énoncé très clairement les objectifs poursuivis par une condamnation en dommages-intérêts punitifs, soit : (a) la prévention, (b) la dissuasion, (c) la punition, et (d) la dénonciation[243].

[241] De Montigny, préc., note 240, par. 45
[242] De Montigny, préc., note 240
[243] *Id.*, par. 47 à 56. Ces objectifs ont d'ailleurs été réitérés très récemment dans l'arrêt *Richard* c. *Time inc.*, EYB 2012-202688 (C.S.C.), par. 154-157 (« **Richard** »)

À ces objectifs, nous ajouterons (e) d'autres objectifs qui, à notre avis, méritent d'être soulignés, soit : l'adoption et le maintien de bons comportements et l'encouragement de l'exercice du recours.

Voyons ces objectifs tour à tour.

(a) La prévention

Prévenir, c'est « empêcher que quelque chose se produise »[244]. Il s'agit de prévenir l'inexécution d'une obligation ou l'atteinte à un droit. Il ne s'agit pas de prévenir tous les comportements fautifs, mais seulement ceux dont la répétition doit être prévenue ou ceux qui méritent une dénonciation[245].

La fonction préventive des dommages-intérêts punitifs est énoncée à l'article 1621 al.1 du Code civil : « lorsque la loi prévoit l'attribution de dommages-intérêts punitifs, ceux-ci ne peuvent excéder, en valeur, ce qui est suffisant pour assurer leur fonction préventive. » Cette fonction doit exister tant au moment de la prise de décision d'octroyer des dommages-intérêts punitifs (lorsque discrétionnaire) que lors de l'évaluation de leur quantum.

À la lecture de l'article 1621, nous pourrions croire que la fonction préventive intervient seulement après l'inexécution de l'obligation ou l'atteinte à un droit. La fonction préventive vise en effet à prévenir la récidive du comportement socialement inacceptable. Or, s'il est vrai que la fonction préventive est réactive, elle est également proactive[246]. En effet, en étant consacrés dans le Code civil et dans différents textes législatifs, dont la Charte québécoise, les dommages-intérêts punitifs préviennent l'inexécution de l'obligation initiale ou l'atteinte initiale à un droit. À cet égard, la fonction préventive des dommages-intérêts punitifs joue un rôle comminatoire.

---

[244] Pierre PRATTE, « Le rôle des dommages-intérêts punitifs en droit québécois», (1999) 59 *R. du B.* 445, 507
[245] P. ROY, préc., note 230, p.3; *Richard*, préc., note 243, par. 155
[246] P. PRATTE, préc., note 244, 510

Enfin, nous verrons ci-dessous que la fonction préventive est la fonction des fonctions. Elle enchâsse et d'elle découlent toutes les autres fonctions. Ces dernières deviennent en fait des moyens d'accomplir la fonction préventive des dommages-intérêts punitifs[247].

La sanction en dommages-intérêts punitifs n'aura d'effet préventif que si elle s'applique à des comportements qui auraient pu être évitables[248] et à des personnes pour qui la condamnation représente une charge véritable eut égard à leur situation financière[249]. Enfin, la fonction préventive ne sera efficace que dans les cas où l'acte résulte du choix de l'individu et non d'un comportement spontané. Autrement, l'imposition de dommages-intérêts punitifs n'aura pas une portée préventive, mais seulement punitive[250]. Par exemple, dans l'arrêt *Richard*, la Cour Suprême a tenu compte du fait que le commerçant avait conçu, expressément et de façon calculée, sa publicité de manière à tromper son destinataire afin de justifier la condamnation en dommages-intérêts punitifs[251].

En matière de sécurité des renseignements personnels, nous entrevoyons que l'octroi de dommages-intérêts punitifs pourrait s'avérer pertinent afin de prévenir l'atteinte à la sécurité des renseignements personnels détenus par : (1) une entreprise ayant choisi de ne pas adopter des mesures de sécurité minimales[252]; ou (2) une entreprise qui, eut égard à la récurrence du traitement des renseignements personnels dans le cadre de ses activités, n'a choisi d'adopter que des mesures de sécurité minimales.

[247] De Montigny, préc., note 240, par. 50
[248] En ce sens et par définition, le risque résiduel ne peut être prévenu par le recours en dommages-intérêts punitifs
[249] P. ROY, préc., note 230, p. 196
[250] P. ROY, préc., note 230, p. 95
[251] Richard, préc., note 243, par. 181-183
[252] Par opposition à celle qui aura pris des moyens de sécurité raisonnables mais qui fera l'objet d'une atteinte.

(b) La dissuasion

La dissuasion est un moyen de parvenir à la prévention ou, dis autrement, un aspect de celle-ci. Dissuader c'est « détourner quelqu'un de son dessein »[253]. La dissuasion vise à « empêcher un individu d'agir comme il s'apprêterait à le faire »[254]. Elle vise l'auteur du comportement reproché, afin de le dissuader d'agir en premier lieu ou d'agir à nouveau. La dissuasion vise également à dissuader les membres de la collectivité en faisant de la condamnation de l'auteur fautif un exemple.

La dissuasion sera efficace dans la mesure où une personne, s'apprêtant à agir, procèdera à une analyse sommaire de la sanction anticipée et conclura qu'il est plus avantageux d'éviter la sanction que de risquer l'inexécution de l'obligation ou la violation d'un droit[255].

L'efficacité de la dissuasion dépendra du type de personne visée par la sanction. Le professeur Pierre Pratte (« Pratte »), dans son article « Le rôle des dommages punitifs en droit québécois », identifie quatre groupes d'individus. Il convient de le citer :

> « On peut diviser la population en quatre groupes. Le premier comprend les irréductibles que la peine n'intimide aucunement ou ceux à qui la mise à exécution de la menace fera peu mal. Il peut s'agir, par exemple, d'une personne insolvable qui n'a rien à perdre, rien à saisir. Le deuxième est composé des anormaux et de ceux qui agissent sous le coup de l'impulsion où entrent en jeu de fortes émotions. Pour eux, il est peu probable que la menace puisse les arrêter. En effet, la menace ne peut fonctionner lorsque la passion domine la raison. Le troisième réunit les personnes qui, pour des raisons morales ou à cause de l'éducation reçue, respectent la loi indépendamment de toute menace coercitive. Ces bons débiteurs agissent davantage par conviction personnelle que par crainte des sanctions légales. Le dernier groupe est formé de ceux dont les convictions sont plus fragiles et qui, sans l'existence d'un pouvoir de contrainte, se promèneraient de temps à autre du mauvais côté de la barrière. C'est à cette catégorie d'individus que la dissuasion générale s'intéresse plus particulièrement. En

[253] P. PRATTE, préc., note 244, p. 506
[254] *Id.*
[255] *Id*.

décourageant ces personnes, on prévient l'extension des violations de loi. »[256] (soulignements ajoutés)

Ainsi, la sanction ne sera efficace qu'à l'égard de cette dernière catégorie d'individus indisciplinés et non à l'égard des bons débiteurs n'ayant pas respecté, par malchance, leurs obligations. À titre d'exemple, mentionnons la décision récente *Townsend*, rendue par la Cour Fédérale, où la réclamation du demandeur a été rejetée en l'absence de preuve d'une conduite « délibérée, brutale, odieuse » témoignant « d'un mépris » du droit à la vie privée[257]. Dans cette affaire, la défenderesse avait, certes, enfreint certaines dispositions de la LPRPDE, mais sa faute était minime, résultait d'une simple erreur humaine et n'avait entraîné aucun préjudice pour le demandeur. Mais surtout, la défenderesse avait présenté ses excuses au demandeur et avait corrigé ses politiques déjà en vigueur.

Enfin, afin de dissuader un comportement futur, la preuve des ressources financières de l'auteur du comportement fautif peut devenir un facteur important, notamment lorsque l'auteur invoque des difficultés financières ou que ses ressources financières ont un lien direct avec sa conduite répréhensible[258] ou lorsqu'il existe d'autres circonstances permettant de conclure que la condamnation du défendeur à une somme peu élevée n'aura pas d'effet dissuasif. Nous reviendrons sur la situation financière du débiteur lorsque nous traiterons des facteurs pertinents à la détermination du quantum des dommages-intérêts punitifs[259].

Dans le contexte de la sécurité des renseignements personnels, nous entrevoyons que l'octroi de dommages-intérêts punitifs aurait un effet dissuasif sur les entreprises qui, connaissant leurs obligations, ne jugent pas opportun d'investir dans la protection des renseignements personnels qu'elles traitent ou lésinent sur le choix des mesures de sécurité à adopter.

---

[256] P. PRATTE, *préc.*, note 244, p. 515 et 516
[257] *Townsend* c. *Sunlife*, préc., note 95
[258] *Whiten* c. *Pilot Insurance Co.*, [2002], 1.R.C.S. 595, par. 119 (« **Whiten** »)
[259] *Infra*, p. 97-99

(c) La punition

Lorsque le tribunal décide de punir le débiteur, il indique « à l'auteur de la faute que son comportement et la répétition de celui-ci auront des conséquences pour lui »[260]. La punition a le sens de « châtiment ». L'auteur de la faute est puni parce qu'il le mérite.

Il faut souligner que cette fonction est souvent assortie d'un objectif de dissuasion et de prévention à l'égard de l'auteur fautif : « ne le refais plus ».

La fonction punitive des dommages-intérêts punitifs est controversée[261]. Sans alimenter cette controverse, il nous suffit de mentionner que la punition ne devrait pas être le seul objectif envisagé lorsque le tribunal décide d'accorder des dommages-intérêts punitifs afin de ne pas en faire une sanction de nature purement pénale[262].

En matière d'atteinte à la sécurité des renseignements personnels, il nous semble que l'octroi de dommages-intérêts devrait accomplir une fonction punitive que dans les cas extrêmement répréhensibles. Ce serait le cas, par exemple, d'une entreprise n'ayant pris aucune mesure de sécurité ou des mesures si négligeables ou désuètes qu'elles équivalent à une absence de mesure de sécurité.

(d) La dénonciation

La condamnation en dommages-intérêts punitifs joue également un rôle de dénonciation lorsque le tribunal désire souligner le caractère particulièrement répréhensible du comportement fautif dans l'opinion de la justice. La dénonciation se manifeste alors par l'octroi de dommages-intérêts punitifs et une déclaration qui, ensemble, visent à communiquer l'opinion de la justice à propos du caractère répréhensible de la conduite[263]. À cet égard, la dénonciation accomplit également une

[260] Richard, préc., note 243, par.155
[261] P. ROY, préc., note 230, 223-226
[262] *Chaput* c. *Romain*, [1955] R.C.S. 834
[263] Richard, préc., note 243, par. 155

fonction punitive rétributive vu l'opprobre qui lui est associé[264]. Dans une moindre mesure, la déclaration accomplit également une fonction préventive et dissuasive auprès de la collectivité[265]. Par exemple, une entreprise donnée, considérant la sanction d'une entreprise de son industrie, pourrait décider de modifier son comportement afin d'adopter des mesures qu'elle n'avait pas envisagées, qu'elle lésinait d'adopter ou qu'elle remettait à plus tard.

La dénonciation se justifie particulièrement dans le cadre du respect des droits et libertés fondamentales[266]. À cet égard, nous croyons que la dénonciation participe, dans des circonstances où il a été mis à mal, à la défense du droit atteint. Par exemple, dans l'arrêt De Montigny, le juge Lebel, rendant les motifs de la Cour, débute son explication relative aux objectifs visés par les dommages exemplaires par leur fonction dénonciatrice :

> « L'octroi de ces dommages a pour but de marquer la désapprobation particulière dont la conduite visée fait l'objet. Il est rattaché à l'appréciation judiciaire d'une conduite, non à la mesure des indemnités destinées à rétablir un préjudice réel, pécuniaire ou non. [267]»

En matière de protection des renseignements personnels, l'octroi de dommages-intérêts punitifs pourrait être opportun dans le cas où une entreprise, œuvrant dans une industrie particulière impliquant un traitement récurrent de renseignements particulièrement sensibles, a négligé d'adopter des mesures de sécurité raisonnables. Ainsi, l'octroi de dommages-intérêts punitifs pourrait non seulement avoir une fonction de dénonciation à l'égard de ses propres pratiques, mais également une fonction de dénonciation collective auprès des pratiques des entreprises de son industrie.

---

[264] *Id*.
[265] *Id*.
[266] De Montigny, préc., note 240, par. 47
[267] *Id*.

(e) Les autres fonctions

Outre les moyens précités, il existe d'autres moyens d'accomplir la fonction préventive des dommages-intérêts punitifs. Ces moyens sont en fait incidents aux fonctions précitées, soit la fonction persuasive et la fonction facilitatrice de l'octroi de dommages-intérêts punitifs.

D'abord, tout comme ils peuvent être dissuasifs, les dommages-intérêts punitifs peuvent, de façon positive, être persuasifs. En effet, les dommages-intérêts punitifs peuvent persuader un débiteur d'accomplir quelque chose qu'il n'avait pas initialement l'intention de faire, de telle sorte qu'il adoptera un meilleur comportement. Par exemple, dans le contexte de l'adoption de mesures de sécurité, une condamnation à des dommages-intérêts punitifs pourrait inciter l'entreprise condamnée à modifier l'ensemble de ses pratiques et prendre des mesures de sécurité raisonnables.

Ainsi, l'octroi de dommages-intérêts punitifs pourrait avoir pour effet de remédier à l'attitude volontairement laxiste, passive ou ignorante adoptée par les entreprises en raison du flou normatif discuté sous le Titre I[268]. La menace d'une condamnation en dommages-intérêts punitifs persuaderait une entreprise indisciplinée de faire un effort honnête afin de procéder à une évaluation globale des risques et à l'adoption de mesures de sécurité raisonnables.

Par ailleurs, et cette considération nous amène au second moyen, l'octroi de dommages-intérêts punitifs placera l'entreprise qui a pris des mesures de précautions dans une meilleure position juridique que celle qui n'en a pas pris du tout ou trop peu. En effet, il est illogique et frustrant que les débiteurs indisciplinés ou récalcitrants ne supportent pas de sanctions plus élevées que les entreprises qui ont adopté certaines mesures de sécurité, mais qui ont quand même été trouvées fautives. Tel que le souligne le professeur Pratte :

> « L'on peut excuser le débiteur qui a fait diligence dans la mise en place de moyens favorisant l'exécution, et ce, même si l'inexécution a eu lieu.

[268] *Supra*, p. 37-53

> Toutefois, on devrait sanctionner celui qui n'a rien fait pour empêcher la contravention ou qui s'est contenté de trop peu, alors que par un effort raisonnable il aurait pu éviter l'inexécution qui, bien que non souhaitée, paraissait prévisible »[269]. (soulignement ajouté)

L'octroi de dommages-intérêts punitifs, en sanctionnant un écart marqué des normes de comportement socialement acceptables, et non en sanctionnant une faute simple (ou un simple écart), favoriserait donc l'adoption et le maintien de bons comportements[270].

Enfin, l'octroi de dommages-intérêts punitifs aurait également pour effet de faciliter l'exercice du recours. En effet, nous avons vu, sous le Titre I, que les comportements fautifs ne donnent pas toujours lieu à des poursuites, soit parce que le dommage n'est pas susceptible d'indemnisation ou soit parce qu'il est difficile d'identifier, parmi toutes les sources du dommage, celle qui a causé le préjudice subi par la victime. L'octroi de dommages-intérêts punitifs favoriserait l'exercice des recours là où le recours en dommages-intérêts compensatoire semble échouer. En effet, nous verrons plus loin que l'appréciation de la preuve du préjudice et du lien causal doit tenir compte des fonctions du recours en dommages-intérêts punitifs et non être limitée par la fonction compensatoire du recours en dommages-intérêts[271]. Ainsi, l'exercice du recours s'en trouverait encouragé.

Certains perçoivent l'octroi des dommages-intérêts punitifs comme une « surindemnisation » ou un « enrichissement injustifié » de la victime. Or, cette perception omet de considérer que c'est l'individu, seul, qui exerce et supporte les difficultés de son recours. Tel que le souligne la Cour Suprême du Canada dans l'arrêt *Whiten*:

> « […] personne d'autre que l'appelante ne saurait être raisonnablement disposé à investir une somme d'environ 320 000$ en frais de justice dans un long procès afin d'établir que l'assureur s'est conduit de façon abominable dans ce dossier. La surindemdemnistation d'un demandeur est

[269] P. PRATTE, préc., note 244, 519
[270] *Id.*, 521 Voir notamment l'arrêt Richard, préc., note 243
[271] Infra, p.80-84

accordée en contrepartie de ce service socialement utile. » [272] (soulignements ajoutés)

Faciliter l'exercice des recours contribue aux fonctions préventives des recours en dommages-intérêts compensatoires et punitifs. En effet, la menace de l'exercice d'un recours n'aura un effet dissuasif (ou préventif) que si elle a une chance véritable de succès. L'octroi de dommages-intérêts punitifs inciterait les victimes à s'adresser aux tribunaux[273]. C'est la possibilité de cette « surindemnisation» qui permettrait à la victime de poursuivre celui qui autrement se tirerait à bon compte d'une situation qui déconsidère ses droits[274].

***

Il appert de notre étude des fonctions des dommages-intérêts punitifs que certaines d'entre elles sont communes à celles des dommages-intérêts compensatoires, notamment les fonctions préventives et dissuasives. Cependant, leur importance n'est pas la même. L'octroi de dommages-intérêts punitifs vise d'abord à prévenir le comportement répréhensible par opposition à l'octroi de dommages-intérêts compensatoires qui vise d'abord à réparer le préjudice subi par la victime. De fait, par opposition au recours compensatoire, le recours en dommages-intérêts punitifs vise précisément à sanctionner les comportements répréhensibles. Nous verrons que cette distinction est clé, tant dans l'appréciation des conditions d'ouverture du recours que de l'évaluation du quantum.

Vu ses fonctions, le recours en dommages-intérêts punitifs est d'intérêt. En matière de sécurité des renseignements personnels, il pourrait s'avérer être une mesure de contrainte efficace. Qui plus est, la fonction préventive des dommages-intérêts ne s'accomplirait que dans des circonstances limitées : soit afin de prévenir les comportements volontaires et

[272] Whiten, préc., note 258, par. 37
[273] PRATTE, préc., note 244, 543-544
[274] Pauline ROY, « Différentes manifestations de la peine privée en droit civil québécois », (2004) 38 *R.J.T.* 263, 289

récurrents qui s'écartent grandement des normes de comportements socialement acceptables. Seules les entreprises indisciplinées, c'est-à-dire celles qui ont connaissance de leur obligation de sécurité, mais qui choisissent de l'ignorer ou de faire le strict minimum, devraient être visées. Celles qui adoptent déjà de bonnes pratiques, quoiqu'elles puissent être trouvées fautives, ne devraient pas être condamnées à des dommages-intérêts punitifs. Ainsi, l'équilibre entre la protection des renseignements personnels et le besoin de leur utilisation commerciale serait préservé.

Sous-partie 2 — L'exercice du recours en dommages-intérêts punitifs dans le cadre d'une atteinte à la sécurité des renseignements personnels

Nous avons vu précédemment que le recours en dommages-intérêts punitifs peut constituer, en théorie, un modèle efficace afin de favoriser l'adoption de mesures de sécurité raisonnables. Il convient maintenant d'étudier, dans une perspective plus pratique, les dispositions légales pouvant fonder l'exercice d'un tel recours, les conditions d'ouverture du recours et l'évaluation du quantum. Dans l'étude des conditions d'ouverture et de l'évaluation du quantum, les fonctions précitées du recours doivent être considérées.

À l'issue de cette étude, nous pourrons avoir une meilleure idée de l'efficacité pratique de ce modèle de contrainte, en attendant que les praticiens du droit le mettent en œuvre dans le contexte spécifique de la sécurité des renseignements personnels.

(a) Les dispositions législatives fondant l'exercice du recours

Le recours en dommages-intérêts punitifs en est un d'exception. L'article 1621 du Code civil est clair à cet égard : « lorsque la loi prévoit l'attribution de dommages-intérêts punitifs » (soulignement ajouté). L'article 1621 du Code civil ne crée pas le recours. Une

disposition législative doit prévoir le recours. En droit québécois, nous pouvons envisager deux textes législatifs pouvant fonder l'exercice du recours en dommages-intérêts punitifs dans le contexte d'une atteinte à la sécurité des renseignements personnels.

D'abord, et sans équivoque, il y a la Charte québécoise. L'article 49 al.2 de la Charte québécoise prévoit : « en cas d'atteinte illicite et intentionnelle, le tribunal peut en outre condamner son auteur à des dommages-intérêts punitifs ». L'atteinte illicite visée est en fait l'atteinte illicite à un droit protégé par la Charte québécoise. En matière de sécurité des renseignements personnels, nous pouvons affirmer que l'atteinte illicite visera une atteinte au droit à la vie privée, protégé par l'article 5 de la Charte québécoise. En effet, le droit à la protection des renseignements personnels constitue l'une des facettes du droit à la vie privée[275]. Nous pouvons également avancer que l'atteinte illicite visera, dans certains cas, une atteinte au droit à la jouissance paisible et à la libre disposition des biens protégé par l'article 6 de la Charte québécoise. En effet, les conséquences d'une atteinte à la sécurité des renseignements personnels peuvent entraver le droit à la libre disposition de ses biens, même en l'absence de pertes financières[276].

Ensuite, la Loi sur l'accès prévoit, à l'article 167 [277]:

> « À moins que le préjudice ne résulte d'une force majeure, l'organisme public qui conserve un renseignement personnel est tenu de la réparation du préjudice résultant d'une atteinte illicite à un droit reconnu par le chapitre III.

[275] Voir les articles 3, 35 à 41 du Code civil et l'article 1 al.1 LPRPSP : « La présente loi a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil. » Au niveau fédéral, voir aussi l'article 3 LPRPDE: « La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »

[276] Par exemple, dans la décision *Unfasung*, préc., note 53, à la suite du vol de son identité, la demanderesse s'était vue privée l'accès à ses comptes bancaires et avait perdu sa cote de crédit.

[277] Notons que le libellé de l'article 167, al. 1 de la Loi sur l'accès semble faire de la protection des renseignements personnels une obligation de résultat.

> En outre, lorsque l'atteinte est intentionnelle ou résulte d'une faute lourde, le tribunal accorde des dommages-intérêts punitifs d'au moins 200$. » (soulignements ajoutés)

La Loi sur l'accès prévoit également une disposition similaire à l'art. 10 LPRPSP. En effet, l'article 63.1 impose à l'organisme public d'adopter des mesures de sécurité afin de protéger les renseignements personnels qu'il traite :

> « Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.[278]»

Cette disposition a été adoptée récemment, soit en 2006. Elle se situe sous le Chapitre III « Protections des renseignements personnels » et, partant, une violation à ses prescriptions pourrait être sanctionnée par des dommages-intérêts punitifs d'au moins 200$.

L'article 167 vise à compléter les recours déjà offerts aux citoyens en cas de violation à l'une des obligations prévues par la Loi sur l'accès par un organisme public[279]. Son premier alinéa s'inspire du recours sous l'article 1457 du Code civil et s'apparente au recours en dommages prévus par l'alinéa 1 de l'article 49 de la Charte québécoise. Son exercice dépend de la preuve des conditions essentielles de la responsabilité, soit : faute, dommage et lien causal[280]. Cependant, l'État ne pourra repousser sa responsabilité qu'en cas de force majeure[281]. L'article 167 est donc plus contraignant que l'article 1457 du Code civil et l'alinéa 1 de l'article 49 de la Charte québécoise. Quant au deuxième alinéa

---

[278] Loi sur l'accès, art. 63.1
[279] Lina DESBIENS et Diane POITRAS, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et Loi sur la protection des renseignements personnels dans le secteur privé, texte annotés*, Montréal, SOQUIJ, 1996
[280] Wellman, préc., note 62
[281] Raymond DORAY et François CHARRETTE, *Accès à l'information : Loi annotée, jurisprudence, analyse et commentaires*, Volume II, Cowansville, Yvon Blais, 2001 (à jour au 1er juillet 2013)

de l'article 167, il prévoit le recours en dommages-intérêts punitifs de façon similaire à celui de la Charte québécoise, à deux choses près: une faute lourde peut être suffisante pour ouvrir le recours et un seuil minimal de 200$ est fixé par la loi. Le législateur a donc voulu s'assurer que les atteintes intentionnelles des organismes publics soient sanctionnées par des dommages susceptibles d'avoir un effet dissuasif[282]. L'alinéa deuxième de l'article 167 est plus contraignant que celui de l'article 49 de la Charte québécoise à l'égard des organismes publics.

