

Responsabilité civile et sécurité de l'information



La responsabilité et la sécurité du commerce électronique et de l'Internet, 6 octobre



Plan de la présentation



- Responsabilité civile
 - Principes juridiques
 - Rôle des intermédiaires techniques

- Sécurité de l'information
 - Définition
 - Sources législatives

2

La responsabilité civile



Principes juridiques



Responsabilité civile



Obligation :

- Contractuelle
- Extracontractuelle

- De moyen
- De résultat
- De garantie

4

Responsabilité civile extracontractuelle - définition (1 de 2)



Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.

Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.

Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde.

(Art. 1457 C.c.Q.)

5

Responsabilité civile extracontractuelle - définition (2 de 2)



- Doué de raison
-
- Faute
- Dommage/préjudice
- Lien de causalité

6

Faute (1)



Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.

Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.

Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde.

(Art. 1457 C.c.Q.)

7

La loi

ex 1 : Les virus informatiques



Commets un méfait quiconque volontairement, selon le cas :

- a) détruit ou modifie des données;
- b) dépouille des données de leur sens, les rend inutiles ou inopérantes;
- c) empêche, interrompt ou gêne l'emploi légitime des données;
- d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit.



Art. 430. (1.1) C. cr.

8

La loi

ex. 2 : Les logiciels malicieux



Quiconque, frauduleusement et sans apparence de droit :

- a) directement ou indirectement, obtient des services d'ordinateur;
- b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;
- c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa a) ou b) ou une infraction prévue à l'article 430 concernant des données ou un ordinateur;
- d) a en sa possession ou utilise un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas a), b) ou c), ou en fait le trafic ou permet à une autre personne de l'utiliser.



Art. 342.1 (1) C. cr.

est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

9

La loi

ex. 3 : L'hameçonnage



Quiconque, par supercherie, mensonge ou autre moyen dolosif, constituant ou non un faux semblant au sens de la présente loi, frustre le public ou toute personne, déterminée ou non, de quelque bien, service, argent ou valeur :

a) est coupable d'un acte criminel et passible d'un emprisonnement maximal de quatorze ans, si l'objet de l'infraction est un titre testamentaire ou si la valeur de l'objet de l'infraction dépasse cinq mille dollars;

b) est coupable :

(i) soit d'un acte criminel et passible d'un emprisonnement maximal de deux ans,

(ii) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire,

si la valeur de l'objet de l'infraction ne dépasse pas cinq mille dollars.



Art. 380 (1) C. cr.



La loi

ex. 4 : Le vol d'identité



Commet une infraction quiconque, sciemment, obtient ou a en sa possession des renseignements identificateurs sur une autre personne dans des circonstances qui permettent de conclure raisonnablement qu'ils seront utilisés dans l'intention de commettre un acte criminel dont l'un des éléments constitutifs est la fraude, la supercherie ou le mensonge.



Art. 402.2 (1) C. cr.



« Il n'y a aucune légitimité à emprunter l'identité d'une personne pour laisser croire qu'il est le destinataire de la correspondance qui lui est adressée et qu'il est l'auteur des réponses qui y sont données. »
(Laliberté c. Transit Éditeur inc., 2009 QCCS 6177 (CanLI))

11

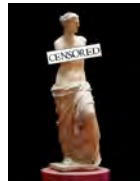
La loi

ex. 4 : Atteintes à la vie privée



Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants:

- 1° Pénétrer chez elle ou y prendre quoi que ce soit;
- 2° Intercepter ou utiliser volontairement une communication privée;
- 3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;
- 4° Surveiller sa vie privée par quelque moyen que ce soit;
- 5° Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public;
- 6° Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.



Art. 36 C.c.Q.

« Invoquant une atteinte illicite à sa réputation et à sa vie privée ainsi que du vandalisme, J... G... (G...) réclame à M... B... (B...) 46 500 \$ à titre de dommages-intérêts. Elle allègue avoir subi ces dommages suite à l'envoi, à des tiers, de photos intimes la représentant nue et au cours de ses ébats sexuels avec B..., ainsi que des vidéos. » J.G. c. M.B., 2009 QCCS 2765 (CanLI)

12

La loi

ex. 4 : Diffamation



Toute personne a droit au respect de sa réputation et de sa vie privée.

Art. 35 C.c.Q.

Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise.



« En l'espèce, la preuve révèle que le défendeur a commis un geste grave car la fiche qu'il a élaborée sur son ordinateur et publiée sur Réseau Contact, constitue une attaque en règle, visant à nuire à l'honneur, à la dignité de la demanderesse (connue du public) et à sa vie privée. » (A c. B, 2009 QCCQ 14676 (CanLII))

13

Les usages

ex. 1 : les pourriels



« it appears clear that sending out unsolicited bulk e-mail for commercial advertising purposes is contrary to the emerging principles of Netiquette. »



1267623 Ontario Inc. v. Nexx Online Inc., 1999 CanLII 15070 (ON S.C.)

14

Dommage



15

Lien de causalité



Doit être la conséquence...

