# Papier en prépublication nº 5

*Droit de l'entreprise : Gouvernance comparée et responsabilité sociétale*

Titre

Le risque « cyber », mission centrale du CA… encore plus avec la COVID-19

Auteur.e.s :

Ivan TCHOTOURIAN

Courriel contact :

ivan.tchotouriand.ulaval.ca

Ouvrage :

« Criminalité économique, cybercriminalité et gestion des risques : Mélanges en l'honneur de la Professeure Isabelle Augsburger-Bucheli », Éditions Helbing Lichtenhahn, à paraître.

Date de mise en ligne : 16 juin 2020

Toute reproduction intégrale ou reproduction d'une partie de l'article est soumis à l'autorisation des auteur.e.s

# Le risque « cyber », mission centrale du CA… encore plus avec la COVID-19

Ivan Tchotourian*

Plan du chapitre

1. Mise en contexte : une question de gouvernance
2. Lois en société par actions et sur les banques : un silence
3. Autres législations : l'exemple de la protection de la vie privée
4. Autorités réglementaires : combler un vide
5. CA : des actions-clés
6. Conclusion : l'enjeu des devoirs

* Professeur agrégé, codirecteur du Centre d'études en droit économique (CÉDÉ), Faculté de droit de l'Université Laval; membre régulier de l'Institut EDS et de la Chaire en gouvernance des sociétés, Faculté des sciences de l'administration de l'Université Laval (FSA). L'auteur remercie M. Alexis Langenfeld (titulaire d'une licence de l'Université Rennes 1 et d'une maîtrise en droit des affaires de l'Université Laval, inscrit en cotutelle en droit à l'Université Laval et à l'Université de Perpignan et boursier FRQSC) pour sa collaboration. À moins d'une indication contraire, les sites Internet sont à jour au 31 mai 2020.

*À elles seules, les cybermenaces sont telles que ce n'est qu'une question de temps avant que toutes les entreprises subissent une cyberattaque*[1].

*La cybersécurité est en train de devenir une des grandes priorités des conseils*[2]

## A. Mise en contexte : une question de gouvernance

« Partout sur le globe, et le Canada n'y échappe pas, la cybercriminalité prend de l'ampleur »[3]. Les produits de la cybercriminalité connaissent un essor important dans « un monde virtuel dépourvu de contrôles et de frontières »[4], marqué par « […] une économie mondiale réseautée et intégrée, [où] les données et les renseignements personnels peuvent voyager rapidement et facilement dans le monde entier, y compris dans les pays qui ont de faibles mesures de protection de la vie privée ou aucune, ce qui peut compromettre le respect de la vie privée des Canadiens à l'étranger »[5]. Les dégâts causés par la cybercriminalité dans le monde sont évalués à 580 milliards d'euros en 2014[6], pour atteindre les 3 000 milliards de dollars américains d'ici 2020[7]. Au Canada, les pertes liées au

---

[1] Center for Board Matters d'EY, *Enjeux de la fin d'exercice 2018 dont doivent tenir compte les comités d'audit canadiens*, EY, 2019 à la p 5, en ligne : https://www.ey.com/fr_ca/audit/what-canadian-audit-committees-should-consider-at-year-end>.

[2] Vanessa COITEUX et Stéphane ROUSSEAU, « Cinq sujets d'actualité en 2019 : la cybersécurité », *Stikeman Elliott* (14 février 2019), en ligne : <https://www.stikeman.com/fr-ca/savoir/droit-canadien-valeurs-mobilieres/Cinq-sujets-d-actualite-en-2019-la-cybersecurite>.

[3] Hélène DESCHAMPS-MARQUIS et Joe ABDUL-MASSIH, « Responsabilité des administrateurs et dirigeants d'entreprise en matière de cybersécurité », dans *Développements récents en droit des affaires*, Cowansville, Yvon Blais, 2019 à la p 3 (PDF) (EYB2019DEV2735).

[4] Commissariat à la protection de la vie privée du Canada, « Lignes directrices pour l'obtention d'un consentement valable », (24 mai 2018), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/>.

[5] *Ibid.*

[6] Valéry MARCHIVE, « Le forum économique mondial insiste sur la menace des cyberattaques », *LeMagIt* (18 janvier 2016), en ligne : <https://www.lemagit.fr/actualites/4500271121/Le-Forum-economique-mondial-insiste-sur-la-menace-des-cyberattaques>.

[7] Commissariat à la protection de la vie privée du Canada, *Vie privée et cybersécurité – Mettre l'accent sur la protection de la vie privée dans les activités de cybersécurité*, décembre 2014 à la p 3, en ligne : <https://www.priv.gc.ca/media/1776/cs_201412_f.pdf>.

vol d'identité se chiffreraient à plus de 500 millions de dollars canadiens par année[8]. Les entreprises sont devenues vulnérables aux cyberattaques, à la cybercriminalité[9], au vol de données personnelles, au non-accès aux données, à l'interruption des affaires, à la divulgation ou diffusion de données, à la compromission liée à un tiers, ou aux menaces d'extorsion.

Les spécialistes s'accordent à identifier huit technologies qui ont un impact significatif pour les entreprises[10] :

- L'intelligence artificielle avec son automatisation des processus robotiques, son apprentissage machine, son traitement du langage naturel, son informatique conversationnelle et ses réseaux neuronaux ;
- La réalité virtuelle et la réalité augmentée ;
- Les drones ;
- La chaîne de blocs ;
- L'Internet des objets ;
- L'impression 3D ;
- La robotique ;
- Le *cloud computing*.

Le *Forum économique mondial* offre un panorama de ces technologies plus vastes dans un rapport publié en 2017[11].