La Loi sur l'accès tire sa source de la Charte québécoise. Tout comme la LPRPSP, elle présente un caractère quasi constitutionnel[283]. Résumé en peu de mots, son objet est d'assurer une meilleure transparence de l'administration publique, notamment quant à la gestion des fonds[284]. Selon Pauline Roy (« Roy »), la présence du recours en dommages-intérêts punitifs dans la Loi sur l'accès s'explique par la volonté du législateur d' « inciter les employés de l'État à faire preuve de la plus grande diligence dans l'exercice de leurs fonctions, afin que les droits fondamentaux des citoyens ne soient pas impunément compromis. [285]»

À notre connaissance, aucune décision rapportée n'a encore analysé soigneusement l'octroi de dommages-intérêts punitifs sous l'article 167 de la Loi sur l'accès, sauf pour citer l'article et étudier son fonctionnement, jugé analogue à celui de l'article 49 de la Charte québécoise[286].

Il est surprenant que LPRPSP ne prévoie pas de disposition analogue à l'art. 167 al.2 de la Loi sur l'accès octroyant des dommages-intérêts punitifs en cas de violation d'une obligation prévue à son article 10. La LPRPSP constitue une loi particulière visant à protéger les renseignements personnels, déclinaison du droit à la vie privée, dans le contexte de leur traitement par les entreprises privées. Tant la LPRPSP que la Loi sur l'accès tirent leur source de l'article 5 de la Charte québécoise. Qui plus est, tant les

[282] Lacroix, préc., note 77
[283] Yvon DUPLESSIS et Jean HÉTU, *L'accès à l'information et la protection des renseignements personnels, lois indexée, commentée et annotée*, Brossard, CCH, 2001 (à jour au 8 avril 2011), p. 10 101
[284] *Id*., p. 10 401
[285] P. ROY, préc., note 230, p.273
[286] Wellman, préc., note 55; Routhier, préc., note 77

entreprises privées que les organismes publics sont maintenant assujettis à une obligation de sécurité analogue[287].

Comment expliquer qu'une même obligation reçoive des sanctions différentes selon l'identité de son débiteur ? Si l'on se reporte en 1982, année où est entrée en vigueur la Loi sur l'accès, nous pouvons penser que l'État exigeait et traitait déjà un volume impressionnant de renseignements personnels. Les renseignements personnels nécessitaient une protection accrue eut égard à leur gestion et à l'utilisation que pouvait en faire l'État et ses organismes. Si l'on se reporte en 1993, année de sanction de la LPRPSP, nous pouvons concevoir que l'utilisation des renseignements personnels n'avait pas encore atteint l'ampleur ni l'enjeu commercial qu'elle représente aujourd'hui pour les entreprises privées. Nous pouvons également penser que les individus conservaient la liberté de contracter avec les entreprises de leur choix. Nous pouvons aussi comprendre que l'adoption de la LPRPSP et, plus tard de la LPRPDE, ont été le résultat de compromis entre des intérêts concurrents, soit la protection de la vie privée et le besoin commercial d'accès aux renseignements personnels[288]. Enfin, l'article 49 de la Charte québécoise prévoyait déjà les recours en dommages-intérêts compensatoires et punitifs. Ainsi, à l'époque, il n'a peut-être pas été jugé nécessaire de prévoir dans la LPRPSP un recours en dommages-intérêts punitifs distinct.

Cependant, l'absence d'un recours en dommages-intérêts punitifs dans la LPRPSP est d'autant plus surprenante qu'une atteinte à l'obligation de sécurité sous la LPRPDE pourra, elle, donner lieu à une condamnation en dommages-intérêts[289]. Or, les dommages-intérêts de la *common law* accomplissent non seulement une fonction compensatoire, mais également des fonctions dissuasives et dénonciatrices associées aux dommages-intérêts punitifs[290]. Les recours sous la LPRPSP sont donc différents de ceux sous la LPRPDE. Pourtant, la LPRPSP n'est-elle pas censée être « essentiellement similaire » à la LPRPDE?

---

[287] Pour les entreprises privées, voir : LPRPSP, art.10. Pour les organismes publics, voir : Loi sur l'accès, art.63.1

[288] Pour une genèse de la LPRPDE, voir : *Englander* c. *Telus Communications Inc.*, 2004 CAF 387, par. 8 et suiv.

[289] LPRPDE, art. 14 et 16.

[290] Ward, préc., note 82

Enfin, d'un point de vue pratique, cette incohérence entre les trois lois peut donner lieu à des situations tout aussi incohérentes. Prenons l'exemple d'une personne qui conserve des renseignements pour un organisme public et une entreprise privée. Elle sera assujettie au recours en dommages-intérêts punitifs de l'article 167[291]. Elle sera également assujettie au recours en dommages-intérêts des articles 14 et 16 LPRPDE[292]. Mais, si elle conserve des données pour une entreprise régie par la LPRPSP, elle ne sera assujettie à aucun recours spécifique[293].

À l'heure actuelle, dans un contexte où le traitement des renseignements personnels est omniprésent et que l'équilibre entre leur protection leur besoin commercial vacille[294], l'absence d'un recours en dommages-intérêts punitifs dans la LPRPSP nous semble incohérente et difficilement justifiable. À notre avis, il serait à propos que le législateur révise sa position relativement à l'exercice d'un recours en dommages-intérêts punitifs dans le cadre de la LPRPSP afin de l'harmoniser tant aux recours sous la LPRPDE qu'aux recours sous la Loi sur l'accès. Pour l'heure, les organismes publics et les entreprises privées ne sont pas dans la même situation juridique quant à la sanction de l'obligation de sécurité. Il en est de même pour les entreprises privées assujetties à la LPRPDE et pour celles assujetties à la LPRPSP.

Pour les fins de la présente partie, nous étudierons l'exercice du recours en dommages-intérêts punitifs dans le droit québécois actuel, tant sous la Charte québécoise que sous la Loi sur l'accès.

[291] Voir les articles 67.2 et 68 de la Loi sur l'accès, lesquels se situent dans le chapitre III de la loi.
[292] Code Type, préc., note 16, principe 4.1.3. et LPRPDE, art.14 et 16
[293] Ce sont les articles 17 LPRPSP et 25 LCCJTI qui prévoient les obligations d'une personne qui conserve des données pour une autre.
[294] *Supra*, p. 2

(b) Les conditions d'ouverture

Le caractère exceptionnel du recours en dommages-intérêts punitifs implique la preuve de conditions d'ouverture. Tout dépendant du texte législatif autorisant l'octroi de dommages-intérêts punitifs, les conditions d'ouverture pourront varier.

Avant d'étudier les conditions d'ouverture sous la Charte québécoise et la Loi sur l'accès, quelques remarques préalables sur la nécessité de prouver les conditions essentielles du régime de responsabilité civile, à savoir la faute, le dommage et le lien de causalité. En effet, la pertinence préventive du recours en dommages-intérêts punitifs serait vaine si l'ouverture du recours se butait aux mêmes difficultés que le recours en dommages-intérêts compensatoires.

Si le caractère autonome de l'exercice du recours en dommages-intérêts punitifs a été consacré dans l'arrêt *De Montigny*, il en va différemment de son exercice[295]. Alors que les positions majoritaires et minoritaires dans l'arrêt *Béliveau St-Jacques* s'accordaient pour assujettir le recours en dommages-intérêts punitifs aux conditions essentielles du régime de responsabilité civile[296], les propos du juge Lebel dans l'arrêt De Montigny sèment le doute :

> « En raison de la finalité particulière du recours qu'il prévoit, l'art. 49 al. 2 peut, en effet, viser des actes et des conduites qui ne cadrent pas avec la notion de faute civile, ne tombant pas ainsi dans le domaine d'application du régime général de responsabilité civile.[297]»

Ces propos laissent croire qu'un comportement attentatoire à un droit protégé ne constituerait pas nécessairement une faute civile. Dis autrement, la preuve d'une faute civile ne serait pas nécessaire pour conclure à une atteinte illicite à un droit protégé. Le

[295] Voir pour une étude détaillée : Mélanie SAMSON, *Les interactions de la Charte des droits et libertés de la personne avec le Code civil du Québec : une harmonie à concrétiser*, Thèse de doctorat, Faculté de droit, Université Laval, 2012
[296] De Montigny, préc., note 240, par. 43
[297] *Id.*, par. 44

raisonnement nous semble tautologique. La violation injustifiée d'un droit protégé par la Charte québécoise constitue en soi une faute civile[298]. C'est donc le point de départ de l'analyse qui importerait afin de favoriser pleinement l'exercice des recours prévus par la Charte québécoise.

Subséquemment, dans l'arrêt *Bou Malhab* c. *Diffusion Métromédia CMR*, la juge Deschamps, rendant les motifs majoritaires de la Cour Suprême, a précisé :

> « L'article 49 de la *Charte québécoise* prévoit le droit à la réparation du préjudice causé par une atteinte illicite aux droits de la personne. La *Charte québécoise* n'a toutefois pas créé un régime indépendant et autonome de responsabilité civile qui ferait double emploi avec le régime général (*de Montigny* c. *Brossard (Succession)*, 2010 CSC 51, [2010] 3 R.C.S. 64, par. 44). Les principes généraux de la responsabilité civile servent toujours de point de départ pour l'octroi de dommages-intérêts compensatoire à la suite d'une atteinte à un droit (*Béliveau St-Jacques* c. *Fédération des employées et employés de services publics inc.*, [1996] 2 R.C.S. 345, par. 119 (le juge Gonthier) et par. 16 et 25 (la juge L'Heureux-Dubé, dissidente en partie), et *de Montigny*). [299]»

Il est clair que la juge Deschamps traite du recours en dommages-intérêts compensatoires de l'alinéa 1 de l'article 49 de la Charte québécoise. Cette position vaut-elle pour le recours en dommages-intérêts punitifs? Considérant que le concept d' « atteinte illicite » est à la base des deux recours de l'article 49, nous serions portés à croire que ces mots doivent recevoir la même interprétation. Si le législateur avait voulu y donner un sens différent, il l'aurait prévu[300].

Par ailleurs, selon notre compréhension, l'interprétation du juge Lebel n'exclut pas les conditions de la responsabilité civile. Son interprétation assure simplement que le droit de la responsabilité civile ne limitera pas la protection des droits et libertés prévus par la Charte québécoise en subordonnant l'ouverture de son recours à la démonstration d'une

[298] L'article 1457 du Code civil stipule : « Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle […] » (soulignements ajoutés)
[299] *Bou Malhab*, préc., note 240, par. 23
[300] *Contra* : si le législateur avait voulu que les recours soient assujettis à la preuve d'une faute, il l'aurait mentionné spécifiquement.

faute susceptible de compensation. Cette interprétation est conforme avec l'interprétation large et libérale que doit recevoir la Charte québécoise, de « manière à réaliser les objets généraux qu'elle sous-tend de même que les buts spécifiques de dispositions particulières »[301] et ainsi donner plein effet au recours de l'alinéa 2. Cette interprétation tient également compte des objectifs visés par le recours en dommages-intérêts punitifs, lesquels sont différents de ceux du recours compensatoire. Enfin, l'interprétation du juge Lebel ne nous semble pas contredire celle énoncée par la Cour Suprême dans l'arrêt *Béliveau St-Jacques*. Au contraire, son interprétation s'harmonise avec la démarche exposée par la juge l'Heureux-Dubé dans l'arrêt *St-Ferdinand* qu'il cite d'ailleurs:

> « Pour conclure à l'existence d'une atteinte illicite, il doit être démontré qu'un droit protégé par la Charte a été violé et que cette violation résulte d'un comportement fautif. Un comportement sera qualifié de fautif si, ce faisant, son auteur transgresse une norme de conduite jugée raisonnable dans les circonstances selon le droit commun ou, comme c'est le cas pour certains droits protégés, une norme édictée par la Charte elle-même […] »[302] (soulignements ajoutés)

Selon la juge L'Heureux-Dubé, l'atteinte illicite constitue une violation d'un droit protégé résultant d'un « comportement fautif ». Elle ne limite pas le « comportement fautif » à une transgression d'une norme de conduite jugée raisonnable selon le droit commun (la faute de l'article 1457 C.c.Q.). Le comportement fautif peut également être la transgression d'une norme édictée par la Charte. Ainsi, dans la mesure où un droit garanti sera violé de façon injustifiée, il y aura atteinte illicite résultant d'un « comportement fautif » au sens de la démarche proposée par la juge l'Heureux-Dubé. Ainsi, selon notre compréhension, tant la faute civile que la violation injustifiée d'un droit garanti pourront entraîner une « atteinte illicite » au sens de l'article 49 de la Charte.

Cette interprétation vaut également pour la preuve du dommage et du lien causal qui, même si elle est nécessaire, sera de nature différente. À cet égard, il faut se rappeler que les dommages-intérêts punitifs visent à sanctionner la conduite répréhensible du

[301] Béliveau St-Jacques, *préc*., note 234, par. 42
[302] St-Ferdinand, préc., note 236, cité dans De Montigny, préc., note 240, par. 58

défendeur et non à réparer le préjudice subi[303]. Ainsi, bien que la preuve du dommage demeure selon nous nécessaire (soit la preuve de l'atteinte au droit), il n'est pas nécessaire d'établir l'existence d'un préjudice indemnisable, c'est-à-dire d'un préjudice subi (soit la conséquence de l'atteinte au droit). Le recours en dommages-intérêts punitifs pourra s'ouvrir dans les cas où le préjudice est minime ou difficile à évaluer ou à démontrer[304]. Les conséquences, pécuniaires et morales, de l'atteinte illicite constituent un préjudice, quoique non indemnisable[305]. Il répugne de penser que les démarches préventives afin d'éviter les conséquences d'une atteinte illicite à un droit protégé auront pour effet de rendre irrecevable tout recours. Par ailleurs, l'atteinte illicite à un droit protégé ne constitue-t-elle pas en soi un dommage, à tout le moins extrapatrimonial, pour les fins du recours en dommages-intérêts punitifs[306]? Quant à la causalité, sa preuve s'établit en grande partie dans le contexte de l'examen de l'atteinte illicite et intentionnelle. En effet, le demandeur doit établir que le comportement (fautif ou injustifié) de l'entreprise rendait objectivement prévisible l'atteinte illicite au droit protégé. Il n'est pas nécessaire de prouver le lien de causalité entre le comportement (fautif ou injustifié) et les conséquences de l'atteinte. Dis autrement, il faut établir que le comportement de l'entreprise (fautif ou injustifié) rendait objectivement prévisible l'atteinte au droit à la vie privée, à la libre disposition des biens et/ou à la protection des renseignements personnels de l'individu concerné. Ainsi, selon notre compréhension, la preuve des conditions essentielles de la responsabilité civile demeure, mais leur appréciation doit être souple et adaptée aux objectifs du recours en dommages-intérêts punitifs.

Ceci étant dit, revenons aux conditions particulières d'ouverture du recours. Nous avons déjà mentionné que la Charte québécoise exige la preuve d'une atteinte illicite et

---

[303] De Montigny, préc., note 240, par. 65

[304] *Brault & Martineau inc.* c. *Riendeau*, [2010] R.J.Q. 507 (C.A.); Sébastien GRAMMOND, « Un nouveau départ pour les dommages punitifs », (2012) 42 R.G.D. 105

[305] Par exemple, les inconvénients liés à la mitigation des dommages dans le cas d'une atteinte qui n'a pas encore donné lieu à une conséquence réellement préjudiciable.

[306] De Montigny, préc., note 240, par 46 et 57 : l'absence de dommages-intérêts compensatoires ne rend pas irrecevable le recours en dommages exemplaires. Voir aussi : Mélanie SAMSON, « L'atteinte illicite à un droit protégé par la Charte québécoise : source d'un préjudice inhérent ? », *Revue des droits et libertés fondamentaux*, 2012, chron. n°20, en ligne : http://webu2.upmf-grenoble.fr/rdlf/?p=2703 (consulté le 26 août 2013)

intentionnelle à un droit protégé. L'article 167 al. 2 de la Loi sur l'accès exige, quant à lui, la preuve d'une atteinte intentionnelle ou d'une faute lourde.

Enfin, outre ces conditions textuellement prévues par les dispositions législatives autorisant le recours en dommages-intérêts, nous traiterons de deux autres conditions, identifiées par Pauline Roy, qui devraient être considérées dans l'octroi des dommages-intérêts punitifs lorsque cette décision est discrétionnaire[307].

(i) L'atteinte illicite

Tant la Charte québécoise que la Loi sur l'accès exigent la preuve d'une atteinte illicite afin d'octroyer des dommages-intérêts punitifs. Considérant que le recours sous l'alinéa 2 de l'article 167 de la Loi sur l'accès est analogue à celui sous l' alinéa 2 de l'article 49 de la Charte québécoise, nous présumerons que les enseignements récents de la Cour Suprême s'appliquent aux deux dispositions.

Nous retenons la définition de « comportement fautif » proposé par la juge l'Heureux-Dubé dans l'arrêt *Béliveau St-Jaques*. Dans le cas de la Charte québécoise, il faut démontrer que l'entreprise a commis une faute entraînant une violation à un droit protégé ou qu'elle a posé un geste violant un droit protégé par la Charte et que cette violation est injustifiée. Dans le cas de la Loi sur l'accès, l'alinéa 2 de l'article 167 édicte « en outre, lorsque l'atteinte est intentionnelle ou résulte d'une faute lourde […] ». Quoiqu'il ne soit pas question d'atteinte illicite au second alinéa, il nous semble que le second alinéa réfère à l' « atteinte illicite à un droit reconnu par le chapitre III » prévue à l'alinéa précédent. Ainsi, l'atteinte illicite consistera en l'omission de prendre les mesures de sécurité raisonnables ayant entraîné une violation du droit à la protection des renseignements personnels (faute).

[307] En effet, certaines lois ne prévoient aucune discrétion dans l'ouverture du recours lorsque les critères d'ouverture sont remplis, par exemple : *Loi sur la protection des arbres*, L.R.Q., c. P-37 et *Loi sur l'accès*, art. 167

Le critère de l'atteinte illicite nous permet de constater que la preuve de l'atteinte illicite semble moins exigeante sous la Loi sur l'accès que le recours sous la Charte québécoise. Certes, le demandeur devra établir la preuve d'un comportement fautif. Rappelons-nous, à cet égard, que le fardeau de preuve sera renversé. C'est l'entreprise qui devra établir qu'elle a adopté des mesures de sécurité raisonnables. Par contre, la Loi sur l'accès dispense le demandeur de la preuve de l'atteinte à un droit protégé sous la Charte, c'est-à-dire le droit à la vie privée. Si, dans certaines circonstances, cette preuve sera évidente, considérant l'éparpillement des renseignements personnels et la nature évanescente du droit à la vie privée, nous pouvons envisager des cas où cette preuve pourrait être difficile. Par exemple, si un organisme public communique, sans autorisation, un renseignement personnel public à un tiers, il n'y aura pas d'atteinte à la vie privée. Par contre, l'organisme public n'aura pas respecté ses obligations légales au sens de la Loi sur l'accès. En effet, la Loi sur l'accès a pour objectif de protéger les renseignements personnels. Quoique les renseignements personnels constituent une facette de la vie privée, c'est précisément leur atteinte que son recours en dommages-intérêts punitifs vise à sanctionner. Ainsi, nous croyons que l'atteinte illicite sera plus facile à établir sous la Loi sur l'accès.

Ce constat nous amène à réitérer la nécessité d'un amendement législatif à la LPRPSP. En effet, actuellement, les individus victimes d'une atteinte à la sécurité des renseignements personnels traités par un organisme public se trouvent dans une meilleure position juridique que s'ils sont victimes d'une atteinte à la sécurité des renseignements personnels traités par une entreprise privée. Pourtant, nous pouvons avancer, sans grand risque de nous tromper, que l'ensemble des entreprises privées traitent des renseignements personnels. Pire, de par leur nature commerciale, nous pouvons aussi penser qu'elles n'emploient pas autant de ressources que l'État à leur protection[308]. Il est donc nécessaire qu'elles soient contraintes par des mesures similaires à celles de l'article 167 al.2 de la Loi sur l'accès.

[308] K. Soo Hoo, préc., note 2

(ii) L' atteinte intentionnelle

Cette deuxième condition d'ouverture n'est pas exactement la même si le recours est intenté sous la Charte québécoise que sous la Loi sur l'accès. La Charte québécoise exige que l'atteinte soit intentionnelle. La Loi sur l'accès exige que l'atteinte soit intentionnelle ou qu'elle résulte d'une faute lourde.

Voyons d'abord le cas de l'atteinte intentionnelle. La juge l'Heureux-Dubé, dans l'arrêt St-Ferdinand, définit l'atteinte intentionnelle comme suit :

> « Dans cette perspective, afin d'interpréter l'expression «atteinte illicite et intentionnelle», il importe de ne pas confondre le fait de vouloir commettre un acte fautif et celui de vouloir les conséquences de cet acte. À cet égard, le deuxième alinéa de l'art. 49 de la *Charte* ne pourrait être plus clair: c'est l'atteinte illicite -- et non la faute -- qui doit être intentionnelle. En conséquence, bien que certaines analogies soient possibles, je crois qu'il faille néanmoins résister à la tentation d'assimiler la notion d'«atteinte illicite et intentionnelle» propre à la *Charte* aux concepts traditionnellement reconnus de «faute lourde», «faute dolosive» ou même «faute intentionnelle. […]
>
> En conséquence, il y aura atteinte illicite et intentionnelle au sens du second alinéa de l'art. 49 de la *Charte* lorsque l'auteur de l'atteinte illicite a un **état d'esprit** qui dénote un désir, une volonté de causer les conséquences de sa conduite fautive ou encore s'il agit en toute **connaissance** des conséquences, immédiates et naturelles ou au moins extrêmement probables, que cette conduite engendrera. Ce critère est moins strict que l'intention particulière, mais dépasse, toutefois, la simple négligence. Ainsi, l'insouciance dont fait preuve un individu quant aux conséquences de ses actes fautifs, si déréglée et téméraire soit-elle, ne satisfera pas, à elle seule, à ce critère.»[309] (soulignements et emphase ajoutés)

L'atteinte intentionnelle consiste à vouloir la conséquence du comportement fautif, soit l'atteinte au droit fondamental protégé ou, dans le cas de la Loi sur l'accès, au droit à la protection des renseignements personnels. Ainsi, l'atteinte par « inadvertance », comme

[309] St-Ferdinand, préc., note 236, par.118

ce fut le cas dans la décision Wellman, précitée, ne serait pas visée[310]. La véritable question qu'il faut se poser est donc : l'entreprise avait-elle l'intention de porter atteinte au droit à la vie privée de l'individu concerné? L'organisme public avait-il l'intention de ne pas protéger les renseignements personnels de l'individu concerné[311]? À notre sens, la question n'est pas : l'entreprise ou l'organisme public avait-t-il l'intention de causer les conséquences pouvant découler de l'atteinte au droit, par exemple : la peur, le stress, l'angoisse, la perte de temps, la fraude, le vol d'identité, la perte de crédit, etc. La réponse à cette dernière question sera la plupart du temps négative, surtout quand l'atteinte ne résulte pas d'une source interne. Évidemment, dans le cas où l'entreprise ou l'organisme public aura voulu les conséquences de l'atteinte au droit, l'examen de l'atteinte intentionnelle sera plus facile. Ceci étant dit, revenons à la véritable question : l'entreprise a-t-elle voulu porter atteinte au droit à la vie privée de la personne concernée ou avait-elle connaissance des conséquences extrêmement probables de son comportement? L'organisme public a-t-il sciemment décidé de ne pas prendre les mesures raisonnables afin de protéger les renseignements personnels ou avait-il connaissance des conséquences extrêmement probables de son comportement? En pratique, nous croyons qu'il sera peu fréquent qu'une entreprise ait sciemment voulu porter atteinte au droit à la vie privée ou que l'organisme public n'ait pas voulu protéger les renseignements personnels qu'il traite. Il faudrait une absence totale de mesures de sécurité pour satisfaire ce critère. Par ailleurs, la preuve de l'état d'esprit de l'entreprise ou l'organisme public sera très difficile à établir. Cela sera d'autant plus vrai dans les cas où il n'y aura pas de relation étroite entre le ou les individus concernés et l'entreprise ou l'organisme public.