- Logique
 - Directe
 - Immédiate
- ... de la faute.

Question de fait...

16

La responsabilité civile



Rôle des intermédiaires techniques



Principe



- Contrôle
 - Contrôle éditorial? (ex.: blogues)
- Connaissance
 - « Notice and takedown »
- Rôle
 - Passif
 - Actif

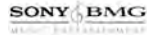
16

Domaines visés



- Violation des droits d'auteur

- Plagiat
- Fichiers Mp3
- Piratage de films



- Diffamation



- Violation de la vie privée



- Vol d'identité

- Virus informatiques



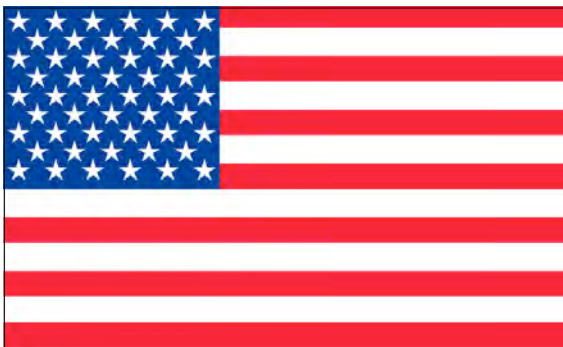
- Etc.

19

Différent selon la juridiction...



20



États-Unis

21

Droits d'auteurs (art. 202 - DMCA)



A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if—

- (1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
- (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
- (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
- (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
- (5) the material is transmitted through the system or network without modification of its content.

22

Diffamation (CDA art. 230 c) (1)



- (1) TREATMENT OF PUBLISHER OR SPEAKER- No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
- (2) CIVIL LIABILITY- No provider or user of an interactive computer service shall be held liable on account of—
 - (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
 - (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

23

Diffamation (CDA art. 230 c) (2)



Donc aucune présomption de contrôle éditorial...

- *Cubby, Inc. v. CompuServe Inc.*

« Plaintiffs have not set forth any specific facts showing that there is a genuine issue as to whether CompuServe knew or had reason to know of Rumorville's contents. Because CompuServe, as a news distributor, may not be held liable if it neither knew nor had reason to know of the allegedly defamatory Rumorville statements, summary judgment in favor of CompuServe on the libel claim is granted. »

- *Stratton Oakmont c. Prodigy Services*


« PRODIGY's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice. For the record, the fear that this Court's finding of publisher status for PRODIGY will compel all computer networks to abdicate control of their bulletin boards, incorrectly presumes that the market will refuse to compensate a network for its increased control and the resulting increased exposure. »

BBS

24



Simple transport ("Mere conduit")
(Directive sur le commerce électronique, art. 12)



1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit **pas responsable** des informations transmises, à condition que le prestataire:

- a) ne soit **pas à l'origine** de la transmission;
- b) **ne sélectionne pas** le destinataire de la transmission

et


- c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.

2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation.

26

Forme de stockage dite "caching"
(Directive sur le commerce électronique, art. 13)



1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire ne soit **pas responsable** au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que:

- a) le prestataire ne **modifie pas l'information**;
- b) le prestataire se conforme aux conditions d'accès à l'information;
- c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises;
- d) le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information

et

- e) le prestataire agit promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible.

2. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette fin à une violation ou qu'il prévienne une violation.

27

Hébergement
(Directive sur le commerce
électronique, art. 14)



1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit **pas responsable des informations stockées à la demande d'un destinataire du service** à condition que:

a) le prestataire n'ait pas effectivement **connaissance** de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente

ou

b) le prestataire, dès le moment où il a de telles connaissances, **agisse promptement** pour retirer les informations ou rendre l'accès à celles-ci impossible.

2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.

28

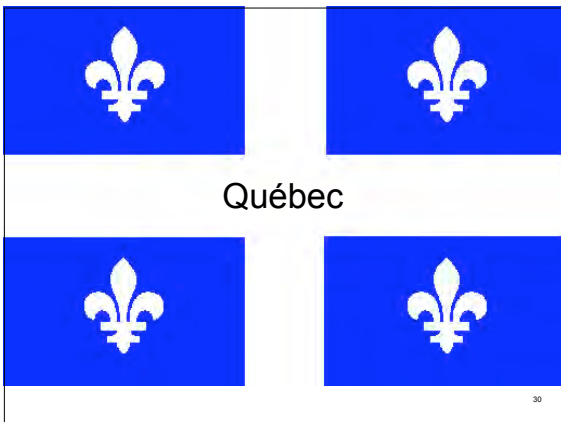
Absence d'obligation générale en
matière de surveillance
(Directive sur le commerce
électronique, art. 15)



1. Les États membres **ne doivent pas imposer** aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une **obligation générale de surveiller les informations** qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.