Ces technologies émergentes constituent un outil essentiel pour façonner l'avenir des industries et permettre aux entreprises de demeurer concurrentielles. Mais, elles sont – aussi et surtout – un

---

[8] David DESCÔTEAUX et Berin SZOKA, « Protection des données personnelles : l'impact économique de la réglementation d'Internet » (2013) *Les notes économiques* à la p 2.

[9] David S. WALL, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge, Polity, 2007 ; Bernadette H. Schell et Clemens Marin, *Cybercrime: A Reference Handbook*, Santa Barbaram Abc-Clio, 2004.

[10] PwC Governance Insights Center, *How can boards tackle the Essential Eight and other emerging technologies? Emerging technologies are transforming companies. What should your board know about them?*, PWC, juin 2017 à la p 3, en ligne : <https://www.pwc.com/us/en/governance-insights-center/publications/assets/essential-emerging-technologies-corporate-boards.pdf>.

[11] *The Global Risks Report 2017*, 12e éd., Genève, World Economic Forum à la p 43.

risque « significatif »[12] pour elles. Le risque technologique est devenu une question de gouvernance, au-delà de son aspect purement technique[13]. « Alors qu'autrefois, la sécurité des infrastructures informationnelles était une question qui était traitée par l'équipe de technologies de l'information […], aujourd'hui, toute organisation sait qu'il s'agit d'un risque important sur lequel la haute direction [et le CA doivent] exercer une supervision sérieuse »[14]. En ce domaine, les entreprises ont besoin d'une gouvernance renouvelée ou 3.0. Au Canada, la cyberattaque qui a touché la caisse populaire *Desjardins* a fait trembler l'économie et les entreprises québécoises (mais aussi canadiennes). Les chiffres sont éloquents : cette affaire aurait touché environ 4,2 millions de clients et ce sont les informations personnelles des clients qui ont été attaquées[15]. Les données volées, dont les noms et prénoms, dates de naissance, numéros d'assurance sociale, adresses et numéros de téléphone, adresses courriel et les « habitudes transactionnelles » des membres, auraient été transmises illégalement à des tiers qui ont déjà eu l'occasion d'atteindre certains membres par un hameçonnage[16]. Plus récemment, la pandémie mondiale a intensifié ce risque

---

[12] *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*, AMF (février 2020) à la p 5.

[13] Sébastien JACQUIER, « Entre convivialité, productivité ou sécurité, quelle voie choisir pour les PME à l'ère du tout numérique? Du choix cornélien à l'action préventive » dans Ivan TCHOTOURIAN et Jean-Christophe BERNIER, dir, *Gouvernance d'entreprise, conformité et criminalité économique*, Cowansville, Yvon Blais, 2019, 123 à la p 132 ; Hugh GROVE, Mac CLOUSE et Laura GEORG SCHAFFNER, « Digitalization impacts on corporate governance » (2018) 7:4 Journal of Governance and Regulation, 53 ; Davies, *rapport sur la gouvernance 2018*, 2019 à la p 89 et s. ; KPMG Cyber, *cyber security : it's not just about technology*, KPMG, 2014, en ligne : <https://advisory.kpmg.us/articles/2016/cyber-security-not-just-about-technology.html> ; et aussi les travaux signalés sur la page de l'ECGI) : ECGI, « Technology and Corporate Governance», en ligne : <https://ecgi.global/content/technology-and-corporate-governance-0>.

[14] (Nous soulignons) Danielle FERRON, Tommy TREMBLAY et Jean-François DE RICO, « Cybersécurité : c'est aussi une question de gouvernance », *Langlois bulletin-conseil* (14 septembre 2018), en ligne : <https://langlois.ca/cybersecurite-cest-aussi-une-question-de-gouvernance/>.

[15] Tristan PÉLOQUIN et Hugo PILON-LAROSE, « Vol de données chez Desjardins: 4,2 millions de victimes », *LaPresse* (2 novembre 2019), en ligne : <https://www.lapresse.ca/actualites/justice-et-faits-divers/201911/01/01-5248031-vol-de-donnees-chez-desjardins-42-millions-de-victimes.php>.

[16] Jérôme LABBÉ, « Vol massif de données personnelles chez Desjardins », *Radio-canada* (21 juin 2019), en ligne : <https://ici.radio-canada.ca/nouvelle/1193006/caisses-populaires-desjardins-vol-donnees-personnelles> ; Jean-Michel GENOIS GAGNON, « Vol de données chez Desjardins : "l'enfer" d'un hameçonnage », *Le Journal de Québec* (9 juillet 2019), en ligne : <https://www.journaldequebec.com/2019/07/09/lenfer-dunhameconnage> ; La Presse Canadienne, « Vol de

technologique avec le recours massif au télétravail : « The global coronavirus outbreak is adding another layer of cybersecurity risk as companies ask their employees to work remotely. Indeed, the shift to remote work may create of new potential avenues for unauthorized access to company data and information technology systems from hackers and cyber criminals »[17]. La distanciation sociale et le besoin d'isolement ont, en effet, accéléré l'adoption de technologies permettant l'accès à distance, souvent au détriment des normes rigoureuses d'évaluation et d'atténuation du risque inhérent à une telle démarche, et ont accru la dépendance des entreprises aux fournisseurs de services[18]. Parmi les risques nouveaux figurant :

- « Access to confidential company data through unsafe home or public Wi-Fi networks;
- Vulnerable VPNs due to outdated software;
- Ineffective backup and recovery systems;
- Reduced security on personal devices and computers; […]
- Sharing of proprietary information on workplace chat apps.
- In addition, with the COVID-19 outbreak, phishing emails may target employees using coronavirus as a bait to lure them into clicking on links or attachments infected with malware, resulting in theft of usernames and passwords »[19].