Ce qui sera plus susceptible de se produire est le cas où l'entreprise ou l'organisme public a connaissance des conséquences naturelles ou immédiates ou extrêmement probables de sa conduite. Par exemple, nous pouvons envisager que ce sera le cas de l'entreprise ou de l'organisme public qui aura choisi d'adopter une attitude laxiste, passive ou volontairement ignorante relativement à la sécurité des renseignements personnels qu'elle

[310] Wellman, préc., note 55
[311] Dans ce cas-ci, notons que l'atteinte intentionnelle et la faute intentionnelle se recoupent considérant que le comportement fautif et l'atteinte illicite se superposent.

traite[312]. Il faut se rappeler que les dommages-intérêts punitifs sanctionnent les écarts marqués. Ainsi, le critère de l'intentionnalité ciblerait les entreprises ou les organismes publics dont les activités, à cause de la manière dont elles décident de les exercer, créent le risque d'une atteinte probable qu'elles ne peuvent ignorer. Cette atteinte ne devrait pas être supportée par l'individu concerné.

Il sera intéressant de voir comment la jurisprudence examinera le critère de l'atteinte intentionnelle dans le cas d'une atteinte à la sécurité des renseignements personnels. Récemment, dans l'affaire *Université Laval* c. *Association du personnel administratif de l'Université Laval*[313], l'arbitre de griefs a condamné l'employeur au paiement de dommages-intérêts punitifs équivalent aux frais du syndicat pour l'arbitrage. L'employeur avait demandé à un employé du Service de la sécurité des technologies et des systèmes d'information d'accéder au service de messagerie de l'association du personnel afin d'identifier l'employé qui avait, par courriel, porté à l'attention du syndicat une mesure contraire à la convention collective. L'arbitre en est venu à la conclusion que l'employeur, en agissant de la sorte, avait porté atteinte à un droit protégé par la Charte québécoise. Selon l'arbitre, l'employeur avait spécifiquement cherché à « lever, sans leur aval, hors de leur connaissance et sans raison, le voile assurant la confidentialité des participants à une communication reconnue privée »[314]. L'intention, dans ce cas-ci, était claire. Dans une autre affaire récente, la Caisse populaire Desjardins d'Aylmer a été condamnée à payer des dommages-intérêts punitifs à son client au motif qu'elle avait porté atteinte à sa réputation. La juge Marie Pratte note que pour que l'atteinte soit illicite, elle doit résulter d'un « comportement inadéquat »[315]. En l'espèce, la Caisse avait communiqué des informations erronées à des bureaux de crédit et avait négligé de les corriger. Le tribunal n'a eu pas de difficulté à conclure qu'il s'agissait d'une atteinte illicite au droit à la réputation. Quant à l'atteinte intentionnelle :

---

[312] Par exemple, dans la décision Nammo, préc., note 81, par. 69, la Cour Fédérale mentionne : « A credit reporting agecy make a profit from trading in the personnal information of others. Such business, perhaps more so than others, ought to be aware of the need of the accuracy and prompt correction of inaccurate information. Such businesses should expect to be held to account when they fail to do so.»

[313] *Université Laval* c. *Association du personnel administratif professionnel de l'Université Laval*, D.T.E. 2011T-189 (T.A.)

[314] *Id.*, par. 91

[315] *Caisse populaire Desjardins d'Aylmer* c. *Roy*, 2012 QCCQ 287, par. 104

> « En l'espèce, la Caisse n'avait certes pas le dessein bien arrêté de nuire à la réputation de son client. Toutefois, en repoussant unilatéralement la date d'échéance du contrat, et en permettant que les prétendus défauts de paiement soient enregistrés informatiquement et deviennent ainsi des données accessibles au bureau de crédit, la Caisse agissait « en toute connaissance des conséquences extrêmement probables » que cette conduite allait engendrer. »[316]

Enfin, la Loi sur l'accès autorise également l'exercice du recours en dommages-intérêts punitifs dans le contexte d'une faute lourde. Soulignons que c'est la faute qui est lourde et non l'atteinte. La faute lourde est définie à l'article 1474 du Code civil comme étant « celle qui dénote une insouciance, une imprudence ou une négligence grossière ». Le *Dictionnaire de droit privé* définit la faute lourde comme la « faute que ne commettrait pas même la personne la moins soigneuse »[317]. Vulgarisée à l'extrême, la faute lourde est celle qui révèle un « je-m'en-foutisme » envers les intérêts d'autrui, mais sans l'intention de nuire positivement à autrui. Ainsi, à notre avis, l'ignorance de l'entreprise ou de l'organisme public quant aux obligations lui incombant pourrait constituer une faute lourde.

Ce critère nous semble moins exigeant que l'atteinte intentionnelle[318]. Si ce critère peut s'expliquer sous la Loi sur l'accès, s'agit-il d'un bon critère dans le contexte de l'obligation de sécurité des entreprises?

Selon Pauline Roy, cette condition moins exigeante se justifie par la volonté du législateur de protéger la vie privée des citoyens contre les « intrusions injustifiées de l'État et de ses organismes»[319]. Qu'en est-il des intrusions injustifiées des entreprises et de leurs employés? Certes, l'ensemble des entreprises traite un volume de renseignements personnels. Elles utilisent également ces renseignements pour leurs fins commerciales.

---

[316] *Id.*, par. 124

[317] France ALLARD et *al*., *Dictionnaire de droit privé et lexiques bilingues, « Les obligations »*, Cowansville, Éditions Yvon Blais, 2003

[318] Notons qu'en common law, les dommages-intérêts punitifs ne seront accordés que si le défendeur « a eu une conduite malveillante, arbitraire ou extrêmement répréhensible, qui dérogent aux normes ordinaires de conduite », Whiten, préc., note 258, par. 94. Le critère d'ouverture dépasse donc la faute simple. Nous n'avons pas étudié où se situe ce critère par rapport à la faute lourde et l'atteinte intentionnelle.

[319] P. ROY, préc., note 230, p. 259

Cependant, l'entreprise n'est pas exactement dans la même situation que l'État ou ses organismes. Les individus peuvent techniquement exercer leur choix quoiqu'en pratique ce choix soit limité. Il faut également se rappeler l'existence de la libre concurrence entre les entreprises. Ainsi, les individus concernés ne sont pas complètement à la merci des entreprises comme ils sont à la merci de l'État. Afin de ne pas entraver inutilement la libre circulation des informations nécessaires aux activités commerciales, adopter la faute lourde comme condition d'ouverture du recours en dommages-intérêts punitifs ne nous semble pas adéquat.

Par ailleurs, le professeur Pratte émet des réserves sur l'opportunité de sanctionner une atteinte non intentionnelle par des dommages-intérêts punitifs. Selon lui, la plupart des activités humaines peuvent entraîner la violation d'un droit ou l'inexécution d'une obligation[320]. L'atteinte intentionnelle viendrait limiter les circonstances dans lesquelles la condamnation en dommages-intérêts punitifs est nécessaire sans paralyser les initiatives régulières qui pourraient, de manière non intentionnelle, porter atteinte à un droit[321]. De plus, vu le caractère indéfini de l'obligation de sécurité, sanctionner par des dommages-intérêts punitifs l'inexécution de l'obligation ou l'atteinte à un droit dans un contexte où l'entreprise ne se doutait pas de son inexécution ou de l'atteinte, même par insouciance, serait infliger un fardeau trop grand sur les entreprises. Dans ce cas, l'octroi de dommages-intérêts compensatoires serait suffisant pour prévenir un comportement similaire à l'avenir.

En fait, la différence entre l'insouciance de la faute lourde et la connaissance des conséquences naturelles ou extrêmement probables de l'atteinte intentionnelle est précisément la « connaissance ». Sanctionner l'absence de connaissance par des dommages-intérêts punitifs n'aurait pas la fonction préventive voulue. La fonction préventive ne sera accomplie que dans la mesure où l'entreprise a choisi d'être insouciante vis-à-vis les intérêts d'autrui. Dans ces cas, le critère de l'atteinte intentionnelle serait rempli parce l'entreprise « ne pouvait pas ne pas savoir » les conséquences de son geste. Ainsi, il nous semble que l'atteinte intentionnelle soit plus

[320] P. PRATTE, préc., note 244, 503-504
[321] *Id*.

fidèle aux fonctions préventive et dissuasive des dommages-intérêts punitifs. Ces fonctions n'ont d'emprise que sur les comportements dont les conséquences étaient susceptibles d'être évitées, c'est-à-dire dont les conséquences étaient soit voulues ou soit connues par l'auteur de l'atteinte illicite[322].

Ainsi, quoique nous réitérons l'intérêt d'un amendement législatif à la LPRPSP afin d'y introduire une disposition similaire à l'art. 167 al. 2, ce recours en dommages-intérêts punitifs ne devrait s'ouvrir que dans le cas d'une atteinte illicite et intentionnelle. De plus, le recours s'harmoniserait à celui de la Charte québécoise, d'où la LPRPSP tire sa source, quoiqu'il serait plus spécifique.

iii) Les autres conditions

Ce n'est pas parce que les conditions précitées sont réunies que des dommages-intérêts punitifs doivent être accordés. La Charte québécoise prévoit que des dommages-intérêts peuvent être accordés. Le tribunal dispose de la discrétion de les accorder ou non. Par contre, la Loi sur l'accès n'accorde pas de discrétion au tribunal. Si l'organisme public viole son obligation de sécurité prévue à l'article 63.1 ou si elle porte autrement atteinte au droit à la protection des renseignements personnels, et ce, de façon intentionnelle, le tribunal accorde des dommages-intérêts punitifs d'au moins 200$. La discrétion du tribunal se situe alors uniquement au niveau de la détermination du quantum.

Selon Pauline Roy, l'octroi de dommages-intérêts punitifs devrait être subordonné à la réunion de deux circonstances qui permettront de garantir que l'attribution de dommages-intérêts punitifs accomplira leur fonction préventive. Cette première circonstance est l'existence d'une relation de pouvoir entre l'auteur du comportement fautif et la victime[323]. Ainsi, les dommages-intérêts punitifs influenceront l'auteur du comportement fautif que si le « préjudice résulte de l'usage social ou intellectuel, sans égard aux risques

[322] P. Roy, préc., note 230, p.95
[323] P. ROY, préc., note 230, p. 231

qui peuvent en résulter de porter atteinte aux droits et libertés d'autrui.»[324] Ensuite, la seconde circonstance est celle d'un contexte qui présente « un certain élément de pérennité », dans le sens où l'auteur du comportement fautif sera appelé à prendre des décisions semblables pouvant avoir des incidences similaires dans le futur :

> « […] Le droit de la responsabilité civile doit permettre de prévenir les conduites prévisibles et susceptibles de se reproduire, parce qu'elles ne résultent pas d'un comportement isolé et intempestif, mais bien d'une décision réfléchie ou d'un automatisme qui se manifeste dans l'exercice d'une activité régulière, visant alors les attitudes récurrentes ou qui ont un effet de pérennité. »[325]

Au sujet de ces deux conditions, il convient de considérer l'arrêt Whiten[326]. Quoique cet arrêt ait été rendu en *common law*, son intérêt est indéniable dans l'appréciation du recours en dommages-intérêts punitifs en droit civil afin d'en préciser les balises[327]. Rappelons brièvement les faits. Dans cette affaire, le jury de la Cour de l'Ontario avait accordé des dommages-intérêts punitifs d'un million de dollars. Ce montant avait été réduit par la Cour d'appel à 100 000$, d'où le pourvoi devant la Cour Suprême du Canada. La Cour Suprême, dans une décision majoritaire, a rétabli le jugement de première instance. Cependant, le juge Lebel, dissident, aurait maintenu la décision de la Cour d'appel, notamment pour le motif que la somme d'un million de dollars dépassait les « limites rationnelles » appropriées à ce type de sanction :

> « Il n'a toutefois été produit aucune preuve indiquant que cette conduite survient régulièrement dans le cours des activités de Pilot.
>
> […]

---

[324] *Id.*
[325] *Id.*, p. 218
[326] Whiten, préc., note 258
[327] *Markakian* c. *Marchés Mondiaux CIBC inc.*, EYB 2006-106729 (C.S.); J.-L. BAUDOUIN et P. DESLAURIERS, préc., note 33, par. 1-380; Stéphane BEAULAC, « Les dommages-intérêts punitifs depuis l'affaire Whiten et les leçons à en tirer en droit québécois », (2002) 36 *R.J.T.* 637, p. 679 et s.; Suzanne GAGNÉ, « Les suites de l'affaire Whiten : l'affaire Markakian et les dommages-intérêts punitifs », *Développements récents en litige commercial*, 2007, Volume 277, 137

> Quelles fins serviraient donc des dommages-intérêts punitifs dans un tel contexte et, une fois ces fins déterminées, quelle serait la somme raisonnable et proportionnée? » […] En l'absence d'éléments de preuve relatifs à quelque faille de la culture de l'entreprise Pilot ou aux problèmes ou aux maux particuliers qui affligeraient le secteur de l'assurance, il ne reste que le désir de punir adéquatement certains actes […] »[328] (soulignements ajoutés)

Quoique les enseignements de l'arrêt Whiten doivent recevoir une portée limitée puisqu'ils sont tirés de la *common law*, il est intéressant de noter que le juge Lebel ait considéré si le comportement reproché avait eu lieu dans le cours des activités normales de la compagnie fautive afin de déterminer si la décision d'octroyer des dommages-intérêts punitifs respectait les rationalités (fonctions) qui lui sont sous-jacentes. Par ailleurs, notons que la vulnérabilité du créancier et l'abus de pouvoir ont été considérés, dans l'arrêt Whiten, dans les motifs de la majorité[329]. Ces notions ont cependant été considérées dans le cadre de la révision du quantum qui avait été accordé par le jury en première instance et non dans l'exercice de la discrétion relative à l'octroi des dommages-intérêts punitifs. Il n'en demeure pas moins que les deux circonstances additionnelles énoncées par Pauline Roy ont fait l'objet de considération par la Cour Suprême dans l'examen du recours en dommages-intérêts punitifs.

À l'instar de Pauline Roy, nous croyons que ces deux circonstances doivent être considérées dans le cadre du recours en dommages-intérêts punitifs. Autrement, l'utilisation du recours aux dommages-intérêts punitifs pourrait rapidement devenir un mode de punition supplantant le droit pénal. Une question demeure : ces deux circonstances doivent-elles être réunies au stade de l'ouverture de recours ou de l'évaluation du quantum? Il ne sera pas nécessaire de trancher cette question pour les fins de notre propos[330]. Par contre, nous pouvons soutenir que la réunion de ces deux circonstances sera généralement satisfaite dans le contexte du traitement des

[328] Whiten, préc., note 258, par. 159 et 160
[329] *Id.*, par. 114
[330] Comme piste de réflexion, mentionnons que le critère de « récurrence » de la conduite reprochée devrait être reconsidéré au regard de l'arrêt De Montigny. Dans cette affaire, faut-il le rappeler, l'auteur du crime s'était enlevé la vie. Il était donc clair qu'il n'y aurait pas de récidive à prévenir de cet auteur. Pourtant, la Cour Suprême a jugé bon d'accorder des dommages-intérêts punitifs afin de dénoncer la gravité des actes commis et de les dénoncer « comme une atteinte aux valeurs les plus fondamentales de la société ».

renseignements personnels, que ce soit par les entreprises privées ou par les organismes publics. Peut-être est-ce d'ailleurs pour cette raison que, dans la Loi sur l'accès, le législateur n'accorde pas de discrétion au tribunal une fois que l'atteinte illicite et intentionnelle ou que la faute lourde a été établie. En effet, la communication de renseignements personnels d'un individu à une entreprise ou un organisme public se fera toujours dans le contexte du désir et/ou de l'obtention d'un bien ou d'un service ou dans le contexte d'une relation employeur-employé. Dans ces cas, la nature de la relation entre l'individu et l'entreprise ou l'organisme public est souvent inégale : l'individu étant en position vulnérable. Quant à la « récurrence », l'obligation d'adopter des mesures de sécurité raisonnables n'a pas de fin. Tel que nous l'avons mentionné sous le Titre I, il s'agit d'un processus. Qui plus est, le traitement des renseignements personnels est récurrent dans la poursuite des activités commerciales des entreprises ou des activités de l'État. Ainsi, nous croyons que ces circonstances seront réunies dans la majorité des cas d'atteintes à la sécurité des renseignements personnels. Ces circonstances devraient être considérées dans le cas d'un recours discrétionnaire ou même militer en faveur de l'introduction d'un recours qui n'est pas discrétionnaire.

(c) L'évaluation du quantum

Tant le recours sous la Charte québécoise que la Loi sur l'accès octroient discrétion au tribunal afin de déterminer le montant des dommages-intérêts punitifs. Cependant, la Loi sur l'accès prévoit un seuil minimum établi par le législateur : un minimum de 200$ que nous qualifions de symbolique.

L'évaluation du quantum des dommages-intérêts punitifs doit servir à accomplir sa fonction préventive. Pour ce faire, l'article 1621 du Code civil réfère à une liste non exhaustive de facteurs qui doivent guider le tribunal dans l'exercice de sa discrétion, notamment : (i) la gravité de la faute du débiteur et (ii) sa situation patrimoniale ou

l'étendue de la réparation à laquelle il est déjà tenu envers le créancier (« la situation financière de l'auteur du comportement fautif ») [331].

Le montant qui sera attribué résultera de l'appréciation de ces facteurs. Il n'y a certes pas de formule préétablie. Il convient de commenter ces facteurs eut égard à l'exercice du recours dans le contexte d'une atteinte à la sécurité des renseignements personnels traités par une entreprise.

(i) La gravité du comportement fautif

La gravité du comportement fautif est, sans contredit, le facteur le plus important[332]. Les dommages-intérêts punitifs visent à sanctionner un comportement qui constitue un écart marqué du comportement socialement acceptable.

Le tribunal doit apprécier la gravité du comportement de façon globale, avant la violation, mais également après[333]. Ainsi, à notre avis, la gravité du comportement de l'entreprise qui aurait informé les individus visés par une atteinte et qui aurait pris des mesures pour limiter les conséquences de l'atteinte serait jugée moins grande que celle qui aurait tenté de camoufler l'atteinte.

À titre indicatif, la Cour Suprême, dans l'arrêt *Whiten*, a identifié, de façon non limitative, des circonstances pouvant influencer le caractère répréhensible de l'atteinte, soit : le caractère prémédité de la conduite, l'intention et la motivation du défendeur, le caractère prolongé de la conduite, le fait que le défendeur ait tenté de cacher sa conduite, le fait que le défendeur savait que sa conduite était fautive, le fait qu'il ait tiré profit de sa conduite, et le fait que le défendeur savait que sa conduite portait atteinte à un intérêt de valeur pour le demandeur[334].

---

[331] Voir *Cinar Corporation* c. *Robinson*, 2013 CSC 73, par. 133 et s., pour une analyse récente de ces critères.
[332] Richard, préc., note 243, par. 200
[333] *Id*.
[334] Whiten, préc., note 258, par. 113

La gravité du comportement répréhensible doit s'évaluer eut égard à la fonction préventive des dommages. Ainsi, un comportement qui n'est pas en soi gravement répréhensible pourra donner lieu à des dommages-intérêts punitifs s'il est prévisible qu'il se reproduira. Sa récurrence le rendra grave[335]. Inversement, un comportement gravement répréhensible ne justifiera pas l'octroi de dommages-intérêts punitifs s'il est isolé ou spontané. Rappelons-nous les propos précités du juge Lebel, dissident, dans l'arrêt *Whiten*[336]. Enfin, la Cour Suprême, dans l'arrêt *Richard*, mentionne que la relation de pouvoir qui existe entre l'entreprise et l'individu sera pertinente au stade de l'appréciation de la gravité de l'atteinte[337]. Cette appréciation des circonstances dans lequel intervient le comportement rejoint les critères d'ouverture du « pouvoir » et de la « récurrence », énoncés par Pauline Roy[338]. Il semble donc que la jurisprudence les considère lors de l'évaluation du quantum plutôt que comme condition d'ouverture du recours en dommages-intérêts punitifs.

(ii) La situation financière de l'auteur du comportement fautif

Afin d'être dissuasive, la situation financière de l'auteur fautif doit être considérée. Les dommages-intérêts punitifs n'accompliront pas leur fonction préventive si leur montant constitue une permission de continuer le comportement fautif[339].

Techniquement, la capacité financière du débiteur doit être prouvée[340]. Par contre, une preuve insuffisante, voire absente, n'aura pas pour effet d' « immuniser » le défendeur contre la possibilité d'une condamnation[341]. Le tribunal exercera sa discrétion, sans mesurer la capacité financière réelle, mais de façon raisonnable[342].

---

[335] La « récurrence » précitée a donc un impact au stade de l'évaluation du quantum.
[336] *Supra*, p. 92-93
[337] Richard, préc., note 243, par. 200
[338] *Supra*, p. 92-95
[339] Claude DALLAIRE, « Les dommages-intérêts punitifs et la diffamation : arme de destruction ou tire-pois? », *La diffamation*, Collection Blais, vol. 3, 2009, EYB2009CBL18, p. 3 : « les dommages-intérêts punitifs ne doivent pas devenir une « taxe d'amusement ». »
[340] C.c.Q., art. 1621
[341] Richard, préc., note 243, par. 213
[342] *Id*.

Quoiqu'il n'y ait pas de formule prédéterminée, certains facteurs peuvent être considérés pour établir la capacité financière du débiteur. D'abord, ce que le défendeur devra payer pour indemniser les conséquences de son comportement fautif doit être considéré[343]. Une condamnation en dommages-intérêts compensatoires peu élevée peut justifier pour le tribunal d'accorder des dommages-intérêts punitifs plus élevés[344]. Cette logique sied particulièrement bien à notre contexte où les dommages sont inexistants ou minimes. Les ressources financières investies par l'entreprise afin d'informer les individus concernés de l'atteinte et de limiter les conséquences de l'atteinte devraient, à notre avis, être également considérées à ce stade. Ensuite, l'identité du débiteur peut être un indicateur de sa capacité financière. Les institutions financières et les grandes entreprises seront susceptibles d'être condamnées à des montants plus élevés que les individus ou les petites et moyennes entreprises, et ce, à faute égale. La Cour Suprême, dans l'arrêt *Whiten*, nous met cependant en garde d'attribuer d'un caractère « anthropomorphique » aux grandes sociétés[345].

Enfin, certains auteurs soutiennent qu'il faut également tenir compte du bénéfice retiré par l'auteur du comportement fautif[346]. Le montant des dommages-intérêts punitifs doit être tel qu'il doit en perdre le bénéfice[347]. Or, nous pouvons déjà anticiper de nombreuses difficultés quant à la preuve de ce bénéfice en matière d'atteinte à la sécurité des renseignements personnels. D'abord, s'agit-il du bénéfice réalisé par l'entreprise à l'égard de l'individu concerné ou du profit général qu'elle a retiré de son comportement fautif dans le cadre de l'ensemble de ses activités? Ensuite, comment établir la valeur du bénéfice retiré? Certes, l'entreprise retire un bénéfice commercial en utilisant les renseignements personnels dans le cadre de ses activités. Mais comment le quantifier? En considérant le chiffre d'affaires, le budget alloué à la sécurité, le profit réalisé dans l'année, l'indemnisation de la victime et\ou l'indemnisation de tous les clients visés s'ils avaient intenté des procédures? La détermination du bénéfice retiré peut facilement

[343] C.c.Q., art. 1621
[344] DALLAIRE, préc., note 339, p. 7; Richard, préc., note 243, par. 214
[345] Whiten, préc., note 258, par. 121
[346] Dans l'arrêt Richard, préc., note 243, la Cour Suprême a tenu compte du fait que la publicité trompeuse de l'intimée avait été financièrement très profitable, quoiqu'aucun chiffre précis n'ait été mis en preuve. La Cour a estimé des dommages-intérêts punitifs au montant de 15 000$.
[347] À ce sujet, voir P. Roy, préc., note 230, p. 539

devenir une question très litigieuse et complexe ayant pour effet de décourager l'exercice du recours.

Afin d'éviter des situations où la conclusion sur la responsabilité de l'auteur du comportement fautif pourrait être influencée par sa capacité financière ou afin d'éviter que la preuve de la capacité financière ne devienne l'enjeu du litige, certaines solutions peuvent être envisagées[348]. Par exemple, l'établissement d'un seuil minimal, tel celui de l'article 167 de la Loi sur l'accès, peut être utile afin de guider le tribunal. Ainsi, la victime saura exactement le minimum qu'elle peut recevoir si elle entreprend des procédures. L'entreprise, quant à elle, connaîtra le risque minimal auquel elle s'expose. Enfin, le tribunal aura un point de départ pour son analyse. Dans d'autres cas, il y aura lieu de considérer, par exemple, la scission d'instance. Ainsi, selon les circonstances, le demandeur devra établir, dans un premier temps, les conditions d'ouverture du recours en dommages-intérêts punitifs et, dans un deuxième temps, le quantum approprié.