2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement.

29



30

Loi concernant le cadre
juridique des technologies de
l'information



Articles pertinents :

- 22 - services de conservation ou de référence
- 25 et 26 - responsable de l'accès et gardien
- 27 - Obligation de surveillance
- 36 - Fournisseur d'accès
- 37 - hébergeur

31

Services de
conservation (1)



22. Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remis par ce dernier ou à la demande de celui-ci.

Cependant, il peut engager sa responsabilité, notamment s'il a de fait **connaissance** que les documents conservés servent à la réalisation d'une activité à **caractère illicite** ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité.

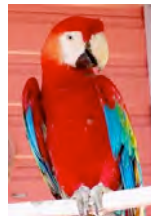


32

Services de
conservation (2)



« Le dossier ne comporte pas de preuve démontrant qu'un ou plusieurs des défendeurs ont le contrôle de ce qui est publié sur le blogue. Certes, ce blogue est accessible par le biais du site web de CECA, mais rien n'indique si l'hyperlien donne accès à un site web différent ou à une autre page du site du CECA. De plus, aucun document n'indique qui en contrôle le contenu. »



Vaillancourt c. Lagacé, 2005 CanLII 29333
(QC C.S.)

33

Services de conservation (3)



« La défenderesse Canoë admet ne pas avoir pris les mesures nécessaires pour faire respecter le règlement de son blogue et pour que les commentaires faisant l'objet du litige n'apparaissent pas sur ledit blogue. Elle soutient à ce sujet que le défendeur Martineau n'a commis aucune faute, car un accord verbal intervenu après la signature de la première entente prévoyait que seul Canoë était responsable de la surveillance du blogue et du respect du règlement. »



Corriveau c. Canoe inc., 2010 QCCS 3396 (CanLII)

34

Services de référence (1 de 3)



22. [...]

De même, le prestataire qui agit à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche, n'est pas responsable des activités accomplies au moyen de ces services. Toutefois, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les services qu'il fournit servent à la réalisation d'une activité à caractère illicite et s'il ne cesse promptement de fournir ses services aux personnes qu'il sait être engagées dans cette activité.



35



AU MOYEN DE : à l'aide de (le moyen exprimé étant généralement concret). ⇔ avec, grâce (à), moyennant.

36

Services de référence (2 de 3)



22. [...]

De même, le prestataire qui agit à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche, n'est pas responsable des activités accomplies au moyen de ces services. Toutefois, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les services qu'il fournit servent à la réalisation d'une activité à caractère illicite et s'il ne cesse promptement de fournir ses services aux personnes qu'il sait être engagées dans cette activité.

Google



CanLII

37

Cesser promptement?



38

Services de référence (3 de 3)



TGI Paris, référé, 12 mai 2003, Lorie c/ M. G.S. et SA Wanadoo Portails



Obligation du gestionnaire du moteur de recherche:

« suppression de la référence au site dès lors qu'elle n'a pu qu'avoir eu connaissance du caractère manifestement illicite de son contenu ».

39

Responsable de l'accès et gardien



25. 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.

26. 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.

40

Obligation de surveillance



27. Le prestataire de services qui agit à titre d'intermédiaire pour fournir des services sur un réseau de communication ou qui y conserve ou y transporte des documents technologiques **n'est pas tenu d'en surveiller l'information**, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités à caractère illicite.

Toutefois, il ne doit prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité, ou pour empêcher les autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions.

41

Fournisseur d'accès



36. Le prestataire de services qui agit à titre d'intermédiaire pour fournir les services d'un réseau de communication exclusivement pour la transmission de documents technologiques sur ce réseau n'est pas responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité.

Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui :

- 1° en étant à l'origine de la transmission du document ;
- 2° en sélectionnant ou en modifiant l'information du document ;
- 3° en sélectionnant la personne qui transmet le document, qui le reçoit ou qui y a accès ;
- 4° en conservant le document plus longtemps que nécessaire pour sa transmission.



42

Hébergeur



37. Le prestataire de services qui agit à titre d'intermédiaire pour conserver sur un réseau de communication les documents technologiques que lui fournit son client et qui ne les conserve qu'à la seule fin d'assurer l'efficacité de leur transmission ultérieure aux personnes qui ont droit d'accès à l'information n'est pas responsable des actions accomplies par autrui par le biais de ces documents.

Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui :

- 1° dans les cas visés au deuxième alinéa de l'article 36 ;
- 2° en ne respectant pas les conditions d'accès au document ;
- 3° en prenant des mesures pour empêcher la vérification de qui a eu accès au document ;
- 4° en ne retirant pas promptement du réseau ou en ne rendant pas l'accès au document impossible alors qu'il a de fait connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau, du fait qu'il n'est pas possible aux personnes qui y ont droit d'y avoir accès ou du fait qu'une autorité compétente en a ordonné le retrait du réseau ou en a interdit l'accès.