Avec la pandémie de Coronavirus, les entreprises et leurs employés sont donc de plus en plus à risque de fraude ou de cyberattaque[20]. En conséquence, le CA doit gérer plus que jamais le risque « cyber ». Comment ? La question est posée… Pour rappel, la gestion des risques est le processus par lequel les organisations commerciales déterminent de manière proactive les types et les niveaux

---

données chez Desjardins : 2,9 millions de membres touchés », *Le Huffington Post* (20 juin 2019), en ligne : <https://quebec.huffingtonpost.ca/entry/vol-donnees-desjardins-fuite-securite_qc_5d0bcc4ae4b0859fc3db79d5>.

[17] Vanessa COITEUX et Stéphane ROUSSEAU, « COVID-19 and Cyber Risk » *Stikeman Elliott* (26 mars 2020), en ligne : <https://www.stikeman.com/en-ca/kh/corporations-commercial-law/COVID19-and-Cyber-Risk>.

[18] Andrew MACDOUGALL, Lawrence E. RITCHIE et John M. VALLEY, « Supervision du conseil d'administration pendant la pandémie de COVID-19 : une liste de contrôle pour les administrateurs », *Osler* (6 avril 2020), en ligne : <https://www.osler.com/fr/ressources/gouvernance/2020/supervision-du-conseil-d-administration-pendant-la-pandemie-de-covid-19-une-liste-de-controle-pour>.

[19] *Supra* note 17.

[20] Jordan DEERING et Daniel A. LESLIE, « Cybersécurité, fraude et responsabilité pendant une pandémie », *Norton Rose Fulbright* (20 mars 2020), en ligne : <https://www.nortonrosefulbright.com/fr-ca/centre-du-savoir/publications/b2e7bd53/cybersecurite-fraude-et-responsabilite-pendant-une-pandemie>.

de risque appropriés pour atteindre leurs objectifs stratégiques[21]. La gouvernance des risques est une composante distincte et essentielle de la gouvernance des entreprises (sociétés commerciales et banques par exemple) d'aujourd'hui. En matière de gouvernance « cyber », cette gestion des risques est confiée au CA[22]. Comment le Canada permet-il au CA de faire face à un tel risque ? Quelles sont les pistes offertes ? À celles et ceux qui sont peu au fait des droits des sociétés et bancaire canadiens et qui espère y trouver une réponse adéquate, ils seront déçus. Pour trouver des lignes directrices précises, il faut sortir du droit « traditionnel ».

## B. Lois en société par actions et sur les banques : un silence

Le droit en matière de sociétés commerciales (provincial[23] ou fédéral[24]) apporte peu de détails sur la mission du CA. Le législateur se contente d'indiquer que le conseil exerce tous les pouvoirs nécessaires pour gérer les activités et les affaires internes de la société ou en surveiller la gestion[25]. Lui est donc reconnue une mission double : la gestion des affaires de la société d'un côté, et la surveillance de la gestion lorsqu'elle est déléguée (par exemple à un dirigeant) d'un autre côté[26].

---

[21] Patrick MIGNAULT, « La gestion du risque d'entreprise » dans Guy LEFEBVRE et Stéphane ROUSSEAU, dir, *Introduction au droit des affaires*, Montréal, Thémis, 2018, 107, à la p 110 et 115 et s ; Geoffrey P. MILLER, *The Law of Governance, Risk Management, and Compliance*, New York, Wolters Kluwer Law & Business, 2014 à la p 553 ; Stephen M. BAINBRIDGE, « *Caremark* and Enterprise Risk Management » (18 mars 2009) UCLA School of Law Document de travail, No. 09-08 à la p 3 (PDF), en ligne : <https://ssrn.com/abstract=1364500>.

[22] Ivan TCHOTOURIAN, Loïc GEELHAND DE MERXEM et Alexis LANGENFELD, « De la conformité légale à la conformité sociétale : Un rôle de plus en plus complexe pour le CA » dans Ivan TCHOTOURIAN et Jean-Christophe BERNIER, dir, *Gouvernance d'entreprise, conformité et criminalité économique : Approche globale et comparative*, Cowansville, Yvon Blais, 2018, 187 à la p 215 et s.

[23] *Loi sur les sociétés par actions*, RLRQ, c. S-31.1 [LSAQ].

[24] *Loi canadienne sur les sociétés par actions*, L.R.C. 1985, c. C-44 [LCSA].

[25] Art 112 LSAQ et art 102 LCSA

[26] Dans le rapport intitule *Where Were the Directors? – Guidelines for Improved Corporate Governance in Canada* (Toronto Stock Exchange Committee on Corporate Governance in Canada, *Where Were the Directors? – Guidelines for Improved Corporate Governance in Canada*, Toronto, TSX, 1994), ce comité avait recommandé que la loi canadienne soit modifiée pour établir clairement que la responsabilité des administrateurs consiste à superviser la gestion de l'activité. Cinq ans plus tard, un rapport canadien intitulé *Five Years to the* Dey recommanda que « [...] director's responsibilities not include any part of day-to-day

Concernant les institutions financières, la législation fédérale réglemente leur gouvernance notamment à travers la *Loi sur les banques*[27]. Définissant la mission du CA, l'article 157(1) de la *Loi sur les banques* est rédigé sur le modèle du droit des sociétés par actions et n'apporte pas plus de précisions si ce n'est de rappeler la double mission du CA[28].

Alors que dans la perspective classique qui est celle du juriste, le CA est vu comme un organe central de la gouvernance d'entreprise (même si la pratique est différente)[29], force est de constater que sa mission est peu détaillée dans les droits sociétaire ou bancaire, encore moins par rapport à l'aspect technologique.