***

Le caractère autonome du recours en dommages-intérêts punitifs sous l'art. 49 al.2 de la Charte permet à la victime d'exercer un recours dans des circonstances où l'exercice de son recours compensatoire n'est pas avantageux ou même possible. En effet, l'exercice du recours en dommages-intérêts punitifs peut remédier à plusieurs des ratés de l'exercice

[348] L'attribution de dommages-intérêts calculés sur la base d'un pourcentage du chiffre d'affaires de l'entreprise pourrait également être considérée. À cet égard, notons que le projet de *Règlement du parlement européen et du conseil 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 (règlement général sur la protection des données)* prévoit une condamnation équivalente à deux pourcent du chiffres d'affaires mondial annuel d'une entreprise qui, par négligence, omet de notifier une violation de données à caractère personnel : COMMISSION EUROPÉENNE, Proposition de *Règlement du parlement européen et du conseil 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 (règlement général sur la protection des données)* en ligne : http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf (consulté le 6 janvier 2013)

du recours de responsabilité civile compensatoire en matière de sécurité des renseignements personnels.

Outre la Charte, il existe d'autres dispositions qui peuvent fonder l'exercice d'un recours en dommages-intérêts punitifs. En effet, la Loi sur l'accès prévoit un recours en dommages-intérêts punitifs non discrétionnaire et assorti d'un seuil minimal. Cependant, ce recours vise les organismes publics. Nous avons vu l'intérêt que pourrait représenter l'introduction d'un recours en dommages-intérêts punitifs analogue à celui de l'article 167 de la Loi sur l'accès dans la LPRPSP. L'introduction d'un tel recours permettrait une meilleure cohérence des sanctions, non seulement à l'égard des organismes publics, mais également à l'égard des entreprises privées régies par la LPRPDE. En effet, la LPRPDE prévoit un recours devant la Cour Fédérale et habilite cette dernière à condamner l'entreprise fautive à des dommages-intérêts ayant les mêmes objectifs que les dommages-intérêts punitifs[349].

Cependant, le recours en dommages-intérêts punitifs ne règle pas tous les problèmes. Par exemple, il n'a pas pour effet de clarifier l'obligation de sécurité des entreprises. Il amène également des difficultés qui lui sont propres. Notamment, en matière de sécurité des renseignements personnels, la preuve de l'atteinte intentionnelle serait limitée, la plupart du temps, aux «conséquences extrêmement probables » de la conduite. Cependant, nous persistons à croire que la connaissance des conséquences extrêmement probables du comportement fautif aurait de bonnes chances d'être prouvée dans le contexte d'une atteinte aux mesures de sécurité ayant trait à la protection des renseignements personnels. Ce serait le cas de l'entreprise qui n'aurait adopté aucune mesure de sécurité ou de celle qui en aurait adopté trop peu. Il lui serait difficile de prétendre qu'elle ignorait les conséquences probables de sa conduite. À cet égard, la décision dans l'affaire *Caisse populaire Desjardins d'Aylmer* appuie notre position. Enfin, depuis que le recours en dommages-intérêts punitifs est devenu autonome avec l'arrêt De Montigny, sauf dans des cas exceptionnels[350], les condamnations demeurent peu élevées et symboliques[351].

[349] LPRPDE, art. 14 et 16; Ward, préc., note 82
[350] Brault & Martineau inc., préc., note 304 (2 000 000$ - recours collectif); Unfasung, préc., note 53 (40 000$); *Compagnie d'assurances Standard Life* c. *Tremblay*, 2010 QCCA 933 (100 000$); *M.C.* c.

Conclusion de la partie A

Il découle de ce qui précède que l'autonomie du recours en dommages-intérêts punitifs sous la Charte peut remédier à plusieurs des lacunes du recours en dommages-intérêts compensatoires en matière de sécurité des renseignements personnels. En effet, la preuve des conditions essentielles de la responsabilité civile tient compte des objectifs de prévention et de dissuasion du recours en dommages-intérêts punitifs. Cela est particulièrement vrai pour la preuve du préjudice. Les dommages-intérêts punitifs pourraient rééquilibrer la pression économique et « réputationnelle » sur les entreprises afin de favoriser l'adoption de mesures de sécurité raisonnables, sans pénaliser les entreprises qui ont déjà de bonnes pratiques. Le recours en dommages-intérêts punitifs pourrait donc s'avérer un moyen de contrainte efficace.

Cependant, le recours ne sera efficace que s'il est exercé avec des chances véritables de succès. D'abord, même en admettant que le recours soit autonome, il n'est pas garanti que les victimes aient la volonté d'intenter une procédure judiciaire en l'absence d'un préjudice subi, seulement dans le but de prévenir un comportement fautif ou injustifié similaire dans le futur. D'où l'intérêt de prévoir une disposition spécifique dans la LPRPSP prévoyant non seulement un recours, mais également un seuil minimal. Le seuil minimal aurait pour effet d'encourager les victimes à exercer leur recours. Ensuite, les tribunaux devront également s'adapter à l'octroi de dommages-intérêts punitifs, en l'absence de toute autre indemnisation[352]. Enfin, tout comme le recours en dommages-intérêts compensatoires, la victime ne pourra intenter un recours en dommages-intérêts punitifs que si elle a connaissance de l'atteinte. L'exercice du recours est donc subordonné à la réalisation d'un événement réellement préjudiciable, par exemple la

---

Service d'aide à domicile Bélanger inc., 2011 QCCS 4471 (50 000$); *Cinar Corporation* c. *Robinson*, 2013 CSC 73 (500 000$)

[351] Caisse populaire Desjardins d'Aylmer, préc., note 315 (750$); De Montigny, préc., note 240 (10 000$); Richard, préc., note 243 (15 000$); Ward, préc., note 82; *Berthiaume* c. *Carignan*, 2013 QCCS 1357 (5000$); *Corbin* c. *Drouin*, 2011 QCCQ 10552 (750$) ; *Commission des droits de la personne et des droits de la jeunesse* c. *Courchesne*, 2013 QCTDP 24 (2000$); *Gilbert c. Drolet (Solution Extérieur)*, 2010 QCCQ 9478 (1000$); *Lefrançois* c. *9127-0587 Québec inc.*, 2013 QCCQ 2638 (750$); *Sauvageau* c. *Raymond*, 2012 QCCQ 8326 (3500$); et *Tremblay* c. *Weyman*, 2011 QCCQ 16099 (3000$)

[352] *Commission des droits de la personne et des droits de la jeunesse* c. *Parent*, 2012 QCTDP 12

fraude bancaire ou le vol d'identité, ou à la notification à l'individu de la survenance d'une atteinte.

Partie B L'obligation de notification

Le corollaire de l'obligation de sécurité est l'obligation de notification. Cette dernière repose sur deux prémisses, soit : le droit de l'individu de savoir et la mitigation des dommages[353]. Or, tel que mentionné précédemment, l'exercice des recours des victimes d'une atteinte à la sécurité de leurs renseignements personnels est subordonné à leur connaissance de l'atteinte[354]. Qui plus est, nous avons vu sous le Titre I que l'obligation de sécurité soulève des difficultés quant à son contenu et sa sanction. Ainsi, l'obligation de sécurité et l'obligation de notification se complètent[355] : la première est préventive tandis que la seconde est curative.

Depuis quelques années, l'introduction d'une l'obligation de notification dans les lois encadrant la protection des renseignements personnels suscite l'intérêt dans plusieurs juridictions. Du côté américain, de nombreux états ont adopté des « security breach notification laws » (« SBNL ») obligeant certains types d'entreprises à informer les individus concernés par une atteinte[356]. À l'heure actuelle, quarante-six États américains, le District de Columbia, Puerto Rico et les Iles Vierges ont adopté des SBNL prévoyant une obligation de notification, dans certaines circonstances[357]. Aucune de ces lois n'est d'application générale. Il n'y a pas encore de loi fédérale créant une obligation générale

[353] Sasha ROMANOSKY, Rahul TELANG et Alessandro ACQUISITI, « Do Data Breach Disclosure Laws Reduce Identity theft? », 30 (2) *J. Pol. Anal. Manage.* 256 (2011), en ligne: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268926 (consulté le 21 juillet 2012)
[354] CAI, 2011, préc., note 222
[355] CAI, « Technologies et vie privée à l'heure des choix de société », préc., note 356, p.39
[356] L. RODE, «Database security breach notification statutes : does placing the responsability on the true victim increase data security? », 43 *Hous. L. Rev.*, 1597, 1612-1633 (2006-2007)
[357] Le champ d'application de ces lois n'est pas uniforme. Nous ne traiterons pas pour les fins du présent texte des différences entre chacune d'elles. Il nous suffit de mentionner que l'obligation de notification fait maintenant partie du paysage législatif américain en matière de protection des renseignements personnels. Voir: NATIONAL CONFERENCE OF STATE LEGISLATURE, *State Security Breach Notification laws*, en ligne: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (consulté le 16 juillet 2012)

et uniforme. Pour l'instant, seulement un canevas législatif sectoriel intègre une obligation de notification en droit américain. Cette situation pourrait bien changer, à plus ou moins long terme, considérant la position récemment adoptée par la Maison Blanche dans le Consumer Privacy Bill of Rights[358]. En effet, ce projet de loi milite en faveur d'une norme de notification nationale.

Du côté européen, la Commission Européenne a déposé, en janvier 2012, une *Proposition de Règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données)*[359] (« Règlement ») visant à remplacer la *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*. Ce Règlement prévoit notamment l'introduction d'une obligation pour les entreprises de notifier l'autorité de contrôle nationale « en cas de violations graves de données à caractère personnel»[360] et de communiquer à la personne concernée la « violation de données à caractère personnel » susceptible « de porter atteinte à la protection des données à caractère personnel ou à la vie privée »[361]. Depuis son dépôt, le Règlement a fait l'objet de trois avis[362] du Groupe de travail « Article 29 » sur la protection des données (« **G29** ») et de propositions d'amendements, notamment dans le rapport de M. Albrecht, rapporteur de la Commission des libertés civiles, de la justice et des affaires

[358] The White House report, préc., note 142
[359] COMMISSION EUROPÉENNE, *Proposition de Règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données*, Bruxelles, le 25.1.2012 COM(2012) 11 final, en ligne : http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf
(consulté le 21 juillet 2012) (ci-après « Règlement »)
[360] *Id.*, art. 31(1)
[361] *Id.*, art. 32(1).
Albrecht
[362] Les trois avis ont été adoptés respectivement le 22 mars 2012, 5 octobre 2012 et le 22 janvier 2013 : WP 191, Opinion 01/2012 on the data protection reform proposals; WP 199, Opinion 01/2012 providing further input on the data protection reform discussions; et WP 200, Working Documents 01/2013, input on the proposed implementing acts, en ligne : http://ec.europa.eu/justice/data-protection/index_en.htm (consultés le 27 août 2013)

intérieures du Parlement européen, publié le 8 janvier 2013 (« Rapport Albrecht »)[363]. Les propositions d'amendements sont présentement en discussion devant le Parlement européen pour une adoption du texte prévue au printemps 2014[364].

Du côté canadien, depuis 2004, la province de l'Ontario a introduit une obligation de notification, dans le contexte de la protection des renseignements médicaux[365]. Des obligations similaires existent dans les provinces du Nouveau-Brunswick[366] et de Terre-Neuve-Labrador[367]. De plus, depuis le 1er mai 2010, la *Personal Information Protection Act* (« PIPA ») albertaine oblige statutairement les entreprises privées à aviser l'Alberta's Information and Privacy Commissioner (« Commissariat albertain ») des données personnelles qui sont perdues, qui font l'objet d'un accès non autorisé ou qui sont divulguées sans autorisation[368]. À notre connaissance, les autres provinces canadiennes n'ont pas encore adopté de dispositions législatives générales obligeant les entreprises privées à divulguer une atteinte aux mesures de sécurité ayant trait aux renseignements personnels.

Au fédéral, dans le cadre de la révision quinquennale de la LPRPDE[369], le projet de loi C-12 (« Projet ») a été déposé pour une première lecture devant le Parlement, le 29 septembre 2011[370]. Soulignons qu'un des éléments saillants dudit Projet est l'introduction d'une obligation pour les entreprises de déclarer au Commissariat « toute atteinte importante aux mesures de sécurité »[371] et de déclarer aux individus toute atteinte

---

[363] Jan Philipp ALBRECHT, Projet de rapport du 17 décembre 2012, 2012/0011 (cod), en ligne : http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387fr.pdf (consulté le 27 août 2013)

[364] CNIL, Projet de règlement européen : agir vite dans un calendrier contraint, 17 juillet 2013, en ligne : http://www.cnil.fr/linstitution/actualite/article/article/projet-de-reglement-europeen-agir-vite-dans-un-calendrier-contraint/ (consulté le 27 août 2013)

[365] *Personal Health Information Protection Act*, S.O. 2004, c.3, Sched. A, art.12(1)

[366] *Personal Health Information Protection and Access Act*, S.N.B. 2010, c. P-7.05, art. 49

[367] *Personal Health Information Protection Act*, S.N.L. 2008 c. P-7.01, art. 15

[368] *Personal Information Protection Act*, S.A. 2003, c. P-6.5, art. 34.1: « (1) 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. [...]»

[369] Pour être plus exacte, six années se sont écoulés depuis la dernière révision de la LPRPDE.

[370] *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, projet de loi, C-12, dépôt et 1ère lecture, 1ère sess., 41e légis., (Can.) (ci-après « Projet »)

[371] *Id.*, art. 10.1 (1)

présentant « un risque réel de préjudice grave » à leur endroit[372]. Récemment, un nouveau projet de loi a été déposé par la députée Chairmaine Bord, du NPD (« Nouveau Projet »)[373]. Ce nouveau projet, jugé « bien meilleur », a été accueilli positivement par les défenseurs de la vie privée[374].

En droit civil québécois, nous serions portés à croire que l'obligation de notification existe déjà, sans qu'il soit nécessaire de la codifier. En effet, la notion de faute de l'article 1457 du Code civil nous semble suffisamment large pour l'englober. Une entreprise prudente et diligente avisera l'individu concerné d'une atteinte à la sécurité de ses renseignements personnels. Cependant, dans un contexte où tant le Commissariat que la CAI semblent en faveur de l'introduction statutaire d'une telle obligation, nous étudierons, pour les fins du présent texte, les éléments constitutifs statuaires nécessaires à l'accomplissement des fonctions de l'obligation. À cet égard, nous tiendrons compte des dispositions actuelles de la PIPA, des dispositions proposées par le Règlement[375], et de celles proposées par le Projet et le Nouveau Projet, afin de nous aider à élaborer le modèle qui aurait le plus de chances de succès.

Sous-partie 1 Les fonctions de l'obligation de notification

Nous avons exposé, sous le Titre I du présent texte, que les individus arrivent difficilement à protéger leurs renseignements personnels en raison des difficultés d'exercice du recours. Nous avons également souligné que les entreprises ne subissent pas une pression économique et « réputationnelle » significative les incitant à prendre des mesures de sécurité raisonnables.

---

[372] *Id.*, art. 10.2 (1)

[373] *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques(pouvoirs de rendre des ordonnances)*, projet de loi, C-475, dépôt et 1ère lecture, 1ère sess., 41e légis., (Can.) (ci-après « Nouveau Projet »)

[374] Éloise GRATTON, *Security breach notification soon becoming mandatory in Canada*, Avril 2013, en ligne: http://www.mcmillan.ca/security-breach-notification-soon-becoming-mandatory-in-Canada (consulté le 27 août 2013)

[375] En effet, non seulement l'Europe est-elle à l'avant-garde en matière de protection de renseignements personnels mais ses règles relatives aux transferts internationaux de données oblige à considérer son positionnement en matière de protection des renseignements personnels.

L'obligation de notification se présente comme une solution afin rééquilibrer la responsabilité entre les individus et les entreprises d'adopter des mesures de sécurité raisonnables, par la réunion de quatre fonctions (et objectifs), soit : la mitigation des dommages, l' « accountability », l'adoption de mesures de préventives et le développement des connaissances. Voyons ces fonctions successivement.

(a) La mitigation des dommages

L'objectif premier de l'obligation de notification est de permettre à l'individu dont les renseignements personnels ont été compromis de prendre des mesures afin de mitiger ses dommages et d'éviter la survenance d'un préjudice futur[376]. Cet objectif découle directement du « droit de savoir » ce qu'il advient du traitement de ses renseignements personnels, peu importe l'existence ou non de mesures de sécurité raisonnables[377]. En notifiant à l'individu concerné, l'entreprise s'évite également une condamnation potentielle en dommages puisqu'elle aide l'individu à réduire les chances de réalisation d'un préjudice futur. En effet, nous avons exposé, sous le Titre I, que c'est seulement si le préjudice se réalise que l'entreprise sera tenue de l'indemniser[378]. Le coût de cette indemnisation risque d'être plus élevé que le coût initial de notification. Il est donc moralement et économiquement justifié pour l'entreprise d'aider l'individu à mitiger le préjudice futur pouvant résulter d'une atteinte à ses mesures de sécurité.

L'obligation de notification ne sera efficace que si l'individu est correctement informé, dans les meilleurs délais possibles, de la survenance de l'atteinte. La détermination du délai de notification optimal pose la difficulté de balancer le temps nécessaire à l'identification de l'atteinte, de sa cause et de ses conséquences, et la nécessité de mitiger

[376] L. RODE, préc., note 356,1621
[377] Projet, art. 2(3) : « « atteinte aux mesures de sécurité » Communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation prévues aux articles 4.7 à 4.7.5 de l'annexe 1 ou du fait que ces mesures n'ont pas été mises en place. »
[378] *Supra*, p. 13-23

les conséquences de l'atteinte dans les meilleurs délais[379]. Ces deux considérations sont intimement liées. En effet, il est impossible de se prémunir contre les conséquences d'un risque qui n'est pas identifié. Par ailleurs, si le délai de notification est trop long, l'objectif de mitigation ne sera pas pleinement atteint : plus le délai est long, plus les chances de survenance d'un préjudice sont grandes[380].

À cet égard, mentionnons que la PIPA prévoit que l'entreprise doit notifier l'atteinte au Commissariat albertain « without unreasonnable delay »[381]. Sur demande du Commissariat albertain, l'entreprise doit notifier l'atteinte aux individus concernés. Le Commissariat fixe le délai de notification[382]. Quant au Règlement, il propose que l'entreprise doive notifier à l' « autorité de contrôle » dans un délai de 24 heures suivant la découverte de l'atteinte[383]. Le Rapport Albrecht suggère 72 heures[384]. Quant à la communication à la personne concernée, le Règlement propose que cette communication soit faite « sans retard indu »[385]. Enfin, le Projet prévoit que l'entreprise doit informer « le plus tôt possible » le commissaire après avoir constaté qu'il y a eu une « atteinte importante ».[386] Par la suite, l'entreprise doit informer l'individu concerné « le plus tôt possible » après avoir déterminé que l'atteinte présente un « risque réel de préjudice grave »[387]. Le Nouveau Projet prévoit que l'entreprise doit aviser le commissaire de tout incident « sans retard injustifié » après avoir constaté la perte ou la communication de

---

[379] John LAWFORD et Janet LO, *Data Breaches : worth noticing?*, Public Interest Advocacy Center (2012), p. 54-59, en ligne: disponible à l'adresse: www.piac.ca/files/data_breaches_worth_noticing_publication_version_final_final.pdf (consulté le 11 juillet 2012) (ci-après « **PIAC** »)

[380] SCHWARTZ et JANGER, préc., note 115, 19

[381] PIPA, art. 34.1

[382] *Id.*, art. 37.1 (b)

[383] Règlement, art. 31(1) : « En cas de violation de données à caractère personnel, le responsable du traitement en adresse notification à l'autorité de contrôle sans retard injustifié et, si possible, 24 heures au plus tard après en avoir pris connaissance. Lorsqu'elle a lieu après ce délai de 24 heures, la notification comporte une justification à cet égard. »

[384] Rapport Albrecht, préc., note 373, p. 39-40

[385] Règlement, art. 32(1) : « Lorsque la violation de données à caractère personnel est susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée, le responsable du traitement, après avoir procédé à la notification prévue à l'article 31, communique la violation sans retard indu à la personne concernée. »

[386] Projet, art. 10.1 (3) : « La déclaration contient les renseignements prévus par règlement et est faite selon les modalités réglementaires, le plus tôt possible après que l'organisation a constaté qu'il y a eu atteinte importante à ses mesures de sécurité. »

[387] Projet, art.10.2 (5) : « L'avis est donné le plus tôt possible après que l'organisation a confirmé qu'il y a eu atteinte et a conclu qu'elle est tenue de le donner en vertu du paragraphe (1). »

renseignements personnels ou l'accès non autorisés à ceux-ci[388]. Par contre, rien ne l'empêche d'aviser directement la personne concernée[389]. À l'instar de la PIPA et du Règlement, ni le Projet ni le Nouveau Projet ne proposent la notification à l'individu concerné dans un délai fixe. Nous retenons cependant qu'il existe un consensus pour que la notification à l'individu soit donnée avec diligence.

Or, selon nous, la notification ne sera donnée avec diligence que si les circonstances y donnant ouverture sont évaluées de façon objective par la personne appropriée. Par exemple, le Projet prévoit deux notifications, soit une au commissaire et une à l'individu. Dans un premier temps, l'entreprise doit notifier au commissaire les cas d' « atteintes importantes »[390]. Il revient à l'entreprise de qualifier l'atteinte selon les critères prévus à l'article 10.1(2), soit : (a) la sensibilité des renseignements personnels; (b) le nombre d'individus touchés par l'atteinte; et (c) l'évaluation par l'organisation que l'atteinte représente un problème d'ordre systémique[391]. Or, nous soumettons que, pour être efficace, la nécessité de notifier une atteinte au commissaire doit être basée sur une évaluation simple et objective et non sur une évaluation subjective de l'importance de l'atteinte. En effet, la simple lecture des éléments de l'article 10.1 (2) soulève des questions. Comment l'entreprise évaluera-t-elle la sensibilité de renseignements qui ne la concernent pas? L'entreprise est mal placée pour évaluer ce que constitue un renseignement personnel sensible[392]. Qu'est-ce qu'un problème « d'ordre systémique »? L'entreprise aura tendance à adopter la position que l'atteinte résulte d'un problème isolé et non «systémique »[393]. De leur côté, le commissaire et l'individu concerné pourraient bien avoir une tendance opposée[394]. Il n'y aura cependant pas moyen de vérifier si l'atteinte est systémique puisque l'information ne sera qu'entre les mains de

[388]Nouveau Projet, art. 10.01 (4) : « L'avis est donné sans retard injustifié après la découverte de la perte ou de la communication des renseignements personnels ou de l'accès non autorisé à ceux-ci. »
[389] Nouveau Projet, art. 10.02 (3) : (3) Rien n'empêche l'organisation d'aviser, de sa propre initiative, la personne concernée par la perte ou la communication de renseignements personnels ou l'accès non autorisé à ceux-ci; le cas échéant, elle en informe sans délai le commissaire.
[390] Projet, art. 10.1 (1)
[391] Projet, art. 10.1(2)
[392] PIAC, préc., note 379, 32-35. Par exemple, dans la décision Randall, préc., note 64, la Cour Fédérale a jugé que les renseignements portant sur l'utilisation du demandeur du centre de culture physique de son employeur constituaient des renseignements personnels sensibles.
[393] *Id.*
[394] *Id.*

l'entreprise[395]. Par ailleurs, reconnaître le caractère « systémique » de l'atteinte représente quasiment l'admission d'une faute, ce que peu d'entreprises seront prêtes à concéder[396]. L'évaluation de ces deux critères ne peut donc être que subjective et biaisée par l'intérêt personnel de l'entreprise de ne pas notifier[397]. Les éléments prévus à l'article 10.1(2) laissent entièrement discrétion à l'entreprise de notifier l'atteinte au commissaire, ce qui mine l'atteinte des objectifs nécessaires à la mitigation des dommages. Par conséquent, nous soumettons que les éléments énoncés à l'article 10.1(2)(a) et (c) ne devraient pas être considérés ou devraient être considérée de façon « objective » afin que le commissaire soit notifié dès que possible[398]. Dans un deuxième temps, le Projet prévoit une notification à l'individu concerné si l' « atteinte présente un risque réel de préjudice grave »[399]. Encore une fois, il revient à l'entreprise qualifier le préjudice et son risque de réalisation, selon une liste d'éléments[400]. Or, nous soumettons que, pour être efficace, l'obligation de notification à l'individu concernée doit être basée sur une évaluation adéquate de ces différents éléments par la personne appropriée. Autrement, outre la question du délai de notification, il pourrait en résulter une absence de notification.