43

L'exemple d'ebay® (1 de 3)



● États-Unis



Non responsable



Non responsable

44

L'exemple d'ebay® (1 de 3)



● Europe (France)



Responsable



Responsable

45

L'exemple d'**eBay**[®]
(1 de 3)



● Québec

???

46

La sécurité de l'information



Définition



SSL Certificats

Logiciels antivirus Firewall

Cryptographie NIP

Mots de passe

48



Sécurité Informatique

49



50



Sécurité informationnelle

51



Agents de sécurité
serrures **CCTV**
Clôtures Gicleurs d'incendie
Aménagement paysager Etc. 52



Sécurité informatique \neq Sécurité informationnelle 53



contenant

\neq



contenu 54

Sécurité informatique

"It is initially necessary to establish that altering the orientation of magnetic particles, how programs and data are stored, is damage to property. [...] To **damage a program or data** [...] is not to **cause any physical damage** in the way in which it is normally considered: all that is occurring is that the magnetic particles are being altered."
 - Cive GRINGRAS, 1997

Sécurité informationnelle

"The fact that in the modern age magnetic changes on hard disk drives destroy the valuable data, as opposed, for example, to a fire or flood in a warehouse of paper records, does not change the fact that in each instance the losses result from tangible physical changes to the insured property. Likewise, where a hacker attack targets a computer system or Website and **actual physical damage is occurring, data may be deleted**. In either instance the policyholder may point to tangible physical damage"
 - David R. COHEN et Roberta D. ANDERSON, 2000

...

55

Loi concernant le cadre juridique des technologies de l'information

[...] 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. **(article 26)**

56

La sécurité de l'information passe par...

The diagram consists of two overlapping circles. The left circle is labeled 'Sécurité informatique' and contains icons of a computer monitor, a keyboard, and a document. The right circle is labeled 'Sécurité physique' and contains icons of a server rack, a fire extinguisher, and a document. The overlapping area in the center contains icons of a server rack, a fire extinguisher, and a document.

57

Définition: sécurité informatique



Absence réelle de **danger** que la réunion d'un ensemble de conditions matérielles et logiques permet d'obtenir dans la saisie, le traitement et la transmission des données, ainsi que dans la consultation des fichiers automatisés et la production des résultats. (**Grand dictionnaire terminologique**)

58

Définition: sécurité informationnelle



Protection des ressources informationnelles d'une organisation, face à des **risques** définis, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la **confidentialité**, l'**intégrité** et la **disponibilité** de l'information traitée. (**Grand dictionnaire terminologique**)

59

Absence de danger vs. Absence de risques

Risques : « Danger éventuel plus ou moins prévisible. » (**Petit Robert**)

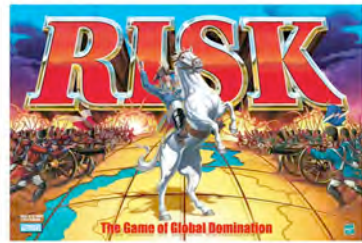
60



Absence de danger = Absence de risques

61

RISQUE?



62

Risques



« danger éventuel plus ou moins prévisible »
Hubert REID, Dictionnaire de droit québécois et canadien

63

Risques



« Événement éventuel, incertain, dont la réalisation ne dépend pas exclusivement de la volonté des parties et pouvant causer un dommage. »

OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

64

Risques



- Dommages physiques (feu, inondation, vandalisme, panne de courant, catastrophe naturelle)
- Interaction humaine (action ou inaction accidentelle ou intentionnelle qui peut interrompre la productivité)
- Défaillance technique (échec des systèmes informatiques et périphériques)
- Attaques internes ou externes (pirates, bidouilleurs, etc.)
- Abus de données (partage de secrets commerciaux, fraude, espionnage, vol)
- Perte de données (destruction intentionnelle ou non intentionnelle d'informations)
- Erreurs logicielles (erreurs informatiques, erreurs de saisie, dépassement de la mémoire tampon)

65

Risques



« danger éventuel **plus ou moins prévisible** »



Hubert REID, *Dictionnaire de droit québécois et canadien*

« Événement éventuel, incertain, dont la réalisation ne dépend pas exclusivement de la volonté des parties et pouvant causer un dommage. »

OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

66


Risques

→ Gestion des risques

67

Gestion des risques




« Ensemble des activités qui consistent à recenser les risques auxquels l'entité est exposée, puis à définir et à mettre en place les mesures préventives appropriées en vue de supprimer ou d'atténuer les conséquences d'un risque couru. »

