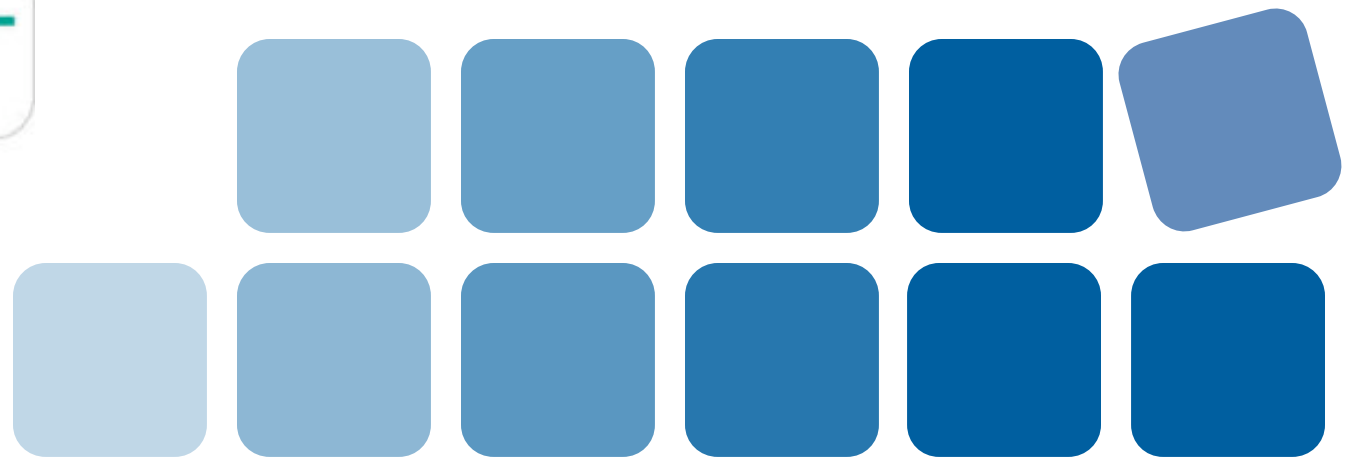
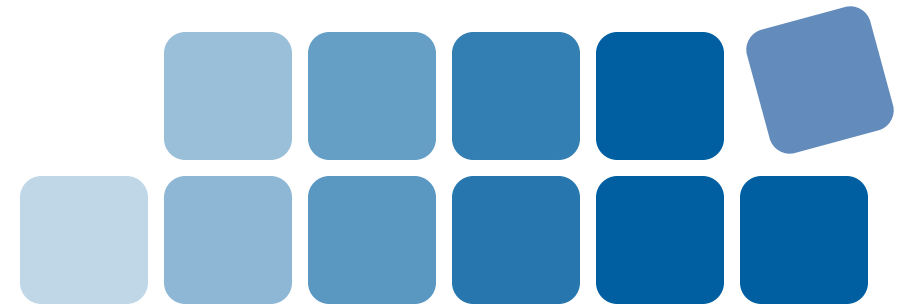


Intrusion dans les systèmes informatiques et méfaits



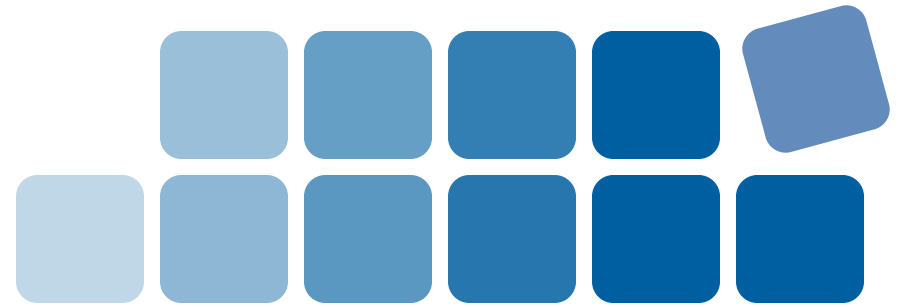
Centre Mont-Royal, Montréal

Le 26 avril 2010



MÉFAIT?