Enfin, dans un contexte où le Projet prévoit une notification préalable au commissaire, il est primordial que les circonstances d'ouverture à considérer soient bien articulées afin que l'individu puisse être, d'une part, informé de l'atteinte et, d'autre part, informé avec diligence.

---

[395] *Id.*
[396] *Id.*
[397] *Id.*
[398] Notons que le Nouveau Projet prévoit la notification au commissaire si l'atteinte présente un « risque de préjudice ». L'examen est donc axé sur l'individu concerné et non l'atteinte. Cet examen revient à l'entreprise. Le Nouveau Projet prévoit le critère du degré de sensibilité afin de déterminer s'il y a un risque de préjudice (art. 10.01 (3)(a)). Cependant, ce critère doit être considéré par l'entreprise de façon objective, telle une « personne raisonnable » (art. 10.01 (2)).
[399] Projet, art. 10.2 (1)
[400] Projet, art. 10.2(2) et 10.2(3) : « (2) Pour l'application du paragraphe (1), « préjudice grave » vise notamment la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles. (3) Les éléments servant à établir si une atteinte aux mesures de sécurité présente un risque réel de préjudice grave à l'endroit de l'intéressé sont notamment le degré de sensibilité des renseignements personnels en cause et la probabilité que les renseignements aient été mal utilisés ou soient en train ou sur le point de l'être. »

(b) L'« accountability »

L' « accountability » est un concept anglo-saxon difficile à traduire en français, sans en bâcler le sens. Le principe d' « accountability » pourrait faire à lui seul l'objet d'un ouvrage. Pour les fins du présent texte, nous nous contenterons de nous référer à la terminologie utilisée par le G29, lequel réfère à la notion de « responsabilité » et, selon notre compréhension, de son acceptation :

> « Globalement, on peut toutefois dire qu'il met l'accent sur la manière dont la responsabilité (responsability) est assumée et sur la manière de le vérifier. En anglais, les termes «responsibility» et «accountability» sont comme l'avers et le revers d'une médaille et sont tous deux des éléments essentiels de la bonne gouvernance. On ne peut inspirer une confiance suffisante que s'il est démontré que la responsabilité (responsability) est efficacement assumée dans la pratique.[401]» (soulignements ajoutés)

L' « accountability » est un principe de protection des données reconnu depuis l'adoption des lignes directrices de l'OCDE, en 1980[402]. Par ailleurs, l' « accountability » ou la « responsabilité » est le tout premier principe directeur énoncé dans le Code type de la LPRPDE. Il s'agit du principe des principes, celui qui enchâsse et duquel découlent tous les autres principes en matière de protection des renseignements personnels.

Il implique pour les organisations de s'engager à adopter des mesures de protection des renseignements personnels, de les mettre en œuvre et d'accepter, ultimement, la responsabilité de leur protection[403]. Il implique également pour l'entreprise d'être en mesure « to demonstrate accountability »[404].

---

[401] GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis n° 3/2010 sur le principe de la responsabilité*, adopté le 13 juillet 2010, en ligne: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf (consulté le 21 juillet 2012)
[402] OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, préc., note 4
[403] COMMISSARIAT, *Un programme de gestion de la vie privée, la clé de la responsabilité*, en ligne : http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_f.asp#b (consulté le 17 juillet 2012)
[404] COMMISSARIAT, *The case for reforming the Personal Information Protection and Electronic Documents Act*, préc., note 222, p.15

Frank Work, ancien Commissaire à la vie privée de l'Alberta, soulignait, à juste titre : « mandatory notification is essential for accountability on the part of compagnies holding information.[405]» En effet, l'obligation de notification oblige l'entreprise à reconnaître l'existence d'une atteinte et à rendre compte de sa gestion aux individus concernés. Cette reddition de compte s'effectue nécessairement par la notification, en signalant : l'atteinte, la cause de l'atteinte, les renseignements personnels compromis, les mesures prises pour limiter les dommages, les mesures que l'individu doit prendre pour mitiger ses dommages et les ressources disponibles.

L'obligation de notification est donc l'un des éléments constitutifs de l' « accountability » et de son acceptation[406]. Évidemment, cet objectif ne sera atteint que dans la mesure où l'obligation de notification mène véritablement à la notification des atteintes et ne laisse pas entière discrétion aux entreprises de déterminer l'opportunité de les notifier. Tel que mentionné précédemment, quoiqu'il puisse conceptuellement l'être, cet objectif ne semble pas intégré dans les termes du Projet.

(c) **L'adoption de mesures préventives**

L'obligation de notification vise à créer une pression économique et « réputationnelle » sur les entreprises les incitant à adopter des mesures de sécurité raisonnables en premier lieu.

D'un point de vue économique, la vaste opération que doit déployer l'entreprise afin de notifier les individus concernés par une atteinte s'avère onéreuse en termes d'énergie, de temps et d'argent[407]. Cette opération implique, entre autres, d'identifier l'atteinte, la source de l'atteinte, les renseignements personnels compromis et les individus à qui

[405] Jeremy HAINSWORTH, «Get good people and listen to them», *Lawyers weekly*, Vol. 32, No. 6, 8 juin 2012, p.20; C.E. GIDEON, préc., note 3,152
[406] L'obligation de notification s'intègre dans le plan de responsabilité, voir : COMMISSARIAT, préc., note 403
[407] L. RODE, préc., note 356, 1628

notifier[408]. Elle implique également l'élaboration d'un protocole de gestion de l'atteinte, si aucun n'est en place au moment de l'atteinte, et sa mise en œuvre[409]. Elle implique enfin de déterminer le contenu de l'avis, de rédiger l'avis et de le notifier, à tous les individus concernés[410], selon un mode de communication, de préférence directe (soit par téléphone ou par lettre)[411]. Toutes ces étapes représentent des frais pour l'entreprise, sans compter qu'elles doivent être réalisées dans les meilleurs délais possible. Selon une étude récente de la firme de Ponemon : « data breaches in 2010 cost their companies an average of $214 by compromised record»[412]. Ainsi, la logique sous-jacente à l'obligation de notification est la suivante : la perspective de devoir gérer la notification d'une atteinte aura pour effet d'inciter les entreprises à prendre des mesures de sécurité raisonnables en premier lieu[413].

À cet égard, mentionnons que l'efficacité de l'obligation de notification est malheureusement incertaine [414]. D'abord, selon certaines études américaines, la diminution des atteintes à la sécurité informationnelle depuis l'adoption des SBNL est négligeable[415]. Par contre, il faut noter qu'il est encore tôt pour tirer des conclusions quant à l'efficacité de l'obligation. En effet, l'obligation de notification a probablement eu et aura encore pour effet d'augmenter le nombre d'atteintes rapportées. Il faudra surveiller de près si l'obligation de notification incite les entreprises à adopter des mesures de sécurité raisonnables. Ensuite, certains auteurs soutiennent que, malgré les démarches et les coûts engagés par les entreprises afin de notifier les atteintes, les avis

---

[408] Voir, par exemple, les exigences règlementaires de l'avis sous la PIPA : Alta Reg 366/2003, art. 19 et 19.1

[409] *Id.*; COMMISSARIAT, préc., note 403

[410] Selon l'article 10.3 du Projet, l'entreprise doit aussi notifier toute autre organisation, si celle-ci est en mesure de réduire le risque de préjudice. Voir aussi : Alta Reg 366/2003, art. 19

[411] PIAC, préc., note 379, 65-68 ; Alta Reg 366/2003, art. 19 et art. 19.1

[412] THE PONEMON INSTITUTE, *2010 Annual Study: U.S. Cost of a Data Breach*, en ligne: http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach (consulté 16 juillet 2012)

[413] L. RODE, préc., note 356, 1628; S. ROMANOSKY, R. TELANG et A. ACQUISITI, préc., note 353, 9

[414] Jane W. KINN, «Are "Better" security breach notification laws possible?», 24 *Berkeley Technology Law Journal*, (2009), en ligne: http://papers.ssrn.com/sol3/papers.cfm?abstractid=1416222 (consulté le 21 juillet 2012)

[415] IT Channel : le quotidien des marchés verticaux, 4 mars 2011, en ligne : http://www.itchannel.info/articles/116033/3-entreprises-4-ont-ete-piratees-cours-deux-dernieres-annees.htmlhtt< > (site consulté le 6 mars 2011); S. ROMANOSKY, R. TELANG, A. ACQUISITI, *préc.*, note 353; C.E. GIDEON, préc., note 3, 153

trouvent souvent le chemin de la corbeille sans même avoir été ouverts par les individus concernés (« enveloppe triviality »)[416]. Pour ceux qui ouvrent les enveloppes, certains auteurs rapportent que la réaction des individus à la suite d'une notification est « quite relaxed »[417]. À quoi bon engager des frais pour notifier les individus dans ce cas? Si les principaux concernés choisissent d'ignorer l'atteinte, l'efficacité de l'obligation de notification sera remise en question :

> « […] such legislative efforts seek to impose unnecessary and burdensome costs, in terms of time and money, on both organizations, as well as clients who may make no necessary steps to protect themselves notwithstanding such notification.[418]»

Enfin, l'obligation de notification fait supporter à toutes les entreprises un risque économique et « réputationnel », sans égard aux bonnes pratiques déjà adoptées par certaines d'entre elles. Nous pouvons estimer que les entreprises qui ont déjà de bonnes pratiques seront désavantagées comparativement à celles qui n'en ont pas[419]. En effet, en ayant déjà des mesures de sécurité en place, il est plus probable qu'improbable qu'une entreprise puisse détecter une atteinte à ses mesures de sécurité que celle qui n'en a pas. Le risque serait plus élevé pour ces entreprises que les entreprises récalcitrantes. L'efficacité de l'obligation de notification relativement à ces dernières ne serait donc pas optimale. Considérant ce qui précède, il est important que les modalités de l'obligation tiennent bien compte de ces inconvénients.

Quant au risque « réputationnel », la mauvaise publicité entourant la notification d'une atteinte vise à inciter les entreprises à adopter des mesures de sécurité raisonnables en premier lieu. *A priori*, la notification envoie le message, à tort ou à raison, qu'une entreprise donnée n'a pas su protéger adéquatement les renseignements personnels qui lui ont été confiés. Le risque « réputationnel » tient au fait que l'individu concerné pourrait

[416] SCHWARTZ et JANGER, préc., note 115, 952 ; J.W. KINN, préc., note 415, p. 19; L. RODE, préc., note 356, 1626
[417] L. RODE, préc., note 356, 1626
[418] C.E. GIDEON, préc., note 3, 152
[419] J.W. KINN, préc., note 414, 17;

décider de mettre fin à sa relation d'affaires avec l'entreprise afin de la punir de son « mauvais comportement »[420]. L'intensité du risque « réputationnel » dépendra de la qualité de la gestion de l'atteinte par l'entreprise et de la nature de l'atteinte[421]. En effet, si l'entreprise est pro-active et qu'elle envoie un avis informant ses clients de la nature de l'atteinte, de la cause de l'atteinte, des mesures déjà mises en place par elle pour mitiger les risques de préjudice, il est probable que le dommage « réputationnel » soit minime[422]. Par contre, si, malgré son obligation légale, l'entreprise ne divulgue pas l'atteinte (pour autant que l'atteinte soit découverte par les individus concernés) ou si les modalités de notification ne sont pas raisonnables, elle fera probablement face à un dommage « réputationnel » plus important[423]. Il en sera de même si la nature des renseignements compromis est très sensible[424]. Ainsi, la logique sous-jacente à l'obligation de notification est de favoriser l'adoption de mesures de sécurité raisonnables afin d'éviter ou de réduire le risque « réputationnel » créé par la notification.

À cet égard également, mentionnons que l'efficacité de l'obligation de notification est malheureusement incertaine. La réputation n'a pas une importance uniforme pour toutes les entreprises[425]. L'entreprise qui ne fait déjà pas preuve d'une éthique d'affaires élevée sera insensible au risque « réputationnel » créé par l'obligation de notification. Il est aussi possible que le risque associé à la perte de clientèle, en cas de notification, soit si grand qu'une entreprise préfèrera ne pas divulguer l'atteinte. Certains auteurs soutiennent que la mauvaise publicité associée à la notification encourage les entreprises à taire tout incident malencontreux, empêchant ainsi les victimes de mitiger leurs dommages[426]. De plus, considérant que les renseignements personnels sont éparpillés parmi plusieurs entreprises, une entreprise peut décider de ne pas divulguer une atteinte dans son système. En effet, nous avons mentionné, sous le Titre I, qu'il sera presque impossible pour l'individu concerné de prouver que son préjudice résulte de l'atteinte aux mesures de sécurité de cette entreprise donnée. Par ailleurs, nous avons également mentionné sous le Titre I que

[420] L. RODE, préc., note 356, 1621; CAI, Rapport Quinquennal 2011, préc, note 222, p. 38
[421] PIAC, préc., note 379, 61-62
[422] *Id.*; L. RODE, préc., note 356, 1629
[423] PIAC, préc., note 379, 61-62
[424] *Id.*
[425] SCHWARTZ et JANGER, préc., note 115, 930-931
[426] *Id.*

la probabilité que l'individu décide de cesser sa relation d'affaires n'est pas très élevée[427]. Enfin, soulignons que de nombreuses entreprises traitent des renseignements personnels sans avoir une relation étroite avec les individus concernés. Dans ces cas, l'obligation de notifier ne crée pas le même risque « réputationnel » pour ces entreprises que pour celles qui traitent directement avec les individus[428]. Ces considérations nous font donc douter de l'efficacité de l'obligation de notification eut égard au risque « réputationnel ».

Enfin, à l'heure actuelle, soulignons que l'adoption de mesures de sécurité raisonnables par la création d'un risque économique et « réputationnel » ne semble pas être un objectif sous-jacent important au Projet de loi C-12. En effet, tel que déjà mentionné, la notification, tant au Commissariat qu'aux individus concernés, relève de l'entière discrétion de l'entreprise selon son évaluation subjective des éléments applicables. Il est donc primordial que les circonstances donnant ouverture à l'obligation de notification créent un risque suffisant pour les entreprises, mais sans être contre-productives.

(d) Le développement des connaissances

Nous avons mentionné, sous le Titre I du présent texte, qu'une des difficultés soulevées par le régime de responsabilité civile actuel est l'incertitude générée par l'intensité de l'obligation de sécurité informationnelle. Cette difficulté tient, entre autres, au manque de données empiriques en matière d'atteintes à la sécurité informationnelle. Ce manque de données fait en sorte que la survenance d'un événement dommageable est difficilement prévisible pour une entreprise donnée. Au final, le résultat du calcul de la prévention n'est pas fiable[429].

Une des fonctions de l'obligation de notification est de permettre la collecte de données sur les atteintes aux mesures de sécurité ayant trait aux renseignements personnels. Cette collecte permettrait aux entreprises de différents secteurs d'étudier les risques d'atteintes, les impacts de ces atteintes et l'efficacité des mesures préventives. Ainsi, la collecte de

[427] *Supra*, p. 59-61
[428] SCHWARTZ et JANGER, préc., note 115, 931
[429] *Supra*, p. 41-43

données permettrait d'améliorer l'état des connaissances en matière de sécurité des renseignements personnels afin de mieux cibler les menaces et les mesures de sécurité raisonnables à adopter.

La collecte de données serait aussi profitable aux organismes ayant pour mission de protéger les renseignements personnels[430]. En effet, la collecte de données leur permettrait de mieux accompagner et conseiller les entreprises dans le choix des mesures à prendre, de répondre adéquatement aux demandes, tant des individus concernés que des entreprises, et de développer des outils en cas d'atteintes à leur attention[431]. Ainsi, l'obligation de notification permettrait à ces organismes de mieux jouer leur rôle.

Cependant, dans la mesure où l'obligation de notification fait partie d'une loi visant la protection des renseignements personnels, les statistiques ainsi créées seront limitées. Elles ne permettront pas d'étudier les atteintes à la sécurité informationnelle au sens large, mais seulement les atteintes à la sécurité des renseignements personnels. Par ailleurs, dans la mesure où le libellé actuel du Projet laisse aux entreprises une grande discrétion quant à l'opportunité de notifier une atteinte, les données collectées ne seront pas nécessairement complètes, ni représentatives, ni concluantes.

***

Quoique l'introduction statutaire de l'obligation de notification ne nous semble pas nécessaire, l'étude de ses fonctions démontre qu'elle pourrait être utile afin d'encadrer efficacement les modalités de l'obligation. En effet, l'atteinte de ses objectifs (ou l'accomplissement de ses fonctions) dépendra de cet équilibre délicat qui doit exister entre les intérêts des individus et ceux des entreprises. Si le contenu, les modalités et l'exercice de l'obligation de notification ne tiennent pas compte de ces intérêts, l'efficacité de l'obligation sera vouée à l'échec.

[430] CAI, Rapport Quinquennal 2011, préc., note 222, p. 41
[431] *Id*.

Sous-partie 2 Les modalités de l'obligation de notification

Afin que l'obligation de notification puisse accomplir pleinement ses fonctions, le modèle de notification doit tenir compte de certaines considérations clés. Nous traiterons, pour les fins du présent texte, (a) du débiteur de l'obligation de notification et (b) de son créancier.

Notons que d'autres considérations sont également importantes afin que les fonctions précitées soient remplies, notamment : la définition d' « atteintes aux mesures de sécurité »[432], les circonstances donnant ouverture à l'obligation de notification[433], le délai de notification[434] et le contenu de l'avis de notification[435]. Sauf pour les commenter lorsque nécessaire, nous n'en traiterons pas spécifiquement.

(a) Le débiteur de l'obligation

De prime abord, l'identification du débiteur de l'obligation de notification semble anodine : c'est l'entreprise qui subit l'atteinte aux mesures de sécurité ayant trait aux renseignements personnels qui doit notifier cette atteinte aux individus concernés[436].

Cependant, tel que mentionné plus tôt, certaines entreprises traitent des renseignements personnels sans avoir une relation directe avec les individus concernés. Parce qu'elle nous semble appropriée pour expliquer notre propos, nous reprendrons la terminologie utilisée dans le Règlement et nous appellerons ces entreprises les entreprises « sous-

[432] Nous sommes en principe d'accord avec la définition proposée par le Projet, art. 2 (3): « Communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation prévues aux articles 4.7 à 4.7.5 de l'annexe 1 ou du fait que ces mesures n'ont pas été mises en place ». Nous aurions seulement ajouté « modification non autorisée » à l'énumération, afin de couvrir les atteintes à l'intégrité.
[433] Voir nos commentaires, *supra*, p. 107-110.
[434] *Id*.
[435] Pour une étude détaillée, voir: PIAC, préc., note 379, 47-59
[436] *Contra* : l'idée que la notification soit faite aux individus concernés par l'organisme chargé de la protection des renseignements personnels a également circulé. Voir : CAI, Rapport Quinquennal 2011, préc., note 222, p. 41

traitantes »[437]. L'entreprise sous-traitante s'adonne généralement à traiter des renseignements par le biais d'une entente contractuelle la liant à l'entreprise avec laquelle l'individu a directement contracté. Pour reprendre la terminologie utilisée dans le Règlement, nous appellerons cette dernière l'entreprise « responsable du traitement »[438]. Cette situation n'est pas sans soulever la question de l'identification du débiteur véritable de l'obligation de notification. L'entreprise sous-traitante devrait-elle directement notifier l'atteinte aux individus concernés? Est-ce que seulement l'entreprise responsable du traitement devrait notifier l'atteinte? Est-ce que les deux entreprises devraient notifier l'atteinte aux individus concernés?

Le Projet ne tranche pas cette question. L'article 10.2 prévoit que « l'organisation » est tenue de déclarer toute atteinte aux mesures de sécurité ayant trait à des renseignements dont elle a la « gestion » (« control »). L'article 10.3 du Projet prévoit que l'organisation qui avise l'individu concerné doit aviser toute autre organisation si celle-ci peut être en mesure de réduire le risque de préjudice. La PIPA prévoit également la notification par l'organisation qui détient la gestion des renseignements (« control »)[439]. Le Nouveau Projet aussi[440].

La notion de gestion n'est pas définie dans ces textes. Dans un contexte de libre circulation de l'information, identifier l'organisation qui détient la « gestion » des renseignements personnels peut facilement devenir une question litigieuse afin d'éviter la responsabilité de notifier une atteinte. Par exemple, dans l'affaire Avis Car Inc. (« Avis »), Avis avait rapporté au Commissariat albertain un incident concernant la perte ou l'accès non autorisé de renseignements personnels concernant des clients. En effet, les noms, les numéros de carte bancaire et les dates de location avaient illégalement été interceptés par la compagnie mandatée par Avis pour opérer un de ses centres de location. Cette compagnie utilisait un appareil interceptant les informations transférées entre le

[437] Règlement, art. 4(6): « «sous-traitant»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »
[438] Règlement, art. 4(5): « «responsable du traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités, les conditions et les moyens du traitement de données à caractère personnel; […]»
[439] PIPA, art. 34.1(1)
[440] Nouveau Projet, art. 10.01(2)

lecteur de cartes et l'ordinateur utilisé pour la transaction. Lorsqu'Avis a eu connaissance de la situation, elle a alors entrepris d'aviser tous les détaillants émetteurs des cartes de crédit impliquées, mais elle n'avait pas avisé leurs détenteurs (ses clients). À cet égard, Avis plaidait que les détaillants émetteurs étaient dans une meilleure position afin de notifier l'atteinte aux détenteurs. Au sujet de cet argument, le Commissaire a spécifiquement indiqué :

> « I reject Aviscar's submission that it would be most appropriate for the credit card "retailers", as opposed to Aviscar, to advise the affected individuals of this breach. The incident happened to Aviscar, not the credit card "retailers". PIPA requires the organization having the personal information under its control and which experienced the incident to report the incident and where I determine notification is necessary, to notify the affected individuals. In this case Aviscar is the organization that had the personal information under its control and experienced the incident, not the credit card "retailers". The purpose of notification is to enable individuals to take steps as quickly as possible to avoid or mitigate the possible harm that may arise from the incident. Avis car's suggestion that it should not be the party to have to notify because it does not know if the customer's credit card has been fraudulently used is not relevant. Whether the customer's credit card has been fraudulently used yet is not the point. The point is to inform the customer of the potential it may be used so the customer can take any steps he or she deems necessary to prevent fraudulent use. Avis car must notify the affected individuals and provide them with the details of the incident as required by the Regulation.[441] »
> (soulignements ajoutés)

Cette décision ne règle pas complètement la question du chevauchement de la gestion des renseignements personnels par différentes entreprises. Si l'atteinte avait eu lieu dans le système du fournisseur de lecteur engagé par Avis, aurait-elle dû aviser les personnes concernées? Et le fournisseur de lecteur? Cette décision illustre cependant qu'en l'absence d'indications claires, la notion de « gestion » deviendra une question litigieuse lorsque viendra le temps de déterminer qui doit notifier l'atteinte. Or, la survenance d'un

[441] *Aviscar Inc.*, P2011-ND-001, 6 janvier 2011, Numéro de dossier #P1739, Alberta OIPC, en ligne: http://www.oipc.ab.ca/pages/OIP/BreachNotificationDecision.aspx?id=3480 (consulté le 18 juillet 2012)

litige sur l'identité du débiteur de l'obligation aura tôt fait de faire perdre aux individus concernés le temps précieux nécessaire à la mitigation de leurs dommages.

D'autres juridictions ont décidé d'encadrer spécifiquement la question du chevauchement de la gestion. Dans la majorité des SBNL, l'incertitude quant à l'identité du ou des débiteurs de l'obligation de notification a été encadrée par des dispositions prévoyant le cas de l'organisation qui conserve des renseignements sans en être le « owner » ou le « licensee » [442] . Cette organisation (l'équivalent de l'entreprise sous-traitante) a l'obligation d'aviser l'entreprise responsable du traitement d'une atteinte et de collaborer avec celle-ci dans la gestion de l'atteinte.[443] La notification aux individus concernés se fait, elle, par l'entreprise responsable du traitement[444]. Par ailleurs, tel que mentionné précédemment, le Règlement propose que les « sous-traitants » de l'entreprise « responsable du traitement » aient l'obligation d'alerter cette dernière de toute « violation de données à caractère personnel»[445]. C'est l'entreprise « responsable du traitement » qui doit communiquer à la personne concernée la violation[446].