OFFICE DE LA LANGUE FRANÇAISE, Grand Dictionnaire terminologique

68

Gestion des risques



- Vulnérabilités
- Menaces
- Contre-mesures (ou contrôles)

69

Vulnérabilités



« Faiblesse d'un système se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent. »

OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

70

Vulnérabilités



- Techniques  
- Physiques   
- Opérationnelles   
- Liées à la gestion du personnel  

71

Menaces



« Événement potentiel et appréhendé, de probabilité non nulle, susceptible de porter atteinte à la sécurité informatique. »

OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

72

Menaces



- Humaines (pirates, employés)
- Naturelles (tremblements de terre, inondations)
- Techniques (erreurs logicielles)
- Physiques (panne de courant)



73

Contre-mesures



« Mesure prise pour réduire les risques au moyen de la réduction de l'importance des éléments de configuration, des menaces auxquelles ils font face ou de leur vulnérabilité à ces menaces. »

OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

74

Contre-mesures



- Techniques
- Physiques
- Opérationnelles
- Liées à la gestion du personnel

- Réduire les vulnérabilités
- « Réduire » les menaces

75

Risques



Probabilité qu'une menace exploite une vulnérabilité avant qu'une contre-mesure soit mise en place.

76

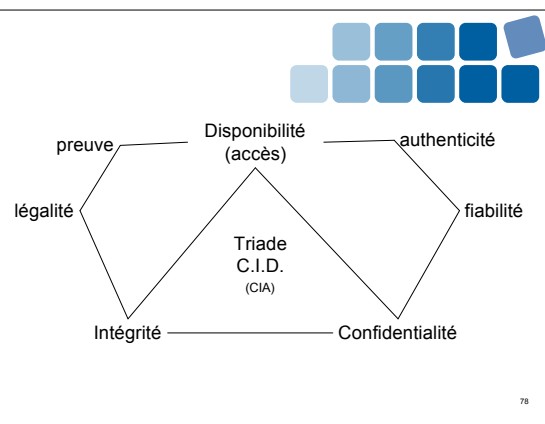
Définition: sécurité de l'information



« Protection des ressources informationnelles d'une organisation, face à des risques définis, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la **confidentialité**, l'**intégrité** et la **disponibilité** de l'information traitée. »

OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

77



78



Définition: sécurité de l'information

[...] 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. (Loi concernant le cadre juridique des technologies de l'information, article 26)

La sécurité de l'information

Sources législatives

The logo of the Centre de recherche en droit public (CRDP) is located in the bottom right corner of the slide. It consists of the letters 'C', 'R', 'D', and 'P' arranged in a 2x2 grid, each inside a small blue square.

Loi sur la protection des renseignements personnels dans le secteur privé



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. (art. 10)

82

Loi sur la protection des renseignements personnels et les documents électroniques



Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. (Annexe 1, art. 4.7)


83

Sécurité de l'information



Protection des renseignements personnels


84



Sécurité de l'information > Protection des renseignements personnels

85

Définition: sécurité de l'information




« Protection des **ressources informationnelles** d'une organisation, face à des risques définis, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée. »

OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

86

Loi concernant le cadre juridique des technologies de l'information



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. (art. 25)

87



« Dans le présent dossier, l'intimé, en hébergeant, sur son propre site internet, les liens informatiques, code d'utilisateur et mot de passe de son frère (chef no. 1), sans protéger adéquatement l'accès à ceux-ci, n'a pas, de toute évidence, respecté les obligations qui lui étaient imposées par l'article 25 de la Loi concernant le cadre juridique des technologies de l'information, soit celles «de 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» »

Chambre de l'assurance de dommages c. Kotliaroff, 2008 CanLII 19078 (QC C.D.C.H.A.D.)

88

Renseignement confidentiel



« [l]a qualification de « renseignements confidentiels » est une question de fait mais elle est aussi évaluée d'une façon objective. Il ne suffit pas que l'employeur décrète que tel ou tel renseignement est confidentiel pour qu'il le soit. Sont habituellement considérés comme confidentiels les secrets de commerce ou de fabrication, les plans et maquettes liées au développement d'une technique ou d'un produit, les listes de clients secrètes ou contenant des renseignements privilégiés [...] ou toute autre information qui n'est pas généralement connue et ne peut pas être obtenue ou reconstituée facilement. »

Marie-France BICH, La viduité post-emploi: loyauté, discrétion et clauses restrictives », dans *Développements récents en droit de la propriété intellectuelle*, Cowansville, Yvon Blais, 2003, p. 243, 305.

89

Renseignement confidentiel



- Critères:
 - l'étendue de la diffusion de l'information à l'extérieur de l'entreprise;
 - l'étendue de la diffusion de l'information au sein de l'entreprise;
 - l'étendue des mesures de sécurité mise en place pour assurer la confidentialité de l'information;
 - la valeur de l'information pour des tiers;
 - l'argent et l'effort investis afin de collecter ou développer l'information;
 - la facilité avec laquelle un tiers pourrait acquérir ou dupliquer l'information par lui-même.