## C. Autres législations : l'exemple de la protection de la vie privée

Des obligations de sécurité sont prévues par les lois fédérales et provinciales sur la protection de la vie privée ou encore, sur la gestion des données[30]. Les sociétés commerciales et les institutions financières doivent composer avec.

---

management » (Institute of Corporate Directors et Toronto Stock Exchange, *Five Years to the* Dey, Toronto, 1999)

[27] *Loi sur les banques*, LC 1991 c 46.

[28] Le BSIF a souhaité aider les institutions financières et les régimes fédéraux en mettant sur pied un plan stratégique 2019-2022 (Canada, Bureau du surintendant des institutions financières, « L'avenir se trace : le BSIF publie son plan stratégique 2019-2022 », Ottawa, Gouvernement du Canada, 25 avril 2019, en ligne : <https://www.osfi-bsif.gc.ca/Fra/osfi-bsif/med/Pages/strpln1922-nr.aspx>. Un des objectifs de ce plan est de mieux préparer les institutions financières aux risques non-financiers, comme les risques liés à la technologie, et accroître leur résilience à l'égard de ces risques (Finance et Investissement, « Risque technologique : le BSIF veut peaufiner ses mécanismes de surveillance », (30 avril 2019), en ligne : <https://www.financeinvestissement.com/nouvelles/actualites/risques-technologiques-le-bsif-veut-peaufiner-ses-mecanismes-desurveillance/>.

[29] Ivan TCHOTOURIAN et Jean-Christophe BERNIER, *Devoir de prudence et de diligence des administrateurs et RSE*, Cowansville, Yvon Blais, 2014 à la p 212 et s, para 151.

[30] Le cadre juridique relatif à la gestion des données comporte plusieurs dispositions législatives, tant aux niveaux provincial que fédéral. Le vol des données personnelles est un sujet auquel de plus en plus de sociétés

À s'en tenir à la protection de la vie privée, des modifications ont été apportées aux lois canadiennes sur la protection des renseignements personnels qui figurent dans le *Règlement sur les atteintes aux mesures de sécurité*[31] et dans la *Loi sur la protection des renseignements personnels et les documents électroniques*[32] (ci-après « LPRPDE »). La LPRPDE s'applique à toute organisation du secteur privé au Canada (société commerciales, banque…) qui recueille, utilise ou communique des renseignements personnels dans le cadre d'une activité commerciale. De façon générale, les modifications apportées à la LPRPDE et au nouveau Règlement établissent un système obligatoire d'avis et de déclaration concernant les atteintes à la sécurité des données. Plus précisément, les atteintes à la sécurité des données doivent faire l'objet d'un suivi à l'interne et, si elles entraînent la perte ou la communication non autorisée de renseignements personnels, l'entreprise devrait en aviser les intéressés et les signaler au commissaire à la protection de la vie privée du Canada. Les nouvelles dispositions exigent aussi que les organisations conservent un registre de toute atteinte aux mesures de sécurité pendant 24 mois après la date à laquelle elles concluent qu'il y a eu atteinte. Cette exigence s'applique que l'atteinte soit susceptible ou non de présenter un risque de préjudice grave pour les individus intéressés. Dans le contexte de la COVID-19, la protection de la vie privée prend une importance particulière[33].

Toutefois, il faut observer qu'au Canada, « […] il n'existe encore aucune obligation imposée par le gouvernement de se doter d'un régime de cybersécurité adéquat »[34].

---

sont confrontées. L'usurpation des données personnelles donne finalement lieu à l'apparition de nouvelles formes de litiges.

[31] Canada, *Règlement sur les atteintes aux mesures de sécurité*, DORS/2018-64.

[32] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5. Son équivalent au Québec est la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ c P-39.1). Les principes généraux dégagés par ces deux lois sont inspirés des lignes directrices de l'Organisation pour la Coopération et le Développement Économique sur les flux transfrontières de données à caractère personnel.

[33] Danielle MILLER OLOFSSON, « COVID-19: n'oubliez pas la protection des données dans votre stratégie de réponse face à la crise », BCF (13 mars 2020), en ligne : <https://www.bcf.ca/fr/intelligence-d-affaires/2020/n-oubliez-pas-la-protection-des-donnees-dans-votre-strategie-de-reponse-face-a-la-covid-19>.

[34] Davies, *supra* note 13 à la p 91.

## D. Autorités réglementaires : combler un vide

À propos des entreprises sous forme de sociétés commerciales (structure majoritaire au Canada), le droit des valeurs mobilières fournit des lignes directrices étoffées. Ainsi, les ACVM ont publié en octobre 2017, l'Avis 33-321 du personnel des ACVM, *Cybersécurité et médias sociaux*[35] qui complète l'Avis 11-332 du personnel des ACVM, *Cybersécurité* publiée en 2016[36]. Ces avis des ACVM soulignent la nécessité d'être conscientes des défis de la cybercriminalité et de prendre les mesures appropriées pour se protéger et protéger leurs clients ou leurs parties intéressées. L'avis le plus récent rappelle aux participants au marché qu'une fois qu'ils ont déterminé que le cyberrisque est important, ils doivent fournir de l'information détaillée et propre à l'entreprise sur les risques et éviter de communiquer de l'information générale et standard. Les ACVM recommandent également que les plans de reprise après une cyberattaque tiennent compte de la façon dont l'entreprise devrait évaluer l'importance d'une cyberattaque pour établir l'information à fournir aux termes de la législation en valeurs mobilières applicable. En outre, les plans devraient préciser à quel moment et de quelle façon cette information doit être communiquée. L'avis de 2017 rappelle enfin aux entreprises d'être vigilantes lors de l'établissement, de la mise en oeuvre et de l'actualisation de leurs mesures de protection et de gestion en matière de cybersécurité.