À l'instar des SBNL et du Règlement, nous soumettons que l'identification du débiteur de l'obligation de notification doit être déterminée ou facilement déterminable à la lecture du libellé de la loi. D'une part, un libellé clair évitera les débats relatifs à l'identité du débiteur de l'obligation. Ainsi, il favorisera la notification rapide de l'atteinte aux individus concernés. D'autre part, du point de vue de l'individu concerné, il semble plus légitime de recevoir la notification de l'entreprise avec laquelle il a contracté et à laquelle il a confié ses renseignements que d'une entreprise sous-traitante dont il ignore peut-être même l'existence. Enfin, l'identification d'un seul débiteur facilitera également, tant pour les entreprises impliquées que pour les individus concernés, la gestion de l'atteinte. Notamment, elle évitera de multiplier inutilement les notifications pour un même incident. En plus d'engendrer des coûts inutiles, cette « sur-notification » entraînerait un désintéressement chez les individus concernés.

[442] PIAC, préc., note 379, p. 64
[443] *Id*.
[444] *Id*.
[445] Règlement, art. 26(2) (f) et 31(2)
[446] Règlement, art. 32(1)

Certes, privilégier la notification par l'entreprise responsable du traitement signifie que celle-ci supportera le risque économique et « réputationnel » d'une atteinte survenue aux mesures de sécurité de l'entreprise sous-traitante. Dans ce contexte, l'obligation de notification n'aurait pas pour effet d'inciter les entreprises sous-traitantes à prendre des mesures de sécurité raisonnables ni de les responsabiliser.

Cependant, nous croyons qu'il est possible de remédier à ces inconvénients. D'une part, les lois du marché auront pour effet d'inciter les entreprises sous-traitantes à adopter des mesures de sécurité raisonnables. En effet, comme l'entreprise responsable du traitement supportera les risques générés par l'entreprise sous-traitante, elle aura le bénéfice de choisir de faire affaire avec l'entreprise sous-traitante qui présentera les meilleures mesures de sécurité. Par ailleurs, le risque économique lié à la notification pourra ultimement être supporté par l'entreprise sous-traitante par l'intermédiaire d'une clause d'indemnisation. D'autre part, les obligations entre les entreprises sous-traitantes et le responsable du traitement pourraient être encadrées, comme c'est le cas dans le Règlement[447]. Par ailleurs, des sanctions devraient être prévues dans le cas où l'entreprise sous-traitante ne notifie pas une atteinte, ne notifie pas une atteinte en temps opportun ou n'offre pas sa collaboration à l'entreprise responsable du traitement alors qu'elle est tenue légalement de le faire. Nous y reviendrons[448].

(b) Le créancier de l'obligation

Le créancier ultime de l'obligation de notification est bien entendu l'individu concerné par l'atteinte. L'entreprise qui constate une atteinte à la sécurité des renseignements le concernant doit l'informer afin qu'il puisse prendre les mesures nécessaires pour mitiger ses dommages. Il s'agit du premier objectif de l'obligation de divulgation.

Mais l'identité du créancier soulève une autre question d'intérêt, celle de la notification au Commissariat (ou son équivalent provincial). Doit-il être notifié? Au préalable?

[447] Règlement, art. 24-29
[448] *Infra*, p. 127 et s.

Nous soumettons que le Commissariat devrait être notifié. D'abord, la notification au Commissariat est conforme à l'objectif visant l'adoption préventive de mesures de sécurité raisonnables. Afin d'éviter d'être sous la loupe du Commissariat, l'entreprise adoptera en premier lieu des mesures de sécurité raisonnables[449]. Un avis au Commissariat est également conforme au principe de l' « accountability », d'autant plus que le Commissariat est chargé de la surveillance et du contrôle de la LPRPDE. Ensuite, la notification au Commissariat permettra de collecter des données sur les atteintes à la sécurité des renseignements personnels et lui permettra de mieux jouer son rôle.

À cet égard, notons que la PIPA prévoit déjà la notification au Commissariat en cas de « risque réel de préjudice grave »[450], c'est-à-dire à la suite d'une évaluation, par l'entreprise, basée sur l'effet de l'atteinte. Le Règlement propose également la notification à l'autorité de contrôle « en cas de violation de données à caractère personnel »[451], c'est-à-dire à la suite d'une évaluation simple de la survenance d'une atteinte. Nous avons vu que le Projet prévoit une notification au commissaire en cas d'atteinte « importante »[452]. Le Nouveau Projet prévoit une notification au commissaire en cas de « risque de préjudice »[453].

Nous soumettons aussi que le Commissariat devrait être notifié en cas d'atteinte aux mesures de sécurité susceptible d'entraîner un préjudice, selon une évaluation objective, sans qualifier l'importance de l'atteinte ou du préjudice. Ainsi, l'obligation de notification ne serait pas discrétionnaire. Un tel avis au Commissariat remédierait au risque de « sous-notification » généré par le libellé actuel de l'article 10.1 du Projet. Il éviterait également de submerger le Commissariat par un excès de notifications pour « toute atteinte ». La notification au Commissariat basée sur la survenance d'une atteinte aux mesures de sécurité susceptible d'entraîner un préjudice favoriserait davantage l'atteinte des objectifs de l'obligation de notification.

---

[449] LPRPDE, art. 11(2) : « Le commissaire peut lui-même prendre l'initiative d'une plainte s'il a des motifs raisonnables de croire qu'une enquête devrait être menée sur une question relative à l'application de la présente partie. » (soulignements ajoutés)
[450] PIPA, art. 34.1(1)
[451] Règlement, art. 31(1) : « En cas de violation de données à caractère personnel, le responsable du traitement en adresse notification à l'autorité de contrôle […] »
[452] Projet, art. 10.1
[453] Nouveau Projet, art. 10.01(2)

Nous soumettons également que la notification au Commissariat devrait être faite au préalable, c'est-à-dire avant que l'entreprise notifie les individus concernés[454]. D'une part, la notification au préalable aurait pour effet de mieux cibler les atteintes qui doivent être notifiées aux individus concernés. D'abord, l'évaluation du « risque réel de préjudice grave » serait faite par le Commissariat, et par non l'entreprise, tel que le prévoit l'article 10.2(1) du projet C-12[455]. En effet, le « risque réel » dépend, notamment, de la « sensibilité des renseignements personnels en cause » et de « la probabilité que les renseignements aient été mal utilisés ou soient en train ou sur le point de l'être »[456]. À la lecture même de ce que constitue un « risque réel de préjudice grave », il est peu probable que l'obligation de notification prévue dans le Projet favorise la notification et, le cas échéant, la notification en temps utile[457]. Encore une fois, l'évaluation du caractère « sensible » de l'information par l'entreprise est très subjective. Il est fort probable que l'entreprise évaluera la « sensibilité » des renseignements selon sa perspective et non celle de l'individu concerné. De plus, l'évaluation de la « probabilité » que les renseignements soient mal utilisés est quasi impossible[458]. Nous avons exposé, sous le Titre I, que la prévisibilité de la survenance d'un événement dommageable est difficile à établir. Le libellé du Projet accorde donc aux entreprises une très grande discrétion afin de déterminer l'opportunité de notifier les individus concernés. Qui plus est, le délai de notification risque d'être inutilement prolongé en raison de la complexité des questions qui doivent être évaluées. Notons que le Nouveau Projet pallie à ces difficultés en

[454] De façon médiane, le Règlement prévoit, aux articles 32(1) et 32(4), la notification préalable à l'autorité de contrôle mais conserve le pouvoir de l'entreprise de procéder directement à la « communication » à la personne concernée. Si elle omet de le faire alors que l'autorité de contrôle est d'avis qu'il devrait y avoir une « communication », cette dernière peut ordonner à l'entreprise de communiquer la violation à la personne concernée.

[455] L'article 37.1(1) de la PIPA prévoit que le Commissariat peut ordonner à l'entreprise de notifier les individus concernés, à la suite de son évaluation du « risque réel de préjudice grave». Cependant, l'article 37.1(7) prévoit que l'entreprise conserve le pouvoir d'évaluer le « risque réel de préjudice grave » et de notifier les individus concernés.

[456] Projet, art. 10.2(2)

[457] Par contre, il faut souligner que la notification de l'atteinte aux individus concernés, basée sur l'importance de l'atteinte plutôt que sur la simple survenance de l'atteinte est préférable afin d'éviter la « sur-notification ». En effet, la « sur-notification » provoque le désintéressement des individus concernés, ce qui mine l'atteinte de l'objectif de mitigation des dommages. À ce sujet, voir : SCHWARTZ et JANGER, préc., note 115

[458] PIAC, préc., note 379, 36-37

prévoyant qu'il revient au commissaire d'évaluer si l'atteinte présente un « risque appréciable de préjudice »[459].

Par ailleurs, les connaissances et l'expérience du Commissariat pourraient être très utiles afin d'évaluer ce que constitue un « risque réel de préjudice grave » ou un « risque appréciable de préjudice »[460]. Ses connaissances et son expérience pourraient même réduire les délais d'évaluation. De plus, le Commissariat, contrairement à l'entreprise, est indépendant. L'évaluation par le Commissariat du « risque réel de préjudice grave » éliminerait les risques « sous-notification » générés par l'article 10.2 (1) du Projet. La notification préalable au Commissariat aurait pour effet de laisser à ce dernier la responsabilité de balancer les intérêts en faveur de la notification et les conséquences économiques et « réputationnel » de la notification, de façon indépendante et impartiale. De plus, la notification préalable aurait aussi pour effet de diminuer les risques de « sur-notification » aux individus concernés. Les entreprises ne seraient pas tentées de systématiquement reporter le fardeau de protection sur les individus en notifiant toute atteinte, même celles qui ne méritent pas de l'être[461]. Cette sur-notification désensibiliserait les individus concernés à la notification d'une atteinte[462]. Conséquemment, elle aurait pour effet de bafouer l'atteinte des objectifs nécessaires à la fonction préventive de l'obligation.

D'autre part, l'intervention préalable du Commissariat dans le mode et le contenu de la notification pourrait favoriser l'accomplissement de l'objectif de mitigation. En effet, le contenu et le mode de notification doivent être adéquats. Afin d'éviter que l'individu concerné ne dispose de l'avis sans l'avoir lu ou sans en avoir compris la teneur, son

[459] Nouveau Projet, art. 10.02(2)
[460] Par exemple, le Commissariat, considérant ses connaissances et son expérience, pourra mieux évaluer si, compte tenu des mesures de protection technologiques en place au sein de l'entreprise et compte tenu de l'avancement des technologies, une information par ailleurs chiffrée pourrait être déchiffrée par une personne non autorisée.
[461] Dana J. LESEMANN, «Once more unto the breach : an analysis of legal, technological, and policy issues involving data breach notification statutes», 4 *Akron Intell. Prop. J.* 222 (2009), en ligne: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1671082, (consulté le 21 juillet 2012): «Companies send out letters to consumers even when there is no evidence of injury, risk of injury, or possibility of injury, but merely when there is evidence that "access to" consumer" PII occurred. As a result, consumer receive so many data breach notification letters that they become numb to the effect. The form letters sent to consumers generally provide them with no information about actual injury or risk, nor do they provide consumers with the ability to judge whether these is any likelihood of injury or risk. »
[462] C.E. GIDEON, préc., note 3, 153

contenu doit être informatif, clair et interpellant. Un contenu de cette qualité représente un défi pour l'entreprise qui notifie directement les individus concernés. La tentation sera grande pour l'entreprise d'atténuer la gravité de l'atteinte, d'en camoufler la cause et d'adopter un ton nonchalant afin de limiter l'impact « réputationnel »[463]. Par ailleurs, il y aurait lieu de privilégier un mode de notification directe (téléphone ou lettre) à un mode de notification indirecte ou « substitute notice » (courriel, avis sur le site web de l'entreprise ou avis dans les médias nationaux).[464] Le mode direct serait préférable pour deux raisons : il permet d'interpeller directement et de façon personnalisée l'individu concerné et il évite l'aggravation de l'atteinte en la publicisant[465]. Par contre, ce mode de communication est plus coûteux que les modes indirects. Encore une fois, l'entreprise pourrait avoir tendance à opter pour l'option la moins coûteuse plutôt que pour celle qui est appropriée.

À l'heure actuelle, le règlement d'application de la PIPA prévoit que l'entreprise doit informer les individus par un avis direct[466]. Par contre, un avis indirect peut être donné si le Commissariat albertain juge que ce n'est pas déraisonnable dans les circonstances[467]. À notre avis, en l'absence d'une notification ordonnée, ce mécanisme a pour inconvénient de créer des délais additionnels. Le Règlement prévoit que la Commission Européenne « peut définir la forme de la communication à la personne concernée prévue au paragraphe 1 et les procédures applicables à cette communication. [468]» Le Projet prévoit que l'avis peut être direct ou indirect, mais ne prévoit pas si un mode doit être privilégié à l'autre, ni dans quelles circonstances[469]. Ces considérations devront être ultérieurement précisées par règlement. Le Nouveau Projet prévoit également que l'avis doit être dans la forme règlementaire ou déterminée par le commissaire[470]. Par exemple, certains modes

[463] SCHWARTZ et JANGER, préc., note 115, 951-953
[464] Par exemple, la SBNL californienne prévoit une notification indirecte si les coûts de la notification excèdent 250 000$ ou si plus de 500 000 notifications doivent être données. Le cas échéant, la notification doit être donnée par courriel, sur le site web de l'entreprise et dans un média majeur national. À cet égard, voir : *California Civil Code*, art. 1798.29(g), 1798.82(g)(2) et *Electronic Signatures in Global and National Commerce Act*, 15 U.S.C. ch. 97 § 7000
[465] C.E. GIDEON, préc., note 3, 161
[466] Règlement, art. 19.1 (1)
[467] Règlement, art. 19.1(2)
[468] Règlement, art. 32(6)
[469] Projet, art. 10.2 (6)
[470] Projet, art. 10.01(5)

pourraient être privilégiés dans le cas d'une atteinte touchant un très grand nombre d'individus afin de les informer, dans les meilleurs délais possibles, mais à des coûts non prohibitifs pour l'entreprise. Nous soumettons que l'intervention au préalable du Commissariat favoriserait l'utilisation du mode de notification le plus approprié, eut égard aux circonstances et à la balance des intérêts en jeux.

En résumé, nous soutenons que le Commissariat est dans une bien meilleure position que l'entreprise pour déterminer les atteintes qui doivent être notifiées aux individus et celles qu'il n'est pas nécessaire de notifier. L'intervention au préalable du Commissariat aurait également l'avantage de favoriser la notification selon un contenu et un mode optimaux. La notification préalable au Commissariat, de toute atteinte aux mesures de sécurité susceptible d'entraîner un préjudice, aurait pour effet de favoriser l'atteinte de l'ensemble des objectifs nécessaires afin d'accomplir la fonction préventive de l'obligation de notification. Évidemment, la notification préalable ne sera efficace que si les délais de notification aux individus concernés n'en souffrent pas. Ce qui implique que le Commissariat doit être investi des ressources nécessaires afin de communiquer son évaluation à l'entreprise dans les meilleurs délais. Autrement, l'objectif de mitigation des dommages en sera bafoué. À cet égard, rappelons que le Commissariat a déjà publié, en 2009, un guide à l'attention des entreprises qui désirent volontairement divulguer les atteintes à la vie privée[471]. Un formulaire de notification en ligne est aussi disponible[472]. Il semble donc que le Commissariat ait déjà la volonté et quelques outils pour jouer ce rôle.

Sous-partie 3 Les sanctions

Les dispositions actuelles de la LPRPDE et de la LPRPSP n'octroient au Commissariat et à la Commission que peu de pouvoirs afin de surveiller et sanctionner l'application de

[471] Commissariat, *La protection de la vie privée au sein de votre entreprise, guide en matière d'atteinte à la vie privée*, en ligne : http://www.priv.gc.ca/resource/pb-avp/pb_hb_f.pdf (consulté le 21 juillet 2012)
[472] Commissariat, Rapport d'atteinte à la vie privée, préc., note 217

leurs lois. Elles ne leur accordent aucun pouvoir de sanction monétaire en cas de contravention. Les dispositions actuelles de la LPRPDE ne prévoient aucune sanction pénale ou sanction administrative pécuniaire si les recommandations du *Code Type* ne sont pas suivies par une entreprise. Les dispositions de la LPRPSP prévoient des sanctions pénales en cas de contravention, mais aucune sanction civile[473]. L'entreprise qui contrevient à l'une des dispositions de la LPRPDE peut faire l'objet d'un recours devant la Cour Fédérale, à l'initiative d'un plaignant ou du Commissariat[474]. Seulement la Cour Fédérale, à l'issue de ce recours, peut ordonner à l'entreprise de « revoir ses pratiques » et la condamner à verser au plaignant des dommages-intérêts[475].

Les dispositions envisagées dans le Projet ne remédient pas à cette situation. Le Nouveau Projet remédie en partie à cette situation. Considérant que le Projet ou le Nouveau Projet risque de servir de modèle au niveau provincial, nous étudierons leurs dispositions pour les fins de notre propos, en faisant les nuances nécessaires.

Les dispositions du Projet ne prévoient aucune disposition octroyant au Commissariat le pouvoir d'ordonner à une entreprise de notifier une atteinte aux individus concernés[476]. Elles ne prévoient aucune sanction si l'entreprise ne se conforme pas à son obligation de notification.

En fait, les dispositions du Projet octroient au Commissariat bien peu de pouvoirs afin de surveiller le non-respect de l'obligation de notification. Certes, elles élargissent les circonstances dans lesquelles le Commissariat peut procéder à l'étude d'une plainte à celles entourant l'omission de notifier[477]. Or, l'efficacité de ce pouvoir est vouée à l'échec : comment un individu, qui ignore l'existence même de l'atteinte, peut-il déposer une plainte au motif que l'entreprise serait en défaut de lui notifier une atteinte? L'exercice de ce pouvoir dépendra d'une information divulguée par un informateur ou de la survenance d'un préjudice subi par un individu concerné. Dans le premier cas, les

[473] LPRPSP, art. 91
[474] LPRPDE, art. 14 et 15
[475] LPRPDE, art. 16
[476] Seule la Cour peut ordonner à l'organisation de revoir ses pratiques et de se conformer à son obligation de notification. Voir : Projet, art. 14,: « ordonner à l'organisation de revoir ses pratiques de façon à se conformer aux articles 5 à 10 et 10.2 et aux paragraphes 10.3(3) et (4)»
[477] Projet, art. 11 (1)

délais de traitement de la plainte risquent de faire perdre à l'individu concerné un temps précieux afin de mitiger ses dommages. Dans le second, le mal est fait. La mitigation des dommages s'en trouve bafouée.

Les dispositions du Projet prévoient également qu'après avoir reçu le rapport du Commissaire un plaignant peut s'adresser à la Cour Fédérale pour qu'elle ordonne à une entreprise de notifier une atteinte aux individus concernés[478]. Pour les raisons énoncées au paragraphe précédent, l'efficacité de cette disposition est futile. À ce stade-ci, nous pouvons seulement envisager l'utilisation de cette disposition dans le cas d'une notification insuffisante ou qui n'a pas été faite en temps utile. À tout événement, les délais de procédures auront tôt fait de bafouer l'objectif premier de l'obligation de notification : la mitigation des dommages.

Enfin, le Projet ne modifie pas le pouvoir du Commissariat de procéder à des vérifications auprès des entreprises afin de s'assurer qu'elles se conforment à leur obligation de notification[479]. Le libellé de l'article 18 LPRPDE n'inclut pas l'obligation de notification, laquelle serait prévue dans la nouvelle section 1.1. de la loi. Est-ce un oubli? Il n'est pas clair non plus que le pouvoir de vérification du Commissariat inclut tant les notifications qui doivent lui être faites que celles qui doivent être faites aux individus. Par ailleurs, les critères permettant l'exercice du pouvoir de vérification se prêtent mal à l'obligation de notification. En effet, c'est seulement si le Commissariat a des « motifs raisonnables » de croire que l'entreprise ne se conforme pas à ses obligations qu'il pourra débuter un processus de vérification. Or, tel que mentionné précédemment, il est difficile d'enquêter sur une atteinte « systémique » dont on ignore l'existence. L'efficacité de cette disposition dépendra d'un informateur ou d'un individu ayant déjà subi une atteinte. Notons que la LPRPSP prévoit que la Commission peut enquêter de sa propre initiative[480].

---

[478] Projet, art. 14(1) (a)

[479] LPRPDE, art. 18(1): « Le commissaire peut, sur préavis suffisant et à toute heure convenable, procéder à la vérification des pratiques de l'organisation en matière de gestion des renseignements personnels s'il a des motifs raisonnables de croire que celle-ci a contrevenu à l'une des dispositions de la section 1 ou n'a pas mis en oeuvre une recommandation énoncée dans l'annexe 1; il a, à cette fin le pouvoir : […] » (soulignements ajoutés)

[480] LPRPSP, art. 81

L'insuffisance de pouvoirs de surveillance et l'absence de sanctions à la LPRPDE et dans le Projet proposé se justifient difficilement. Depuis de nombreuses années, le Commissariat réclame une loi qui lui accorde plus de pouvoirs et qui prévoit des peines dissuasives : « the only way to get some corporations to pay adequate attention to their privacy obligations is by introducing the potential for large fines that would serve as an incentive for compliance.[481]»

À la suite du dépôt du Projet pour sa première lecture, la Commissaire Jennifer Stoddart n'a pas manqué d'en souligner le peu de « mordant » :

> « What is put there, I think, was current about three years ago, but in the meantime the world has move on. I really think, like in most jurisdictions now, we need some sanction for egregious data breaches. We need to have powers that will be respected by these huge multinational corporations that are doing business on line and you need strong voice to be heard by them. [482]» (soulignements ajoutés)

Dans son dernier rapport annuel, en juin 2012, le Commissariat réitérait l'insuffisance des pouvoirs que lui accorde le Projet afin de faire respecter la LPRPDE et l'absence de sanction [483] . Récemment encore, le Commissariat souligne : « the days of soft recommendations with few consequences for non-compliance are no longer effective in a rapidly changing environment where privacy risks are on the rise »[484].

À cet égard, les dispositions du Projet sont insatisfaisantes. Cela est difficilement justifiable, surtout eut égard aux dispositions de la PIPA, lesquelles prévoient déjà que le Commissariat albertain peut ordonner à une entreprise de notifier les individus

---

[481] The Globe and Mail, *Canada's privacy commissioner want hefty fines for data breaches*, préc., note 187
[482] Citée dans Sarah SCHMIDT,« Feds dragging their heels on fixing privacy law: Stoddart », *Postmedia news*, 6 juin 2012, en ligne: http://blog.privacylawyer.ca/2012/06/why-heel-dragging-on-privacy-law.html (consulté le 18 juin 2012)
[483] COMMISSARIAT, *Annual report to Parliament 2011- Report on the Personal Information Protection and Electronic Documents Act*, Juin 2012, p. 31 et 51, en ligne: http://www.priv.gc.ca/information/ar/201112/2011_pipeda_e.pdf (consulté le 22 juillet 2012)
[484] COMMISSARIAT, *The case for reforming the Personal Information Protection and Electronic Documents Act*, préc., note 222, p. 6

concernés[485] et que l'entreprise qui fait défaut de notifier une atteinte au Commissariat ou de se conformer à l'ordonnance du Commissariat est passible d'une amende[486]. Cela est d'autant plus injustifiable dans un contexte où les dispositions actuelles du Projet laissent à la discrétion des entreprises l'opportunité de notifier une atteinte au Commissariat et aux individus concernés.

Il est de connaissance générale que le respect d'une obligation ne sera effectif que si le fait de ne pas s'y conformer entraîne des conséquences. Dans la mesure où il n'y a pas de sanction ou que les sanctions ne sont pas applicables, il n'y a pas de raison de notifier une atteinte aux mesures de sécurité[487]. Ainsi, l'absence de sanction rend impossible l'atteinte des objectifs de l'obligation de notification.