Sophie ROMPRÉ, *La surveillance de l'utilisation d'Internet au travail*, Cowansville, Yvon Blais, 2009, p. 31

Pharand Ski Corp. c. Alberta, 1991 CarswellAlta 85 (ABQB), citant Ansell Rubber Co. c. Allied Rubber Industries Pty. Ltd., [1967] V.R. 37 et Dage Nominees Pty. Ltd. c. Viscount Plastics Products Pty. Ltd., [1979] V.R. 167.

Renseignement confidentiel



(1) Pour l'application du présent article, la personne qui fournit des renseignements au Conseil peut désigner comme confidentiels :

- a) les secrets industriels;
- b) les renseignements financiers, commerciaux, scientifiques ou techniques qui sont de nature confidentielle et qui sont traités comme tels de façon constante par la personne qui les fournit;
- c) les renseignements dont la communication risquerait vraisemblablement soit de causer à une autre personne ou elle-même des pertes ou profits financiers appréciables ou de nuire à sa compétitivité, soit d'entraver des négociations menées par cette autre personne ou elle-même en vue de contrats ou à d'autres fins. (**Loi sur les télécommunications, art. 39**)

91

Renseignement confidentiel



Un organisme public ne peut communiquer le secret industriel d'un tiers ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni par un tiers et habituellement traité par un tiers de façon confidentielle, sans son consentement. (**Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, art. 23**)

92

Renseignement confidentiel



- Renseignements confidentiels par nature
- Renseignements confidentiels selon l'interlocuteur
- Renseignements confidentiels selon le contexte de leur communication
- Renseignements confidentiels selon le contexte de leur conservation

93

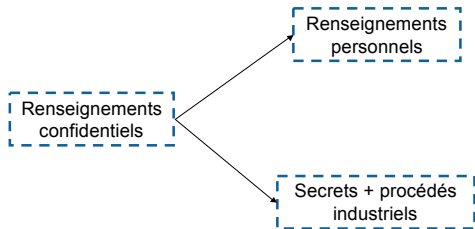
Renseignement confidentiel
« par nature »



- Renseignements personnels (*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q. c. A-2.1, art. 53)
- Renseignements relatifs aux électeurs (*Loi électorale*, L.R.Q. c. E-3.3, art. 40.39)
- NIP (*Loi sur l'assurance maladie*, L.R.Q. c. A-29, art. 9.0.1.1)
- Secrets industriels (*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q. c. A-2.1, art. 23)
- Procédés industriels (*Loi sur la Santé et la sécurité du travail*, L.R.Q. c. S-2.1, art. 123)
- Etc.

94

Renseignement confidentiel
« par nature »



95

Renseignement confidentiel
« selon l'interlocuteur »



- Commission des droits de la personne (*Charte des droits et libertés de la personne*, L.R.Q. c. C-12, art. 93)
- Renseignements sur l'origine d'un incendie obtenu par le ministre de l'assureur ou la municipalité (*Loi sur la sécurité incendie*, L.R.Q. c. S-3.4, art. 150)
- Échanges entre le directeur d'un établissement de détention et une victime (*Loi sur le Système correctionnel du Québec*, L.R.Q. c. S-40.1, art. 175.1)
- Avis du juriconsulte à un député (*Loi sur l'Assemblée nationale*, L.R.Q. c. A-23.1)
- Renseignement obtenu par un agent de surveillance de sentier (*Loi sur les Véhicules hors route*, L.R.Q. c. V-1.2, art. 43)
- Médiateur (*Loi sur les normes du travail*, L.R.Q. c. N-1.1, art. 123.3)
- Notaire (*Loi sur le Notariat*, L.R.Q., c. N-3, art. 14.1)
- Acupuncteur (*Loi sur l'acupuncture*, L.R.Q. c. A-5.1, art. 13)
- Comptable agréé (*Loi sur les comptables agréés*, L.R.Q. c. C-48, art. 22.2)
- Etc.

96

Renseignement confidentiel
« selon le contexte de leur communication »



- Toute information verbale ou écrite recueillie pendant la médiation (*Loi sur les chemins de fer*, L.R.Q. c. C-14.1, art. 19)
- Renseignements obtenus en vertu de la *Loi concernant les droit sur les mutations immobilières* (L.R.Q. c. D-15.1, art. 22)
- Renseignements concernant les conflits d'intérêts des administrateurs de la Caisse de dépôt communiqués au ministre des Finances (*Loi sur la Caisse de dépôt et placement du Québec*, L.R.Q. c. C-2, art. 42)
- Renseignements obtenus en vertu de la *Loi facilitant le Paiement des pensions alimentaires* (L.R.Q. c. P-2.2, art. 75)
- Renseignements relatifs à un cotisant ou un bénéficiaire obtenus en vertu de la *Loi sur le Régime des rentes du Québec* (L.R.Q. c. R-9, art. 207)
- Renseignement fourni à la *Commission des loyers* (*Loi sur la Régie du logement*, L.R.Q. c. R-8.1, art. 91)
- Renseignements obtenus dans l'application de la *Loi concernant les Droits sur les mines* (L.R.Q. c. D-15, art. 80.2)
- Conférence de règlement à l'amiable (*Code de procédure civile*, L.R.Q. c. C-25, art. 151.21)
- Etc.