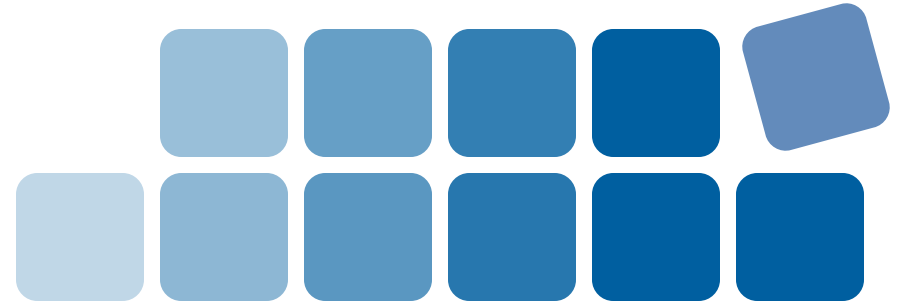
Code criminel



430. (1) Commet un **méfait** quiconque volontairement, selon le cas :

- a) détruit ou détériore un bien;
- b) rend un bien dangereux, inutile, inopérant ou inefficace;
- c) empêche, interrompt ou gêne l'emploi, la jouissance ou l'exploitation légitime d'un bien;
- d) empêche, interrompt ou gêne une personne dans l'emploi, la jouissance ou l'exploitation légitime d'un bien.

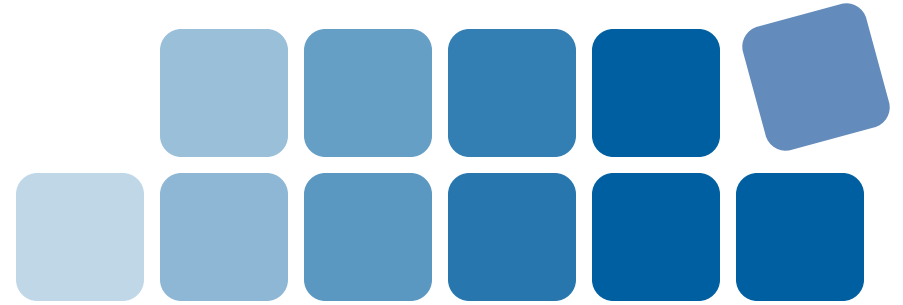
Code criminel



430. (1.1) Commet 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.

Code criminel



342.1 (1) Quiconque, frauduleusement et sans apparence de droit :

a) directement ou indirectement, obtient des services d'ordinateur;

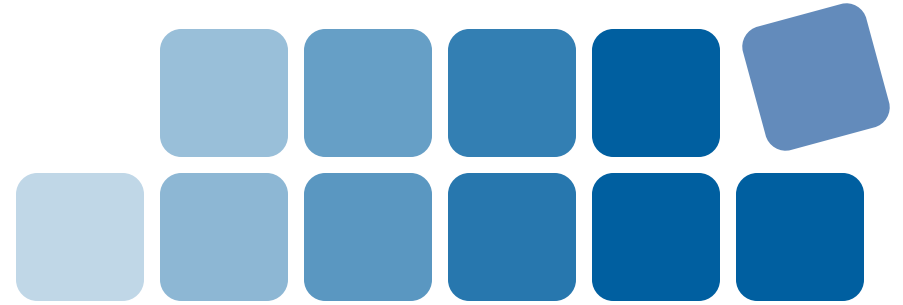
b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;

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,

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.