Pourquoi le Projet prévoit une obligation de notification, mais ne prévoit-il pas de sanction en cas de contravention à l'obligation de notification? Selon notre compréhension, l'absence de sanction s'expliquerait par la difficulté de détecter une contravention à l'obligation de notification. En effet, la seule façon de détecter qu'une entreprise n'a pas respecté son obligation de notification provient d'une dénonciation par un informateur ou le dépôt d'une plainte par un individu. La mise en œuvre de la loi repose donc, encore une fois, sur la victime ou un informateur, potentiellement un employé de l'entreprise contrevenante. Or, pour des raisons évidentes, ces deux sources de détection ne sont pas efficaces. En ce qui concerné l'employé, malgré une disposition de la loi interdisant le congédiement en cas de dénonciation[488] et une disposition lui assurant la protection de l'anonymat[489], il est peu probable qu'il se risquera à dénoncer son employeur. En ce qui concerne l'individu qui a déjà subi le préjudice, il est peu probable qu'il déposera une plainte au motif que l'entreprise aurait dû lui notifier

[485] PIPA, art. 37
[486] PIPA, art. 39(1)(e.1), 39(1)(f) et 39(2)
[487] J.W. KINN, préc., note 414, 12 : « […] rational actors are presumed to be deterred by legal prohibitions when the cost of the violation exceeds the benefits they expect to derive from the violation. Because SBNL's do not commit any significant public resources to increase the probability of apprehension and conviction for failure to report breaches, the expected value of apprehension and conviction for many businesses will be equal to zero»
[488] LPRPDE, art. 27.1
[489] LPRPDE, art. 27

l'atteinte[490]. Ainsi, nous expliquons l'absence de mécanisme de sanctions par l'absence de mécanisme de détection[491].

Afin de remédier à cette situation, nous soumettons que le Commissariat doit avoir le pouvoir de procéder à des vérifications aléatoires de sa propre initiative[492]. Ce pouvoir ne doit pas être restreint par l'existence de « motifs raisonnables ». Autrement, toute détection, autre que précitée, sera impossible. Un pouvoir de vérification aléatoire incitera l'ensemble des entreprises à se conformer à l'obligation de notification afin d'éviter de se faire prendre en flagrant délit. C'est seulement dans la mesure où le Commissariat a un véritable pouvoir de surveillance et de contrôle que la création de sanctions sera utile et leur application possible[493]. Au niveau de la LPRPSP, mentionnons que cette situation n'est pas un problème puisque la Commission peut enquêter de sa propre initiative[494].

Maintenant que nous avons établi que l'existence de sanctions est nécessaire, il convient de s'interroger sur les types de sanctions applicables. Différents types de sanctions peuvent être considérés, notamment : les sanctions civiles, les sanctions pénales et les sanctions administratives pécuniaires. Pour les fins du présent texte, nous n'avons pas l'intention de traiter en détail de chacun de ces types de sanctions, sauf pour mentionner ce qui suit.

Quant aux sanctions civiles, nous avons déjà établi, sous le Titre I, que les sanctions civiles compensatoires sont peu efficaces afin de sanctionner l'obligation de sécurité. Par contre, selon nous, l'obligation de notification améliorerait l'efficacité du recours. D'abord, si elle est bien libellée, l'étendue de l'obligation de notification devrait soulever moins d'ambiguïtés que la « raisonnabilité » de l'obligation de sécurité. Ainsi, la preuve

[490] PIAC, préc., note 379, 71
[491] Il est également possible que des considérations politiques et économiques expliquent cette position.
[492] Notons que le Règlement prévoit, à l'article 52(1)(d), le pouvoir de l'autorité de contrôle d'effectuer des enquêtes de sa propre initiative.
[494] J.W. KINN, préc., note 414, 24 : « In order for SBNL's to provide for such a trigger ex ante, the cost of compliance would have to appear to managers to be greater than the cost of enforcement sanctions discounted by the probability of enforcement action. If the managers of most businesses, especially those that are not public companies, believe the probability that unreported breaches will be detected is negligible, then the cost of compliance will always be higher than the cost of sanctions. »
[494] LPRPSP, art. 81 et s.

de la faute serait simplifiée. Quant au lien causal, nous anticipons que la situation pourrait s'améliorer. En effet, l'obligation de notification étant celle de l'entreprise visée par une atteinte et visant précisément à prévenir la réalisation d'un préjudice futur en découlant, nous entrevoyons difficilement comment il pourrait y avoir un partage de responsabilité avec l'auteur de l'atteinte. De même, la multiplicité des causes du préjudice ne serait plus au centre de l'examen de la causalité. La question deviendrait plutôt : était-il plus probable qu'improbable qu'il en résulterait un préjudice pour l'individu concerné? Quant à la causalité adéquate, elle demeure nécessaire à prouver. L'argument « si j'avais su » ajoute une difficulté à la preuve du lien causal. Est-il plus probable qu'improbable que le préjudice ne serait pas survenu si la victime avait su ? Aurait-elle mitigé ses dommages? Ces mesures auraient-elles empêché la survenance du préjudice? Et même en présumant que l'entreprise avait notifié l'atteinte selon les normes, l'individu concerné aurait-il pu prévenir son préjudice? Toutes ces questions sont très hypothétiques. Enfin, quant à la preuve du préjudice, la situation ne serait pas malheureusement pas différente. Tant l'obligation de sécurité que l'obligation de notification visent à compenser et prévenir le même préjudice. En l'absence de réalisation du préjudice, ce dernier aura le même caractère incertain et minime. Afin que le recours civil soit une véritablement une sanction d'intérêt, il y aurait lieu de prévoir des dommages-intérêts punitifs en cas de contravention à l'obligation de notification[495]. À cet égard, notons que le Nouveau Projet prévoit que l'organisation qui omet de se conformer à une ordonnance du commissaire de notifier l'individu concerné peut se voir imposer des dommages-intérêts punitifs par la Cour[496]. Ainsi, les inconvénients liés à la mitigation des dommages seraient compensés par l'effet de la loi alors qu'autrement ils ne seraient pas indemnisables. Les dommages-

[495] Voir, à titre d'exemple : *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, LC 2010, c 23, art. 51(1)(b) (ci-après « Loi canadienne « anti-spam »)

[496] Nouveau Projet, art. 10.02 (2) et art. 16.1(4). Cette disposition sera efficace en admettant que l'entreprise informe le commissaire en premier lieu. Par ailleurs, il n'est cependant pas clair du libellé du Nouveau Projet si cette sanction vaut seulement en cas de poursuite par le commissaire ou si elle vaut également en cas de poursuite par l'individu concerné. En effet, l'article 16.1 traite du droit d'action du commissaire.

intérêts punitifs seraient par ailleurs un incitatif supplémentaire afin que les entreprises se conforment à leur obligation de notification en premier lieu.

Quant aux sanctions pénales, l'amende demeure une sanction classique. Cependant, elle n'est pas nécessairement gage de bons comportements. Certaines entreprises perçoivent l'amende comme une permission d'enfreindre la loi. Afin d'éviter ce type de comportement, le montant de l'amende maximale doit être suffisamment élevé afin que le coût de l'amende, pour une entreprise donnée, soit supérieur aux coûts qu'elle aurait encourus si elle s'était conformée à son obligation[497]. Ainsi seulement, l'amende aura le caractère préventif et dissuasif nécessaire. Le montant de l'amende devra également être déterminé en tenant compte des mesures de sécurité déjà en place au sein de l'entreprise contrevenante afin de ne pas pénaliser plus que nécessaire les entreprises qui ont déjà de bonnes pratiques.

Enfin, mentionnons que l'établissement de sanctions administratives pécuniaires en cas de contravention de l'obligation de notification est d'intérêt. Le recours aux sanctions administratives pécuniaires est généralement plus rapide que le recours aux sanctions pénales ou civiles[498]. Il constitue aussi un bon incitatif à se conformer à la loi et à dissuader la répétition du comportement contrevenant, sans les inconvénients des recours pénaux ou civils[499]. Par ailleurs, vu le rôle central que nous proposons d'accorder au Commissariat ou à la Commission, l'administration directe de sanctions administratives par le Commissariat ou la Commission s'inscrirait dans la continuité de ses pouvoirs et permettrait de financer ses activités. Au niveau fédéral, ce mode de sanction a déjà été choisi en cas de contravention à la Loi canadienne « anti-spam »[500]. L'entrée en vigueur récente de cette loi ne nous permet pas à ce stade-ci d'en juger l'efficacité. Au niveau européen, nous ne pouvons manquer de mentionner que le Règlement propose également des sanctions administratives pécuniaires, notamment une amende « pouvant s'élever à 1 000 000 EUR ou, dans le cas d'une entreprise, à 2% de son chiffre d'affaires annuel mondial » à quiconque :

[497] PIAC, préc., note 379, 74
[498] *Id.*, 73-74
[499] *Id.*
[500] Loi canadienne « anti-spam », art. 20

> « omet de signaler ou de notifier une violation de données à caractère personnel, omet de la notifier en temps utile ou de façon complète à l'autorité de contrôle ou à la personne concernée conformément aux articles 31 [*Notification à l'autorité de contrôle d'une violation de données à caractère personnel*] et 32 [*Communication à la personne concernée d'une violation de données à caractère personnel*] »

Soulignons l'ingéniosité de l'amende : puisque l'adoption de mesures de sécurité est basée sur une évaluation des coûts et des risques, autant calculer l'amende sur la base du chiffre d'affaires! Par ailleurs, par une lecture conjointe de cette disposition et des articles 31(1) et 31(2) du Règlement, nous comprenons que l'amende vise tant l'entreprise « responsable du traitement » que son « sous-traitant » qui aura omis de l'aviser d'une violation. Ce type de sanction offre l'avantage de responsabiliser le sous-traitant, même s'il ne contracte pas directement avec l'individu concerné.

À tout événement, afin que l'obligation de notification soit efficace, elle doit être assortie de sanctions applicables et dissuasives. L'absence de sanction dans le Projet actuel est un non-sens. Dans ce cas, autant ne pas créer d'obligation de notification.

***

Il découle de l'étude précitée que certaines considérations clés doivent être réunies afin que l'obligation de notification puisse accomplir ses fonctions efficacement. Nous retenons les suivantes :

- le cas échéant, l'entreprise « sous-traitante » doit notifier à l'entreprise « responsable du traitement » toute atteinte aux mesures de sécurité ayant trait à la protection des renseignements personnels, dès la connaissance de l'atteinte;

- l'entreprise « responsable du traitement » doit préalablement notifier l'atteinte au Commissariat ou à la Commission, dès la connaissance de « toute atteinte aux mesures de sécurité susceptible d'entraîner un préjudice »;

- le Commissariat ou la Commission, avec la collaboration de l'entreprise « responsable du traitement » et du « sous-traitant », doit procéder à une évaluation de la nécessité de notifier les individus concernés par une atteinte présentant un « risque réel de préjudice grave », dans les meilleurs délais;

- la notification de l'atteinte aux individus concernés par l'entreprise « responsable du traitement » doit se faire dans un délai de 48 heures de l'évaluation du Commissariat ou de la CAI ou le délai déterminé par lui ou elle;

- le Commissariat et la CAI doivent bénéficier d'un pouvoir de vérification à leur initiative; et

- les sanctions doivent être proportionnées, dissuasives et effectives.

Aucune de ces considérations n'est présentement intégrée dans le Projet.

Conclusion de la partie B

Bien que l'obligation de notification soit curative et non préventive, elle contribue à assurer un niveau plus élevé de responsabilité, et, par conséquent, un plus haut degré de sécurité. D'une part, en étant le corollaire de l'obligation de sécurité, l'obligation de notification améliore l'efficacité du régime afin de compenser et prévenir les atteintes à la sécurité. En effet, en cas de violation, l'obligation de notification serait utile à la victime tant lors de la preuve du comportement fautif que de sa gravité (lors de l'attribution des dommages-intérêts punitifs, le cas échéant). Elle faciliterait également la preuve du lien

de causalité en focalisant l'examen sur le lien entre l'absence de notification et la survenance du préjudice. Ainsi, le régime de responsabilité civile pourrait sanctionner plus efficacement l'absence de notification que l'absence de mesures de sécurité, tout en compensant pour le même préjudice et en prévenant les atteintes à la sécurité des renseignements personnels.

D'autre part, l'entreprise sera plus favorable à adopter des mesures de sécurité raisonnables si elle doit aviser les individus concernés d'une atteinte. Par ailleurs, si elle est poursuivie tout en ayant respecté son obligation de notification, l'entreprise sera dans une position juridique plus sympathique en ayant permis à la victime d'éviter la survenance du préjudice. Idéalement, si l'obligation de notification était bien articulée et s'exerçait efficacement, les entreprises investiraient afin d'adopter de meilleures mesures de sécurité. Il en résulterait un haut niveau de sécurité, moins d'atteintes et, éventuellement, moins de notifications. Ainsi, tant les individus que les entreprises trouveraient cet équilibre nécessaire entre la sécurité et la libre circulation des renseignements personnels.

En ce sens, l'obligation de notification favorise un meilleur équilibre entre la responsabilité des entreprises et celle des individus et assure, globalement, un plus haut degré de sécurité.

Conclusion

Dans le contexte où la LPRPDE et la LPRPSP encadrent le traitement des renseignements personnels sans prévoir de sanction monétaire, nous avions entrepris cette étude dans le but d'analyser l'efficacité du régime de responsabilité civile comme sanction à l'obligation de sécurité des renseignements personnels. Initialement, ce régime nous semblait une sanction monétaire (existante) susceptible d'être efficace considérant ses fonctions préventives et dissuasives incidentes. Malheureusement, notre analyse nous a donné tort.

En effet, nous avons abordé sous le Titre I l'étude des trois conditions essentielles de la responsabilité civile, eut égard à l'obligation de sécurité des renseignements personnels. Nous avons d'abord considéré l'exercice du recours du point de vue de l'individu concerné, en analysant le traitement jurisprudentiel réservé aux cas d'atteintes à la sécurité des renseignements personnels. Nous retenons de la revue jurisprudentielle effectuée que la preuve du préjudice et du lien de causalité rencontre un certain nombre de difficultés qui, cumulées, deviennent propres à la sécurité des renseignements personnels, par opposition aux embûches habituelles. Ces difficultés rendent quasi impossible l'exercice avec succès du recours en responsabilité civile dans le but de sanctionner l'inexécution de l'obligation de sécurité.

Nous avons ensuite étudié l'opportunité pour les entreprises de respecter l'obligation de sécurité qui leur incombe. Notre analyse a porté sur l'étendue de l'obligation de sécurité des entreprises et les impacts d'un recours en responsabilité civile déficient sur leurs comportements. Notre étude a révélé que tant l'obligation en elle-même que sa sanction par un recours en responsabilité civile n'avaient pas pour effet d'inciter les entreprises à s'y conformer, c'est-à-dire à adopter des mesures de sécurité raisonnables.

Devant ce constat désolant, il fallait tenter de revaloriser régime de responsabilité civile comme mesure de contrainte. Dans un premier temps, nous avons profité de l'évolution jurisprudentielle récente pour considérer le recours en dommages-intérêts punitifs comme une solution afin de donner un peu plus de « mordant » au régime de responsabilité civile.

Pour ce faire, les fonctions propres au régime ont fait l'objet d'une nouvelle lecture, en considérant l'obligation de sécurité des entreprises. Nous avons constaté que la principale fonction du recours en dommages-intérêts est de prévenir les comportements qui constituent un écart marqué des normes socialement acceptables, ce que le recours en dommages-intérêts compensatoire semble avoir de la difficulté à accomplir en matière de sécurité des renseignements personnels. Forts de cette constatation, nous avons tenté, de manière prospective, d'anticiper l'exercice d'un recours en dommages-intérêts punitifs dans le contexte d'une atteinte à la sécurité des renseignements personnels. Pour ce faire, le cadre législatif actuel dans lequel s'exercerait le recours a été considéré. Lors de cette analyse, nous avons soulevé les faiblesses du recours et certains aménagements ont été suggérés dont l'introduction du recours dans les lois encadrant la protection des renseignements personnels avec un seuil minimal. Quoique le recours en dommages-intérêts punitifs vise précisément à sanctionner la violation de l'obligation ou du droit protégé, il ressort de notre analyse qu'il ne trouvera application que dans un nombre limité de circonstances vu la nécessité actuelle d'une atteinte intentionnelle. Cela devrait éviter de condamner inutilement les entreprises ayant de bonnes pratiques, mais qui sont malchanceuses.

Le recours en dommages-intérêts punitifs, tout comme le recours en dommages-intérêts, ne peut être exercé que si l'individu concerné a connaissance de l'atteinte. Ce qui nous a amenés à considérer l'obligation de notification comme solution, afin d'inciter les entreprises à s'intéresser à leur obligation de sécurité. Pour ce faire, nous avons d'abord étudié les fonctions de l'obligation afin de nous assurer qu'elle visait bien les objectifs recherchés. Or, non seulement l'obligation de notification servirait à prévenir les atteintes à la sécurité des renseignements personnels, mais, éventuellement, elle permettrait aux entreprises de collecter des données sur leurs pratiques et celle de leur industrie de façon à clarifier leur obligation de sécurité. Ainsi, l'obligation de notification permettrait aux entreprises que mieux comprendre et exécuter l'obligation de sécurité qui leur incombe. Par ailleurs, elle bénéficierait aussi aux individus concernés d'une atteinte. Ceux-ci pourraient tenter de mitiger leurs dommages et intenter leurs recours. En quelque sorte, l'obligation de notification sanctionnerait l'inexécution de l'obligation de sécurité. Quoique l'introduction statutaire de l'obligation de notification ne nous semble pas

nécessaire, nous avons entrepris d'étudier les modalités de son introduction en considérant les différentes propositions législatives qui circulent présentement. Nous avons constaté que, pour être efficace, cette obligation doit être articulée soigneusement, en tenant bien compte des intérêts contradictoires en jeu, d'où l'intérêt d'en délimiter les modalités statutairement. Si elle était bien encadrée, elle permettrait non seulement de favoriser l'exercice du recours en responsabilité civile, mais également de favoriser la naissance d'une véritable culture de la « responsabilité ».

La LPRPDE fêtait ses dix ans, il y a déjà deux ans! Il est temps pour le législateur de rétablir l'équilibre entre la libre circulation de l'information et le besoin de protéger cette information. Cet équilibre est délicat. Il existe une relation contradictoire entre la sécurité informationnelle et la libre circulation de l'information. Plus le niveau de sécurité est élevé, moins l'information circule et inversement. Entre la libre circulation dont voudraient bénéficier les entreprises et le niveau de sécurité maximal dont voudraient bénéficier les individus, il se trouve un spectre de tensions où l'une fait contrepoids à l'autre.

Lorsque la LPRPDE a été adoptée, le législateur a opté pour une loi d'autoréglementation, avec un régime de mise en œuvre « light handed »[501]. Or, si la législation en matière de protection des renseignements personnels n'est pas renforcée par des sanctions dissuasives, elle perdra bientôt sa crédibilité. Malheureusement, il semble nécessaire d'assurer sa mise en œuvre à coups de bâtons! Tel qu'exposé dans le présent texte, le recours en responsabilité civile compensatoire nous semble de peu de secours. Or, deux solutions méritent selon nous d'être considérées dans le cadre d'une réforme de la LPRPDE et la LPRPSP, soit: l'introduction d'une disposition octroyant des dommages-intérêts punitifs et l'encadrement statutaire d'une obligation de notification. Il sera opportun que l'analyse de ses deux solutions se fasse en même temps, de façon à assurer un arrimage harmonieux entre leurs modalités et leurs effets, eut égard aux intérêts en jeu. Enfin, il sera nécessaire que le législateur octroie aux organismes chargés

[501] The Canadian Internet Policy and Public Interest Clinic, *Compliance with Canadian Data Protection Laws: are retailers measuring up?,* avril 2006, p. 42, en ligne: https://www.cippic.ca/sites/default/files/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf (consulté le 11 juillet 2012)

de la protection des renseignements personnels les pouvoirs et les ressources nécessaires à la mise en œuvre de leurs lois. Autrement, aucune de ces mesures ne sera efficace.

Dans un contexte où le régime de responsabilité civile s'est révélé jusqu'à maintenant peu efficace, mais que nous avons plus que jamais besoin d'une réforme sous le signe de la responsabilité, il convient de conclure sur cette citation qui résume bien les dilemmes futurs que nous posera la « responsabilité » avec un grand « R »:

> « Si vous en faites une question de conformité, *vous ferez ce qui est exigé*. Si vous considérez qu'il s'agit d'une question de gestion des risques juridiques, *vous ferez ce qui est nécessaire*. Si vous croyez qu'il s'agit d'une question de responsabilité sociale, *vous ferez ce qui est bien*. Si vous voyez cela comme une occasion d'innover, *vous ferez quelque chose de mieux et de plus ingénieux que tous les autres*, en vous distinguant et en jouant le rôle de leaders courageux et créatifs qui respectent la vie privée des consommateurs et qui sont dignes de confiance. »[502]

[502] Patricia KOSSEIM, « Prêcher par l'exemple : se montrer responsable en matière de protection des donnés », allocution prononcée le 17 avril 2012 dans le cadre du Sommet mondial et de la conférence nationale du printemps de l'ACCJE 2012, en ligne : http://www.priv.gc.ca/media/sp-d/2012/sp-d_20120417_pk_f.asp (consulté le 18 juin 2012)

TABLES BIBLIOGRAPHIQUES

Table de la législation

Fédérale

Projets

Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques, projet de loi, C-12, dépôt et 1ère lecture, 1ère sess., 41e légis., (Can.)

Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques (pouvoirs de rendre des ordonnances), projet de loi, C-475, dépôt et 1ère lecture, 1ère sess., 41e légis., (Can.)

Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications, LC 2010, c 23

Codes

Code criminel, L.R.C. (1985), ch. C-46

Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96

Lois

Charte canadienne des droits et libertés, partie I de la *Loi constitutionnelle de 1982*, [annexe B de la *Loi de 1982 sur le Canada*], 1982, c.11 (R.-U.)

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

Provinciale

Code

Code civil du Québec, L. R. Q., c. C-1991

Lois

Charte des droits et libertés de la personne, L.R.Q., c. C-12

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q. c. A-2.1

Loi sur la protection des arbres, L.R.Q., c. P-37

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1

Loi sur le notariat, L.R.Q., c. N-3

Autres provinces

Alberta

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

Alta Reg 366/2003

Nouveau-Brunswick

Personal Health Information Protection and Access Act, S.N.B. 2010, c. P-7.05

Ontario

Personal Health Information Protection Act, S.O. 2004, c.3

Terre-Neuve

Personal Health Information Protection Act, S.N.L. 2008 c. P-7.01

États-Unis

California Civil Code

Electronic Signatures in Global and National Commerce Act, 15 U.S.C. ch. 97

Textes internationaux

COMMISSION EUROPÉENNE, Proposition de *Règlement du parlement européen et du conseil 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 (règlement général sur la protection des données)*, Bruxelles, le 25.1.2012 COM(2012) 11 final, disponible à l'adresse:

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

Table de la jurisprudence

Québécoise

A.c. *B.*, EYB 2009-168118 (C.Q.)

Aldo Group Inc. c. *Chubb Insurance Company of Canada*, 2013 QCCS 2006

Arpin c. *Bernard Gilles Grenier*, 2004 CanLII 11259 (QCCQ)

Assouline c. *Unfasung*, 2013 QCCA 534

Aubry c. *Éditions Vice-Versa Inc.*, [1998] 1 R.C.S. 591

Augustus c. *Gosset*, [1996] 2 R.C.S. 268

Banque Laurentienne du Canada c. *Pinkerton du Québec Ltée*, EYB 1994

Banque Royale du Canada c. *Dionne*, EYB 2012-207119 (C.S.)

Banque Royale du Canada c. S. (M.), EYB 2010-172365 (C.S.)

Béliveau St-Jacques c. *Fédération des employées et employés de services publics inc.,* [1996] 2 R.C.S. 345

Berthiaume c. *Carignan*, 2013 QCCS 1357

Bessaoud c. *Caisse Desjardins du Marigot de Laval*, 2002 CanLII 23640 (C.Q.)

Bou Malhab c. *Diffusion Métromédia CMR inc.*, [2011] 1 R.C.S. 214

Bouvrette c. *Superpages*, 2004 CanLII 42097 (QCCQ)

Brault & Martineau inc. c. *Riendeau*, [2010] R.J.Q. 507 (C.A.)

Caisse populaire Desjardins d'Aylmer c. *Roy*, 2012 QCCQ 287

Cinar Corporation c. *Robinson*, 2013 CSC 73

Chaput c. *Romain*, [1955] R.C.S. 834

Chéry c. *Banque Royale du Canada*, EYB 2012-201866 (C.S.)