97

Renseignement confidentiel
« selon le contexte de leur conservation »



- Dossier du tribunal (*Loi sur la Protection de la jeunesse*, L.R.Q. c. P-34.1, art. 96)
- Dossier administré par le curateur public (*Loi sur le Curateur public*, L.R.Q. c. C-81, art. 51)
- Dossier de l'*Office des personnes handicapées du Québec* concernant une personne handicapée (*Loi assurant l'exercice des droits des personnes handicapées en vue de leur intégration scolaire, professionnelle et sociale*, L.R.Q. c. E-20.1)
- Dossiers médicaux (*Loi sur les services de santé et les services sociaux pour les autochtones cris*, L.R.Q. c. S-5, art. 7; *Loi sur les services de santé et les services sociaux*, L.R.Q. c. S-4.2, art. 19)
- Dossier Fiscal (*Loi sur le ministère du Revenu*, L.R.Q. c. M-31, art. 69)
- Etc.

98

Pour résumer...



- Renseignements personnels;
- Renseignements publics;
- Secrets commerciaux;
- Listes de clients;
- Salaires des employés;
- Etc.



99

Code civil du Québec



Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.

Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.

Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde. (art. 1457)

100

Intensité de l'obligation



Mesures correspondant au degré de sensibilité

Mesures raisonnables

Les renseignements plus sensibles devraient être mieux protégés.

Obligation de moyens **renforcée**

101

Mesures raisonnables



Les méthodes de protection devraient comprendre :

- a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;
- b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et
- c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement. (Loi sur la protection des renseignements personnels et les documents électroniques, Annexe 1, art. 4.7.3)

102

Mesures raisonnables



- Verrouiller les classeurs et les bureaux
 - *Stacey c. Sauvé Plymouth Chrysler (1991) inc.*, REJB 2002-32362 (C.Q.)
 - Conclusions # 185, 376 et 107
- Adopter des politiques et procédures de contrôle, sensibiliser les employés
 - *Fleury c. C.P. St-Jean Berchmans*, (2002) PV 98 01 15, 16 et 17 (C.A.I.)
 - *X c. Centre médical Boucherville*, (1994) AZ-95151501 (C.A.I.)
 - Conclusions # 52, 304, 54, 242, 11, 292, 177, 377, 226, 374 et 380
- Assurer la confidentialité d'adresses de courriels dans le cadre d'un envoi collectif
 - Conclusion # 277
- L'encodage, le chiffrement ou le hachage de données sensibles
 - Conclusions # 185, 107 et 393
- L'utilisation de mots de passe ou autres identifiants
 - Conclusions # 372, 281, 376, 329, 137 et 324
- Limiter l'accès aux seules personnes ayant besoin de l'information
 - *Bell c. Michigan Council 25 of the American Federation of State, County, and Municipal Employees, AFL-CIO, Local 1023 (US)*
 - Conclusions # 185, 376 et 107.

103

Mesures raisonnables



« Brazos had policies in place to protect the personal information, trained Wright concerning those policies, and transmitted and used data in accordance with those policies. Wright lived in a relatively "safe" neighborhood and took necessary precautions to secure his house from intruders. His inability to foresee and deter the specific burglary in September 2004 was not a breach of Brazos's duty of reasonable care. »

Guin c. Brazos Higher Education Service Corp., Inc.

« la planificatrice financière, en l'espèce, n'avait pas suivi les recommandations de la banque concernant la sécurité matérielle et avait laissé l'ordinateur sans surveillance sur le siège de sa voiture. La commissaire adjointe a par conséquent conclu que la banque n'avait pas respecté le principe 4.7. »

Conclusion # 289

« Les ordinateurs portatifs sont des cibles de choix pour les voleurs, particulièrement ceux qui se trouvent dans les bureaux où les intrus peuvent entrer et circuler librement (c'est-à-dire vol à la tire). Ces lieux doivent être adéquatement protégés en tout temps afin d'assurer la protection des renseignements personnels. Les ordinateurs portatifs ne devraient jamais être laissés sans surveillance et non verrouillés dans un endroit qui n'est pas sécurisé. »

Conclusion # 393

104

Mesures raisonnables



Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels, 2007 CanLII 41283 (C.V.P.C.)