Au Québec, l'Autorité des marchés financiers (ci-après « AMF ») a pris plusieurs positions sur le risque « cyber ». D'un côté, l'article 3.4. de l'Instruction 58-201[37] est incontournable en précisant, à propos du mandat du CA, que :

> « Le conseil d'administration devrait adopter un mandat écrit dans lequel il reconnaît explicitement sa responsabilité de gérance de l'émetteur, notamment sa responsabilité :
>
> […] b) d'adopter un processus de planification stratégique et d'approuver, au moins une fois par an, un plan stratégique qui prend en compte, notamment, <u>les opportunités et les risques de l'entreprise</u>;
>
> c) <u>de définir les principaux risques de l'activité de l'émetteur et de veiller à la mise en œuvre de systèmes appropriés de gestion de ces risques</u> » (Nous soulignons).

---

[35] *Cybersécurité et médias sociaux*, ACVM Avis 33-321 (19 octobre 2017).

[36] *Cybersécurité*, ACVM Avis 11-332 (27 septembre 2016).

[37] *Instruction générale 58-201 relative à la gouvernance*, AMF, art 3.4.

D'un autre côté, la *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications* de février 2020[38] indique qu'un des objectifs des administrateurs est de s'assurer du bon fonctionnement des techniques de l'information et de la communication. À ce titre, le CA devrait s'assurer que :

- « La haute direction fasse la promotion d'une culture d'entreprise fondée sur un comportement éthique et sécuritaire dans l'exploitation des technologies;
- Échanger à l'égard des TIC avec les parties intéressées (internes et externes) afin d'appuyer par une documentation sa compréhension des besoins et porter un jugement sur la conception actuelle et future de la gouvernance des TIC;
- Les rôles et responsabilités de la fonction TIC et des fonctions de gestion de la sécurité de l'information et de la continuité des activités soient clairement définis dans l'établissement et le maintien de la gouvernance des TIC;
- Les structures, rôles et fonctions de support soient évalués régulièrement afin de permettre le développement et l'amélioration continue de la gouvernance des TIC »[39].

Concernant les banques, le *Bureau du surintendant des institutions financières* (ci-après « BSIF ») est l'autorité qui les réglemente à l'échelle fédérale. À l'heure actuelle, le BSIF n'est pas doté d'un règlement obligeant les institutions financières à prendre des mesures précises en matière de cybersécurité. Toutefois, la ligne directrice B-10 : *Impartition d'activités, de fonctions et de méthodes commerciales* énonce les attentes du BSIF en matière d'impartition des services technologiques et de gestion des risques liés à la cybersécurité[40]. Par ailleurs, la ligne directrice sur la *Gouvernance d'entreprise*[41] reconnaît que la prise de risques fait partie intégrante des activités d'une institution financière. Toute institution financière devrait être en mesure de déceler les

---

[38] *Supra* note 12.

[39] *Supra* note 12 à la p 9.

[40] Canada, Bureau du surintendant des institutions financières, « Impartition d'activités, de fonctions et de méthodes commerciales », Ottawa, Gouvernement du Canada, mars 2009, en ligne : <https://www.osfi-bsif.gc.ca/Fra/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx>.

[41] Canada, Bureau du surintendant des institutions financières, « Gouvernance d'entreprise », Ottawa, Gouvernement du Canada, septembre 2018, en ligne : <https://www.osfi-bsif.gc.ca/Fra/fi-if/rg-ro/gdn-ort/gl-ld/Pages/CG_Guideline.aspx>. Pour un commentaire, voir : Stuart S. CARRUTHERS, « Le BSIF publie la version finale de sa ligne directrice modifiée sur la gouvernance d'entreprise », *Stikeman Elliott* (26 septembre 2018), en ligne : <https://www.stikeman.com/fr-ca/savoir/droit-assurances/Le-BSIF-publie-la-version-finale-de-sa-ligne-directrice-modifie-sur-la-gouvernance-d-entreprise>.

risques importants auxquels elle est exposée, d'en évaluer les répercussions potentielles et de mettre en place des politiques et des contrôles pour les gérer efficacement[42]. Dans ce cadre, les membres du CA devraient promouvoir une culture de risque axée sur l'intégrité et la gestion efficace du risque[43] et mettre sur pied un comité de gestion du risque chargé de superviser la gestion du risque à l'échelle de l'organisation[44]. Le 24 janvier 2019, le BSIF a publié le préavis intitulé *Signalement des incidents liés à la technologie et à la cybersécurité*, qui a pris effet le 31 mars 2019. Ce préavis donne des instructions aux institutions financières quant au signalement rapide au BSIF des incidents liés à la technologie et à la cybersécurité.

## E. CA : des actions-clés[45]

Pour répondre adéquatement et spécifiquement au risque « cyber » et combler un certain déficit de confiance en cette matière, tout CA (d'une société commerciale ou d'une banque) devrait mettre en place plusieurs actions-clés ou mesures parmi lesquelles :

- Intégrer les discussions relatives à la technologie dans le processus de surveillance stratégique : le CA devrait saisir et approuver les plans de la direction visant à suivre les technologies prioritaires et à y donner suite[46]. Avec le télétravail que la COVID-19 a fait exploser, le CA devrait comprendre où les données critiques sont détenues ou comment y avoir accès par le biais de services fournis par des tiers et si elles sont protégées de manière adéquate contre les cyberinfractions ou l'ingérence gouvernementale[47].
- Revoir sa composition et sa manière de fonctionner : le CA devrait se demander si sa composition (expertises, qualifications professionnelles, connaissances, expériences) est

---

[42] Canada, Bureau du surintendant des institutions financières, *Ibid* à la p 8.

[43] *Ibid* à la p 7.

[44] *Ibid* à la p 9.