Corbin c. *Drouin*, 2011 QCCQ 10552

Commission des droits de la personne et des droits de la jeunesse c. *Courchesne*, 2013

QCTDP 24

Commission des droits de la personne et des droits de la jeunesse c. *Parent*, 2012 QCTDP 12

Compagnie d'assurances Standard Life c. *Tremblay*, 2010 QCCA 933

Couture c. *Equifax Canada*, 2001 CanLII 20213 (QCCQ)

Cyrenne c. *Municipalité de St-Samuel*, EYB 2005-89615 (C.Q.)

Daméus c. *Banque Nationale du Canada*, 2004 CanLII 20573 (QCCQ)

De Montigny c. *Brossard (Succession)*, [2010] 3 R.C.S. 64

Duchamps c. *Chauvin*, EYB 2010-176107 (C.Q.)

Fernandez c. *Takhar Financial et al.*, 2003 CanLII 3252 (QCCQ)

F.L. c. *Astrazeneca Pharmaceuticals LP*, 2010 QCCS 470

Fortier c. *Zellers inc. et Hudson's Bay Company*, EYB 2009-153198 (C.S.)

France Animation, s.a. c. *Robinson*, 2011 QCCA 1361

Gilbert c. Drolet (Solution Extérieur), 2010 QCCQ 9478

Girao c. *Zarek Taylor Grossman Hanrahan LLP*, 2011 CF 1070

Guarantee Company of North America c. *Phil Larochelle Equipement inc*., EYB 2009

Guardian Trust Co. c. *Frappier & Holland Inc.*, J.E. 78- 532 (C.A.)

Hotte c. *Servier*, [2002] R.J.Q. 230 (C.S.)

J.L. c. *S.B.*, J.E. 2000-1194 (C.S.)

Kingsway Transport Ltd. c. *R.K. Investigations Inc.*, [1996] J.Q. no. 1246 (C.S.)

Laberge c. *Caisse populaire Desjardins de Cowansville*, [1999] R.L. 503 (C.Q.)

Lacroix c. *Bilodeau*, REJB 1998-09843 (C.Q.)

Landry c. *Banque Royale du Canada*, 2011 CF 687

Larose c. *Banque Nationale du Canada*, EYB 2010-181891 (C.S.)

Larente c. *9140-9599 Québec inc.*, 2011 QCCS 3430

Lefrançois c. *9127-0587 Québec inc.*, 2013 QCCQ 2638

Les enterprises Piertrem (1989) inc. c. *Pomerleau Les Bateaux inc.*, EYB 2007-120374 (C.A.)

Louis c. *Banque Laurentienne du Canada*, EYB 2007-112380 (C.Q.)

Markakian c. *Marchés Mondiaux CIBC inc.*, EYB 2006-106729 (C.S.)

Mazzona c. *DaimlerChrysler Financial Services Canada Inc.*, EYB 2012-203721 (C.S.)

M'Boutchou c. *Banque de Montréal*, EYB 2008-150981 (C.S.)

M.C. c. Service d'aide à domicile Bélanger inc., 2011 QCCS 4471

Milunovic c. *Transunion Canada inc.*, EYB 2010-182354 (C.S.)

Milunovic c. *Equifax Canada inc.*, EYB 2012-178059 (C.S.)

Mustapha c. *Culligan du Canada Ltd.*, [2008] 2 R.C.S. 114

Place Biermans c. *C.D.*, [2010] QCCS 4170

Place Biermans c. *C.D.*, 2013 QCCA 64.

Quantz c. *ADT Canada Inc.*, REJB 2002-33495 (C.A.)

Québec (Curateur public) c. *Syndicat national des employés de l'Hôpital St-Ferdinand*, [1996] 3 R.C.S. 211

Richard c. *Time inc.*, EYB 2012-202688 (C.S.C.)

Roberge c. *Bolduc*, [1991] 1 R.C.S. 374

Routhier c. *Sous-Ministre du Revenu*, no AZ-50342967 (C.Q.)
R.S. c. *Commission scolaire A*, 2008 QCCQ 13546

Sauvageau c. *Raymond*, 2012 QCCQ 8326

Séguin c. Général Motors Acceptance Corporation du Canada ltée, 2007 QCCQ 14509

Shoghikian c. *Axxium Vision Inc.*, EYB 2010-177339 (C.Q.)

Stacey c. *Sauvé Plymouth Chrysler*, J.E. 2002

Soucy c. *Visa Desjardins*, 2005 CanLII 23556 (QC C.Q.)

St-*Amant* c. *Meubles Morigeau Ltée*, EYB 2006-104823 (C.S.)

St-Arnaud c. *Facebook*, 2011 QCCS 1506

Timing Inc. c. *Idéation Chou inc.*, 2009 QCCQ 6037

Tremblay c. *Labonté Marcoux*, EYB 2011-195952 (C.Q.)

Tremblay c. *Weyman*, 2011 QCCQ 16099

Unfasung c. *Assouline*, EYB 2011-1890517 (C.S.)

Université Laval c. *Association du personnel administratif professionnel de l'Université Laval*, D.T.E. 2011 (T.A.)

Valiquette c. *The Gazette*, EYB 1996-65651 (C.A.)

V.B. c. *M.S.*, 2012 QCCQ 6460

Wallack c. *Services financiers Daimler-Chrysler Canada inc.*, EYB 2011-190650 (C.Q.)

Wellman c. *Ministère de la sécurité du revenu-secrétariat*, REJB 2002-33036 (C.S.)

Canadienne

Aviscar Inc., P2011-ND-001, 6 janvier 2011, Numéro de dossier #P1739, Office of the information and Privacy Commissionner of Alberta

Biron c. *RBC Banque Royale*, 2012 CF 1095

Englander c. *Telus Communications Inc.*, 2004 CAF 387

Landry c. *Banque Royale du Canada*, 2011 CF 687

Nammo v. *Transunion of Canada*, 2010 CF 1284

Randall c. *Nubodys Fitness Center*, 2010 CF 681

Rosen v. *CIBC*, [2002] O.J. NO 1103 (S.C.)

Royal Bank of Canada v. *Devarenne*, [1998] N.B.J. No 376

Stevens v. *SNF Maritime Metal Inc*., 2010 CF 1137

Townsend c. *Financière Sun Life*, 2012 CF 550
Turner c. *Telus Communications Inc*., 2005 CF 1601
Wansink c. *Telus Communications*, [2007] 4 R.C.F. 375

Ward c. *Vancouver (City)*, [2010] 2 R.C.S. 28

Américaine

Bell v. *Acxiom Corp.,* 2006 U.S. Dist. LEXIS 72477 (E.D. Ark. 2006)

Bell v. *Michigan Council 25AFSCME*, 2005 Mich. App lexis 353 (Mich. Ct. App. 2005)

Claridge v. *RockYou* , 2011 WL 1361588 (N.D. Cal. 2011)

Forbes v. Wells Fargo, 420 F. Supp. 2d 1018 (D. Minn. March 16, 2006)

Giordano v. *Wachovia Sec.,* LLC, 2006 U.S. Dist. LEXIS 52266 (D.N.J. 2006)

Guin v. *Brazos Higher Education Service Corp., Inc.*, No. Civ. 05-668, 2006 WL 288483 (D. Minn. 2006)

Hammond v. *The Bank of New York Mello Corp.*, 2010 U.S. Dist. LEXIS 71996

In re Hannaford Bros. Co., 2011 WL 5007175 (C.A.1.(Me.))

Melancon v. *La. Office Student Fin. Assistance*, 567 F. Supp. 2d 873 (E.D. La. 2008)

Randolph v. *ING Life Insurance and Annuity Co.*, No. Civ. 06-1228 (D.D.C. 2007)

Resnick v. *AvMed*., 2011 U.S. Dist. LEXIS 36686 (S.D. Fla. 2011)

Stollenwerk v. *Tri-West Healthcare Alliance*, No. Civ. 03-0185, 2005, WL 2465906 (D. Ariz. 2006)

T.J. Hooper v. *Northern Barge*, 60 F 2d 737 (2nd Cir. C.A. 1932)

Britannique

Rylands v. *Fletcher*, (1868) 3 L.R.E. & I. App. 330

Table de la doctrine

Monographie et ouvrages collectifs

BAUDOUIN J.-L. et P. DESLAURIERS, *La responsabilité civile, Volume I- Principes généraux*, 7e éd., Cowansville, Éditions Yvon Blais, 2007

CRÉPEAU P.-A., *L'intensité de l'obligation juridique ou des obligations de diligence, de résultat et de garantie*, Cowansville, Yvon Blais, 1989

ALLARD*, F.* et *al*., *Dictionnaire de droit privé et lexiques bilingues, « Les obligations »*, Cowansville, Yvon Blais, 2003

DESBIENS, L. et D. POITRAS, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et Loi sur la protection des renseignements personnels dans le secteur privé, texte annotés*, Montréal, SOQUIJ, 1996

DORAY R.et F. CHARETTE, *Accès à l'information : Loi annotée, jurisprudence, analyse et commentaires*, Volume II, Cowansville, Yvon Blais, 2001 (à jour au 1er juillet 2013)

DUPLESSIS Y., et J.HÉTU, *L'accès à l'information et la protection des renseignements personnels, lois indexée, commentée et annotée*, Brossard, CCH, 2001 (à jour au 8 avril 2011)

ELBEKKALI, A., *Gouvernance, audit et sécurité des TI*, Brossard, CCH, 2008

GAUTRAIS, V.et P.TRUDEL, *Circulation des renseignements personnels et web 2.0*, Montréal, Thémis, 2010

GRATTON, É., ***Understanding Personal Information: Managing Privacy Risks*****,** Markham, Ont., LexisNexis, 2013

HOWARD D. et PRINCE K., *Security 2020 : reduce security risks this decade* (2011)

LABBÉ É., *et al.*, *Guide juridique du commerçant électronique* (version préliminaire), Montréal, 2001

MACKAAY, E. et S. ROUSSEAU, *Analyse économique du droit*, 2e éd., Montréal, Éditions Thémis, 2008

MAITRE, G., *La responsabilité civile à l'épreuve de l'analyse économique*, Paris, L.G.D.J., 2005

MURPHY, M. M., « Privacy protection for customer financial information», dans Ryan F. LEWIS et Gary M. HOWARD (*dir*.), *Information Security Laws: An Introduction,* Hauppauge, N.Y*., Nova Science Publishers,* 2012

ROY, P., *Les dommages exemplaires en droit québécois : instrument de revalorisation de la responsabilité civile*, thèse de doctorat, Montréal, Université de Montréal, 1995

SAMSON, M., *Les interactions de la Charte des droits et libertés de la personne avec le Code civil du Québec : une harmonie à concrétiser*, Thèse de doctorat, Faculté de droit, Université Laval, 2012

SCHNEIER, B., *Beyond Fear* (2003)

SCHNEIER, B., *Secrets & Lies : Digital Security in a Networked World* (2000)

VERMEYS, N. W., « Computer "Insecurity" and Viral Attacks: Liability Issues Regarding Unsafe Computer Systems Under Quebec Law », *Lex Electronica*, vol. 9 n°1, Hiver 2004

VERMEYS, N.W., *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010

WHITMAN, M. E. et H. J. MATTORD, *Readings and cases in information security: Law and Ethics* (2011)

Articles de revue et études d'ouvrages collectifs

BEAULAC S., « Les dommages-intérêts punitifs depuis l'affaire Whiten et les leçons à en tirer en droit québécois », (2002) 36 *R.J.T.* 637

CITRON, D. K., « Reservoirs of danger: the evolution of public and private law at the dawn of the information age », (2006) 80 *CAL. L. REV*. 241

Cynthia CHASSIGNEUX, « La confiance, instrument de régulation des environnements électroniques », (2007) 37 *R.D.U.S.* 441

CHANDLER, J. A., «Negligence Liability for Breaches of Data Security», (2008) 23 *BFLR-CAN* 223

DALLAIRE C., « Les dommages-intérêts punitifs et la diffamation : arme de destruction ou tire-pois? », *La diffamation*, Collection Blais, vol. 3, 2009, EYB2009CBL18

GAGNÉ, S., « Les suites de l'affaire Whiten : l'affaire Markakian et les dommages-intérêts punitifs », *Développements récents en litige commercial*, 2007, Volume 277, 137

GIDEON, C.E., « A new approach to Data Security Breaches», (2009) 7 *Can. J.L. & Tech.* 149

GRAMMOND S., « Un nouveau départ pour les dommages punitifs », (2012) 42 *Revue générale de droit* 105

GRATTON É., *Security breach notification soon becoming mandatory in Canada*, Avril

2013, disponible à l'adresse: http://www.mcmillan.ca/security-breach-notification-soon-becoming-mandatory-in-Canada

HAANAPPEL, P. P.C., (1978) 24 *McGill L.J.* 635

HAINSWORTH J., «Get good people and listen to them», *Lawyers weekly*, Vol. 32, No. 6, 8 juin 2012

HOOFNAGLE C., « Internalizing Identity Theft », (2010) 13 *UCLA Journal of Law and Technology* 1

HUTCHINS J. P. et R. C. FRANÇOIS, « A new frontier : litigation over data breaches », (2009) *The pratical litigator*, disponible à l'adresse : http://www.troutmansanders.com/files/upload/hutchins-newfrontier.pdf

LACOURSIÈRE M., « Chronique- L'utilisation frauduleuse des cartes de débit », *Repères*, Août 2008, *Droit civil en ligne* (DCL), EYB2008REP733

LACOURSIÈRE M., « Propositions de réforme pour une protection des titulaires de cartes de débit victimes de transferts de fonds non autorisés », (2009) *54 McGill L.J.* 91

LESEMANN, D. J., «Once more unto the breach : an analysis of legal, technological, and policy issues involving data breach notification statutes», 4 *Akron Intell. Prop. J.* 222 (2009), disponible à l'adresse: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1671082

MASSINGGALE C. S. et A. F. BORTHICK, « Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services », (1990) 12 *W. New Eng. L.Rev.* 167

MORINGIELLO J., « Warranting Data Security », (2010) 5 *Brook J. Corp. Fin.&Com. L.* (2010)

PRATTE P., « Les dommages punitifs : institution autonome et distincte de la responsabilité civile », (1998) 58 *R. du B.*, 287

PRATTE P., « Le rôle des dommages-intérêts punitifs en droit québécois», (1999) 59 *R. du B.* 445

PHILIPS-NOOTENS S., P.LESAGE-JARJOURA et R. P. KOURI, « La responsabilité du médecin pour le matériel et les produits qu'il utilise », dans Suzanna PHILIPS-NOOTENS, *Éléments de responsabilité civile médicale- Le droit dans le quotidien de la médecine*, 3e édition, Yvon Blais, Cowansville, 2007

RODE, L., «Database security breach notification statutes : does placing the responsability on the true victim increase data security? », 43 *Hous. L. Rev.*, 1597

ROMANOSKY, S., R.TELANG et A. ACQUISITI, « Do Data Breach Disclosure Laws Reduce Identity theft? », 30 (2) *J. Pol. Anal. Manage.* 256 (2011)

ROY P., « Différentes manifestations de la peine privée en droit civil québécois », (2004) 38 *R.J.T.* 263

SAMSON M., « L'atteinte illicite à un droit protégé par la Charte québécoise : source d'un préjudice inhérent ? », *Revue des droits et libertés fondamentaux*, 2012, chron. n°20, disponible à l'adresse: http://webu2.upmf-grenoble.fr/rdlf/?p=2703

SCHWARTZ, P.M. et E. J. JANGER, «Notification of date security breaches », 105 *MICH. L. REV.* 913(2007)

SMEDINGHOFF, T. J., « It's all about trust: the expanding scope of security obligations in global privacy and e-transactions law », 16 MICH. ST. J. INT'L L. 2 (2007-2008)

SOLOVE, D., « *Identity Theft, Privacy and the Architecture of Vulnerability* », 54 *HASTINGS L.J.* 1227, 1231 et 1232 (2002-2003)

SOLUM L. B. et CHUNG M., « The layers principle: internet architecture and law », (2003) *University of San Diego School of law*, disponible à l'adresse: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416263

SOO HOO, K. J., « How much is enough? A Risk-Management Approach to Computer Security », (2000) *CISAC* 13, 3, en ligne: http://iis-db.stanford.edu/pubs/11900/soohoo.pdf

VERMEYS, N. W., *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, thèse de doctorat, Montréal, Faculté de droit, Université de Montréal, 2009

WINN, J. K., « Are better Security Notification Laws possible? », (2009) 24 *Berkley Technology Journal* 33

ZHAO G., « *Decisions may show trend in data breach cases* », (2011) *Chicago Daily Law Bulletin*, disponible à l'adresse: http://www.salawus.com/PubsEvents/pubs/Decisions_May_Show_Trend_In_Data_Breach_Cases.pdf

Documents gouvernementaux

CHAIRE DE RECHERCHE DU CANADA EN SÉCURITÉ, IDENTITÉ ET TECHNOLOGIE, *La sécurité précaire des données personnelles en Amérique du Nord, Une analyse des statistiques*

disponibles, 2008, disponible à l'adresse: http://www.cicc.umontreal.ca/recherche/chercheurs_reguliers/benoit_dupont/chaire_note_recherche1.pdf

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Donner aux petites entreprises les moyens de protéger les renseignements personnels de leurs clients contre les menaces en ligne de plus en plus nombreuses et le scepticisme croissant des consommateurs*, octobre 2011, disponible à l'adresse: http://www.priv.gc.ca/media/nr-c/2011/nr-c_111018_f.asp (dernières modifications: 2011-10-18)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *La protection de la vie privée au sein de votre entreprise- Guide en matière d'atteinte à la vie privée*, 2008, disponible à l'adresse: http://www.priv.gc.ca/resource/pb-avp/pb_hb_f.pdf (dernières modifications: 2008-11-05)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Rapport au Parlement relativement aux lois provinciales essentiellement similaires*, juin 2003, disponible à l'adresse: http://www.priv.gc.ca/leg_c/legislation/leg-rp_030611_f.asp (dernières modifications: 2004-04-01)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Rapport d'atteinte à la vie privée*, 2008, disponible à l'adresse: http://www.priv.gc.ca/resource/pb-avp/pb_form_f.pdf (dernières modifications: 2008-11-05)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels, TJX Companies Inc./Winners Merchant International L.P.*, septembre 2007, disponible à l'adresse: http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_f.asp (dernières modifications: 2007-09-25)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Renseignements juridiques associés à la LPRPDE : Loi provinciales essentiellement similaires à la loi fédérale*, 2003, disponible à l'adresse : http://www.priv.gc.ca/leg_c/legislation/ss_index_f.asp (dernières modifications: 2013-03-22)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *The case for reforming the Personal Information Protection and Electronic Documents Act*, mai 2013, disponible à l'adresse: http://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.pdf

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Un programme de gestion de la vie privée, la clé de la responsabilité*, 2012, disponible à l'adresse : http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_f.asp#b (dernières modifications: 2012-04-17)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Annual report to Parliament 2011- Report on the Personal Information Protection and Electronic Documents Act*, juin 2012, disponible à l'adresse: http://www.priv.gc.ca/information/ar/201112/2011_pipeda_e.pdf

COMMISSION D'ACCÈS À L'INFORMATION, *Aide-mémoire à l'attention des organismes et des entreprises : que faire en cas de perte ou de vol des renseignements personnels?*, avril 2009, disponible à l'adresse : http://www.cai.gouv.qc.ca/documents/CAI_FI_vol_rens_pers_org-ent.pdf

COMMISSION D'ACCÈS À L'INFORMATION, « *Technologies et vie privée, à l'heure des choix de société* », Rapport Quinquennal 2011, juin 2011, disponible à l'adresse: http://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf

LAWFORD J. et J. LO, *Data Breaches : worth noticing?*, Public interest Advocacy Center (2012), disponible à l'adresse: www.piac.ca/files/data_breaches_worth_noticing_publication_version_final_final.pdf

MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, Benoît DUPONT, *Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec*, Septembre 2008, disponible à l'adresse: http://www.benoitdupont.net/sites/www.benoitdupont.net/files/vol_identite%20MSP_0.pdf

The Canadian Internet Policy and Public Interest Clinic, *Compliance with Canadian Data Protection Laws: are retailers measuring up?,* (2006), disponible à l'adresse: https://www.cippic.ca/sites/default/files/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf

Documents internationaux

ALBRECHT, J. P., Projet de rapport du 17 décembre 2012, 2012/0011 (cod), disponible en ligne : http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387fr.pdf

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis n° 3/2010 sur le principe de la responsabilité*, adopté le 13 juillet 2010, disponible à l'adresse: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES :

- WP 191, Opinion 01/2012 on the data protection reform proposals;
- WP 199, Opinion 01/2012 providing further input on the data protection reform discussions;
- WP 200, Working Documents 01/2013, input on the proposed implementing acts;

disponible à l'adresse: http://ec.europa.eu/justice/data-protection/index_en.htm

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontaliers des données à

caractère personnel, 23 septembre 1980, disponible à l'adresse: http://www.oecd.org/fr/internet/economiedelinternet/lignesdirectricesdelocdesurlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité, 25 juillet 2002, en disponible à l'adresse :http://www.oecd.org/sti/interneteconomy/15582260.pdf

PCI SECURITY STANDARD COUNCIL, 2006-2013, disponible à l'adresse : https://www.pcisecuritystandards.org/security_standards/

PHOENIX STRATEGIC PERSPECTIVES, *Rapport final, Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée*, (2013), disponible à l'adresse: http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_f.pdf

THE PONEMON INSTITUTE, *2010 Annual Study: U.S. Cost of a Data Breach*, disponible à l'adresse: http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

THE WHITE HOUSE, *Consumer data privacy in a networked world : a framework for protecting privacy and promoting innovation in the global digital economy*, Washington, February 2012, disponible à l'adresse: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

NATIONAL CONFERENCE OF STATE LEGISLATURE, *State Security Breach Notification laws*, disponible à l'adresse: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (dernières modifications 20 août 2012)

Articles de journaux

CBC News, *Canada's privacy laws inadequate for digital age, watchdog says*, 23 mai 2013, disponible à l'adresse: http://www.cbc.ca/news/technology/story/2013/05/23/technology-privacy-jennifer-stoddart.html

CNIL, Projet de règlement européen : agir vite dans un calendrier contraint, 17 juillet 2013, disponible à l'adresse: http://www.cnil.fr/linstitution/actualite/article/article/projet-de-reglement-europeen-agir-vite-dans-un-calendrier-contraint/

Cyberpresse, *Vie privée : des sanctions plus sévères pour les entreprises*, 4 mai 2011, disponible à l'adresse: http://argent.canoe.ca/lca/affaires/canada/archives/2011/05/20110504-174101.html (dernières modifications 21 février 2013)

KITTEN T., *ACH Fraud: Judge denies Patco Motion No jury expected to hear about dispute with Ocean Bank*, 9 août 2011, disponible à l'adresse: http://www.bankinfosecurity.com/ach-fraud-judge-denies-patco-motion-a-3939/op-1

The Globe and Mail, *Canada's privacy Commissionner wants hefty fines for data breaches*, 4 mai 2011, disponible à l'adresse: http://www.theglobeandmail.com/technology/canadas-privacy-commissioner-wants-hefty-fines-for-data-breaches/article578748/ (dernières modifications 24 août 2012)

Sarah SCHMIDT,« Feds dragging their heels on fixing privacy law: Stoddart », *Postmedia news*, 6 juin 2012, disponible à l'adresse: http://blog.privacylawyer.ca/2012/06/why-heel-dragging-on-privacy-law.html

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, DE JESUS R., *Exploring Federal Privacy Breach Notification in Canada*,1er avril 2013, disponible à l'adresse: https://www.privacyassociation.org/publications/2013_04_01_exploring_federal_privacy_breach_notification_in

Conférence

KOSSEIM P., « Prêcher par l'exemple : se montrer responsable en matière de protection des donnés », allocution prononcée le 17 avril 2012 dans le cadre du Sommet mondial et de la conférence nationale du printemps de l'ACCJE 2012, en ligne : http://www.priv.gc.ca/media/sp-d/2012/sp-d_20120417_pk_f.asp (dernières modifications 2012-05-17)

STODDARDT, Jennifer, « *Sécurité et protection de la vie privée : protéger l'information dans un monde transparent* », discours prononcé le 1er juin 2011, en ligne : http://www.priv.gc.ca/media/sp-d/2011/sp-d_20110601_f.asp (dernières modifications 2011-07-25)

Sites Internet

Commissariat à la protection de la vie privée du Canada : http://www.priv.gc.ca
Commission d'accès à l'information : www.cai.gouv.qc.ca

Google : http://www.google.com

Grand dictionnaire terminologique: http://www.granddictionnaire.com