105

Mesures raisonnables



T.J. Hooper c. Northern Barge, 60 F. 2d 737 (1932)

106

Mesures raisonnables



« Le fait qu'un professionnel ait suivi la pratique de ses pairs peut constituer une forte preuve d'une conduite raisonnable et diligente, mais ce n'est pas déterminant »

Roberge c. Bolduc, [1991] 1 R.C.S. 374.

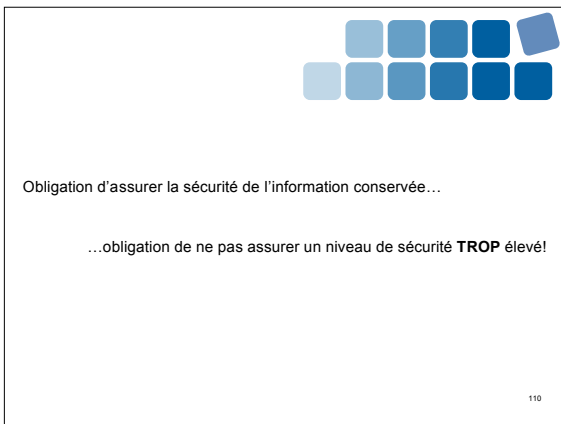
107

Mesures raisonnables ?



108







Contrôles d'accès physiques



- Règlements d'urbanisme
 - Clotûres, barrières, fossés, etc.
 - Ex.: Le *Règlement sur les clôtures* de Montréal interdit:
 - L'érection de clôtures de plus de 90 cm de hauteur
 - Le barbelé
- Code du bâtiment
 - Impose la présence de parcours sans obstacle
 - Interdit les mécanismes de verrouillage électromagnétique
- Code civil du Québec (art. 36) et Charte des droits et libertés de la personne (art. 46)
 - Limitent l'utilisation des caméras de surveillance

112

Contrôles d'accès administratifs



[...] La vérification de l'identité ou de l'identification doit se faire dans le respect de la loi. [...] La vérification de l'identité d'une personne peut aussi être effectuée à partir de **caractéristiques, connaissances** ou **objets** qu'elle présente ou possède. (**Loi sur la protection des renseignements personnels dans le secteur privé, art. 40**)

113

Contrôles d'accès administratifs



Nul ne peut refuser d'acquiescer à une demande de bien ou de service ni à une demande relative à un emploi à cause du refus de la personne qui formule la demande de lui fournir un renseignement personnel sauf dans l'une ou l'autre des circonstances suivantes:

- 1° la collecte est nécessaire à la conclusion ou à l'exécution du contrat;
- 2° la collecte est autorisée par la loi;
- 3° il y a des motifs raisonnables de croire qu'une telle demande n'est pas licite.

En cas de doute, un renseignement personnel est réputé non nécessaire. (**Loi sur la protection des renseignements personnels dans le secteur privé, art. 9**)

Connaissances...

114

Contrôles d'accès administratifs



Nul ne peut exiger que l'identité d'une personne soit établie au moyen d'un procédé ou d'un dispositif qui porte atteinte à son intégrité physique. [...] (Loi sur la protection des renseignements personnels dans le secteur privé, art. 43)

Nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. [...] (Loi sur la protection des renseignements personnels dans le secteur privé, art. 44)

...caractéristiques...



115

Contrôles d'accès administratifs



[...] À moins que la loi le prévoit expressément en vue de protéger la santé des personnes ou la sécurité publique, nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve. (Loi sur la protection des renseignements personnels dans le secteur privé, art. 43)

... objets.



116

Obligations de divulgation



- Code des professions
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et/ou Loi sur la protection des renseignements personnels dans le secteur privé
 - Droit d'accès
 - Droit de correction
- Loi sur les compagnies
 - Oblige la divulgation de:
 - Liste des clients
 - Propriété intellectuelle
 - Etc. (art. 98, 191)
 - Droit d'accès à des tiers (vérificateur) (art. 114, 207)
- Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes
 - Oblige la divulgation de certaines transactions (art. 7)

117



Toute personne peut se dégager de sa responsabilité pour le préjudice causé à autrui par suite de la divulgation d'un secret commercial si elle prouve que l'intérêt général l'emportait sur le maintien du secret et, notamment, que la divulgation de celui-ci était justifiée par des motifs liés à la santé ou à la sécurité du public. **(Code civil du Québec, art. 1472)**

118



Code criminel



Sans compter les contraintes imposées par le droit pénal...



Loi sur les armes à feu



Loi sur les dispositifs émettant des radiations

119



... et les règles relatives à la prescription.

120

Pour conclure...



121

Merci...



Nicolas Vermeys
Directeur adjoint
Laboratoire sur la cyberjustice
nicolas.vermeys@umontreal.ca
Tél. : (1) 514-343-6111 (0652)
Fax : (1) 514-343-7508