[45] Certains passages de cette partie sont extraits de l'article suivant : Ivan TCHOTOURIAN, « CA et nouvelles technologies » (16 janvier 2020) *Contact* (blogue), en ligne : <http://www.contact.ulaval.ca/article_blogue/ca-et-nouvelles-technologies/>.

[46] Institut des administrateurs de sociétés – Section du Québec, *Les technologies émergentes : Comprendre les bouleversements à venir. Guide d'introduction pour l'administrateur de sociétés*, avril 2019, à la p 4, en ligne : <https://www.iasquebec.com/fr/les-technologies-emergentes-comprendre-les-bouleversements-a-venir/>.

[47] *Supra* note 18.

adéquate[48] et former ses membres[49]. Le CA ne devrait plus se réunir une ou deux fois par an pour revoir sa stratégie[50]. Le CA devrait aussi mieux utiliser la technologie pour faciliter ses processus de communication et d'information et aider à la tenue de ses réunions.

- S'assurer d'avoir pris certaines mesures : le CA devrait vérifier la préparation d'un plan d'intervention en cas d'incident[51] ; la réalisation régulière d'exercices sur table et simulations de cyberattaques en groupe, avec l'équipe d'intervention et d'autres professionnels de l'organisation ; et ne pas hésiter à faire appel à un conseiller externe en cas de problème[52].
- Adopter ou mener des examens attentifs sur les règlements, les programmes et les politiques reliées aux enjeux de technologie et de télétravail[53] : structure technologique organisationnelle incluant les mesures de protection mises en place ; gestion de l'information (qu'est-ce qui est conservé ? À quel endroit ? Pour combien de temps ? Qui y a accès ?...)…[54].
- Nommer un cadre supérieur pour exécuter la stratégie numérique : le CA devrait avoir un de ses membres qui assume la responsabilité personnelle de la technologie sans pouvoir déléguer son pouvoir (chef des technologies ou de l'information, *Chief Technology Officer* (CTO) ou *Chief Information Officer* (CIO))[55].
- Créer un comité spécialisé dans les technologies : ce comité permettrait de développer une vision globale ; de gérer les enjeux opérationnels liés à la mise en œuvre des stratégies et

---

[48] *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*, AMF (juin 2019) à la p 5.

[49] *Supra* note 20.

[50] Center for Board Matters d'EY, *Insights on how boards approach digitalization*, EY, 2018.

[51] *Supra* note 17.

[52] *Supra* note 3 à la p 20 et s.

[53] *Supra* note 17.

[54] *Supra* note 14.

[55] Il devrait présenter au CA des propositions technologiques et des statuts de la mise en œuvre des stratégies et encadrements liés aux technologies (*Supra* note 48 à la p 13). En dehors du CA, l'AMF requiert aussi de nommer un responsable de la haute direction (chef de la sécurité de l'information) qui devrait surveiller le déploiement de l'encadrement relatif à la sécurité de l'information et à la sécurité physique des infrastructures technologiques de l'institution; et un autre (*Chief Information Security Officer* (CISO)) – la même ou non – qui devrait surveiller l'encadrement approuvé par le CA à l'égard de la collecte, l'emmagasinage et l'utilisation des données.

encadrements approuvés par le CA liés aux mutations technologiques ; de diminuer les risques liés aux technologies ; de générer de nouveaux canaux de croissance ; ou encore d'accompagner l'entreprise dans sa transformation numérique.

- Engager des tiers consultants pour auditer les systèmes de cybersécurité de l'entreprise et pour fournir des recommandations d'amélioration[56].
- Mettre en place des programmes de formation pour les salariés à propos des risques « cyber »[57].
- Superviser la création par la direction d'une culture qui perçoit les questions de technologie comme étant l'affaire de tous.
- Veiller à ce que l'entreprise ait souscrit une assurance adéquate contre les fraudes ou les atteintes à la cybersécurité, notamment dans un contexte de télétravail[58].

## F. Conclusion : l'enjeu des devoirs

Les sociétés commerciales et les banques – et leurs CA – sont susceptibles d'être exposés à une plus grande responsabilité en matière de risque « cyber » pendant la pandémie de COVID-19[59]. Il faut rappeler que le CA a un devoir de loyauté envers l'entreprise et il doit agir avec honnêteté, de bonne foi et au mieux de ses intérêts. En outre, chaque administrateur doit agir avec le soin, la diligence et la compétence dont ferait preuve, en pareilles circonstances, une personne raisonnablement prudente. Le devoir de tout CA consiste donc à éviter que le risque « cyber » ne se concrétise ou à atténuer rapidement ses répercussions. Ceci implique des actions-clés qu'il ne faut surtout pas négliger ou implanter trop tardivement.

---

[56] *Supra* note 20.

[57] *Supra* note 17.

[58] *Supra* note 17.

[59] Guy PLANTE, Alex HARVEY, Pierre LAMONTAGNE et Julie TURCOTTE, « COVID-19 : à l'aube du déconfinement, les conseils d'administration doivent être proactifs et impliqués », BCF (27 avril 2020), en ligne : <https://www.bcf.ca/fr/intelligence-d-affaires/2020/covid-19-a-l-aube-du-deconfinement-les-conseils-d-administration-doivent-etre-proactifs-et-impliques>.

# Bibliographie


## Législation et règlementation :

### Canada

Lois

*Loi canadienne sur les sociétés par actions*, L.R.C. 1985, c. C-44.
*Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5.
*Loi sur les banques*, LC 1991 c 46.

Règlements

Canada, *Règlement sur les atteintes aux mesures de sécurité*, DORS/2018-64.

### Québec

Lois

*Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1
*Loi sur les sociétés par actions*, RLRQ, c. S-31.1.

## Documents issus d'autorités para-publiques et boursières

Canada, Bureau du surintendant des institutions financières, « L'avenir se trace : le BSIF publie son plan stratégique 2019-2022 », Ottawa, Gouvernement du Canada, 25 avril 2019, en ligne : <https://www.osfi-bsif.gc.ca/Fra/osfi-bsif/med/Pages/strpln1922-nr.aspx>.
Canada, Bureau du surintendant des institutions financières, « Gouvernance d'entreprise », Ottawa, Gouvernement du Canada, septembre 2018, en ligne : <https://www.osfi-bsif.gc.ca/Fra/fi-if/rg-ro/gdn-ort/gl-ld/Pages/CG_Guideline.aspx>.
Canada, Bureau du surintendant des institutions financières, « Impartition d'activités, de fonctions et de méthodes commerciales », Ottawa, Gouvernement du Canada, mars 2009, en ligne : <https://www.osfi-bsif.gc.ca/Fra/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx>.
Commissariat à la protection de la vie privée du Canada, « Lignes directrices pour l'obtention d'un consentement valable », (24 mai 2018), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/>.
Commissariat à la protection de la vie privée du Canada, *Vie privée et cybersécurité – Mettre l'accent sur la protection de la vie privée dans les activités de cybersécurité*, décembre 2014, en ligne : <https://www.priv.gc.ca/media/1776/cs_201412_f.pdf>.
*Cybersécurité et médias sociaux*, ACVM Avis 33-321 (19 octobre 2017).
*Cybersécurité*, ACVM Avis 11-332 (27 septembre 2016).
Institute of Corporate Directors et Toronto Stock Exchange, *Five Years to the* Dey, Toronto, 1999
*Instruction générale 58-201 relative à la gouvernance*, AMF.
*Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*, AMF (février 2020).
*Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*, AMF (juin 2019).
Toronto Stock Exchange Committee on Corporate Governance in Canada, *Where Were the Directors? – Guidelines for Improved Corporate Governance in Canada*, Toronto, TSX, 1994

## Ouvrages et monographies

MILLER, Geoffrey P., *The Law of Governance, Risk Management, and Compliance*, New York, Wolters Kluwer Law & Business, 2014.
SCHELL, Bernadette H. et Clemens MARTIN, *Cybercrime: A Reference Handbook*, Santa Barbaram Abc-Clio, 2004.
TCHOTOURIAN, Ivan et Jean-Christophe BERNIER, *Devoir de prudence et de diligence des administrateurs et RSE*, Cowansville, Yvon Blais, 2014.
WALL, David S., *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge, Polity, 2007

**Articles et chapitres d'ouvrages**

BAINBRIDGE, Stephen M., « *Caremark* and Enterprise Risk Management » (18 mars 2009) UCLA School of Law Document de travail, No. 09-08 à la p 3 (PDF), en ligne : <https://ssrn.com/abstract=1364500>.
DESCHAMPS-MARQUIS, Hélène et Joe ABDUL-MASSIH, « Responsabilité des administrateurs et dirigeants d'entreprise en matière de cybersécurité », dans *Développements récents en droit des affaires*, Cowansville, Yvon Blais, 2019, 191.
DESCÔTEAUX, David et Berin SZOKA, « Protection des données personnelles : l'impact économique de la réglementation d'Internet » (2013) *Les notes économiques*.
GROVE, Hugh, Mac CLOUSE et Laura GEORG SCHAFFNER, « Digitalization impacts on corporate governance » (2018) 7:4 Journal of Governance and Regulation, 53.
JACQUIER, Sébastien, « Entre convivialité, productivité ou sécurité, quelle voie choisir pour les PME à l'ère du tout numérique? Du choix cornélien à l'action préventive » dans Ivan TCHOTOURIAN et Jean-Christophe BERNIER, dir, *Gouvernance d'entreprise, conformité et criminalité économique*, Cowansville, Yvon Blais, 2019, 123.
MIGNAULT, Patrick, « La gestion du risque d'entreprise » dans Guy LEFEBVRE et Stéphane ROUSSEAU, dir, *Introduction au droit des affaires*, Montréal, Thémis, 2018, 107.
TCHOTOURIAN, Ivan, Loïc GEELHAND DE MERXEM et Alexis LANGENFELD, « De la conformité légale à la conformité sociétale : Un rôle de plus en plus complexe pour le CA » dans Ivan TCHOTOURIAN et Jean-Christophe BERNIER, dir, *Gouvernance d'entreprise, conformité et criminalité économique : Approche globale et comparative*, Cowansville, Yvon Blais, 2018, 187.

**Rapports, études et autres de groupes gouvernementaux ou d'organisations privées**

CARRUTHERS, Stuart S., « Le BSIF publie la version finale de sa ligne directrice modifiée sur la gouvernance d'entreprise », *Stikeman Elliott* (26 septembre 2018), en ligne : <https://www.stikeman.com/fr-ca/savoir/droit-assurances/Le-BSIF-publie-la-version-finale-de-sa-ligne-directrice-modifie-sur-la-gouvernance-d-entreprise>.
Center for Board Matters d'EY, *Enjeux de la fin d'exercice 2018 dont doivent tenir compte les comités d'audit canadiens*, EY, 2019, en ligne : https://www.ey.com/fr_ca/audit/what-canadian-audit-committees-should-consider-at-year-end>.
Center for Board Matters d'EY, *Insights on how boards approach digitalization*, EY, 2018.
COITEUX, Vanessa et Stéphane ROUSSEAU, « COVID-19 and Cyber Risk » *Stikeman Elliott* (26 mars 2020), en ligne : <https://www.stikeman.com/en-ca/kh/corporations-commercial-law/COVID19-and-Cyber-Risk>.
COITEUX, Vanessa, et Stéphane ROUSSEAU, « Cinq sujets d'actualité en 2019 : la cybersécurité », *Stikeman Elliott* (14 février 2019), en ligne : <https://www.stikeman.com/fr-ca/savoir/droit-canadien-valeurs-mobilieres/Cinq-sujets-d-actualite-en-2019-la-cybersecurite>.
Davies, *rapport sur la gouvernance 2018*, 2019.
DEERING, Jordan et Daniel A. LESLIE, « Cybersécurité, fraude et responsabilité pendant une pandémie », *Norton Rose Fulbright* (20 mars 2020), en ligne : <https://www.nortonrosefulbright.com/fr-ca/centre-du-savoir/publications/b2e7bd53/cybersecurite-fraude-et-responsabilite-pendant-une-pandemie>.
FERRON, Danielle, Tommy TREMBLAY et Jean-François DE RICO, « Cybersécurité : c'est aussi une question de gouvernance », *Langlois bulletin-conseil* (14 septembre 2018), en ligne : <https://langlois.ca/cybersecurite-cest-aussi-une-question-de-gouvernance/>.
Institut des administrateurs de sociétés – Section du Québec, *Les technologies émergentes : Comprendre les bouleversements à venir. Guide d'introduction pour l'administrateur de sociétés*, avril 2019, en ligne : <https://www.iasquebec.com/fr/les-technologies-emergentes-comprendre-les-bouleversements-a-venir/>.
KPMG Cyber, *cyber security : it's not just about technology*, KPMG, 2014, en ligne : <https://advisory.kpmg.us/articles/2016/cyber-security-not-just-about-technology.html> (consulté le 1er juin 2020) ; et aussi les travaux signalés sur la page de l'ECGI) : ECGI, « Technology and Corporate Governance», en ligne : <https://ecgi.global/content/technology-and-corporate-governance-0>.
MACDOUGALL, Andrew, Lawrence E. RITCHIE et John M. VALLEY, « Supervision du conseil d'administration pendant la pandémie de COVID-19 : une liste de contrôle pour les administrateurs », *Osler* (6 avril 2020), en ligne : <https://www.osler.com/fr/ressources/gouvernance/2020/supervision-du-conseil-d-administration-pendant-la-pandemie-de-covid-19-une-liste-de-controle-pour>.
MILLER OLOFSSON, Danielle, « COVID-19: n'oubliez pas la protection des données dans votre stratégie de réponse face à la crise », BCF (13 mars 2020), en ligne : <https://www.bcf.ca/fr/intelligence-d-affaires/2020/n-oubliez-pas-la-protection-des-donnees-dans-votre-strategie-de-reponse-face-a-la-covid-19>.
PLANTE, Guy, Alex HARVEY, Pierre LAMONTAGNE et Julie TURCOTTE, « COVID-19 : à l'aube du déconfinement, les conseils d'administration doivent être proactifs et impliqués », BCF (27 avril 2020), en ligne : <https://www.bcf.ca/fr/intelligence-d-affaires/2020/covid-19-a-l-aube-du-deconfinement-les-conseils-d-administration-doivent-etre-proactifs-et-impliques>.
PwC Governance Insights Center, *How can boards tackle the Essential Eight and other emerging technologies? Emerging technologies are transforming companies. What should your board know about them?*, PWC, juin 2017, en

ligne : <https://www.pwc.com/us/en/governance-insights-center/publications/assets/essential-emerging-technologies-corporate-boards.pdf>.
*The Global Risks Report 2017*, 12e éd., Genève, World Economic Forum.

**Articles de presse et billets de blogue**

Finance et Investissement, « Risque technologique : le BSIF veut peaufiner ses mécanismes de surveillance », (30 avril 2019), en ligne : https://www.financeinvestissement.com/nouvelles/actualites/risques-technologiques-le-bsif-veut-peaufiner-ses-mecanismes-desurveillance/.
GENOIS GAGNON, Jean-Michel, « Vol de données chez Desjardins : "l'enfer" d'un hameçonnage », *Le Journal de Québec* (9 juillet 2019), en ligne : <https://www.journaldequebec.com/2019/07/09/lenfer-dunhameconnage> (consulté le 1er juin 2020)
La Presse Canadienne, « Vol de données chez Desjardins : 2,9 millions de membres touchés », *Le Huffington Post* (20 juin 2019), en ligne : <https://quebec.huffingtonpost.ca/entry/vol-donnees-desjardins-fuite-securite_qc_5d0bcc4ae4b0859fc3db79d5>.
LABBÉ, Jérôme, « Vol massif de données personnelles chez Desjardins », *Radio-canada* (21 juin 2019), en ligne : <https://ici.radio-canada.ca/nouvelle/1193006/caisses-populaires-desjardins-vol-donnees-personnelles>.
*LaPresse* (2 novembre 2019), en ligne : <https://www.lapresse.ca/actualites/justice-et-faits-divers/201911/01/01-5248031-vol-de-donnees-chez-desjardins-42-millions-de-victimes.php>.
MARCHIVE, Valéry, « Le forum économique mondial insiste sur la menace des cyberattaques », *LeMagIt* (18 janvier 2016), en ligne : <https://www.lemagit.fr/actualites/4500271121/Le-Forum-economique-mondial-insiste-sur-la-menace-des-cyberattaques>.
PÉLOQUIN, Tristan et Hugo PILON-LAROSE, « Vol de données chez Desjardins: 4,2 millions de victimes »,
TCHOTOURIAN, Ivan, « CA et nouvelles technologies » (16 janvier 2020) *Contact* (blogue), en ligne : <http://www.contact.ulaval.ca/article_blogue/ca-et-nouvelles-technologies/>.