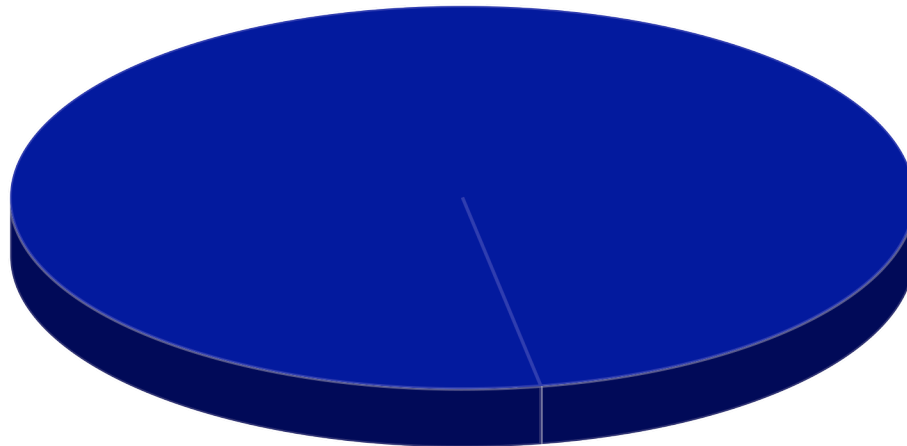
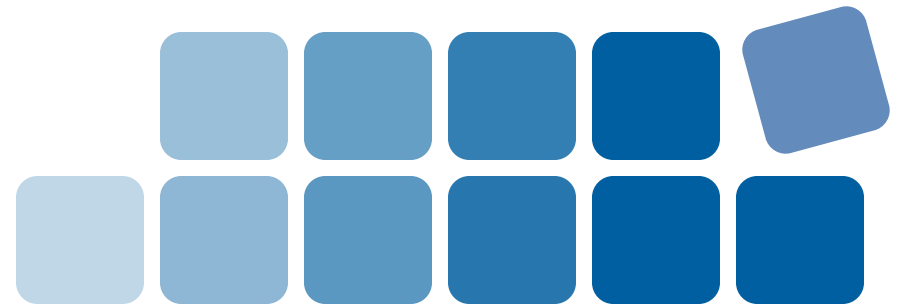
Crime informatique



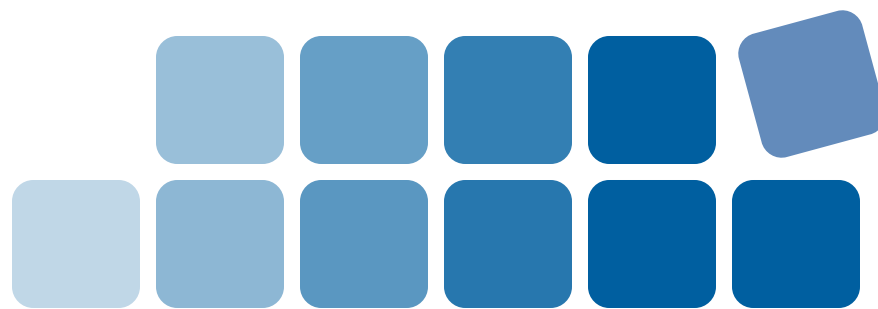
« Acte illicite commis au moyen de l'informatique, ou ayant pour cible le système informatique ou l'un de ses éléments. »

OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

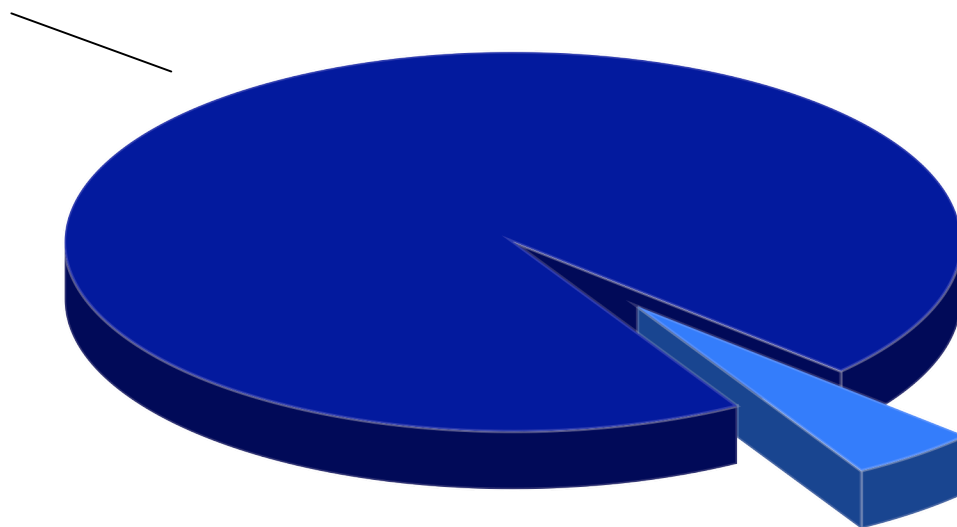
Crime informatique



Crime informatique

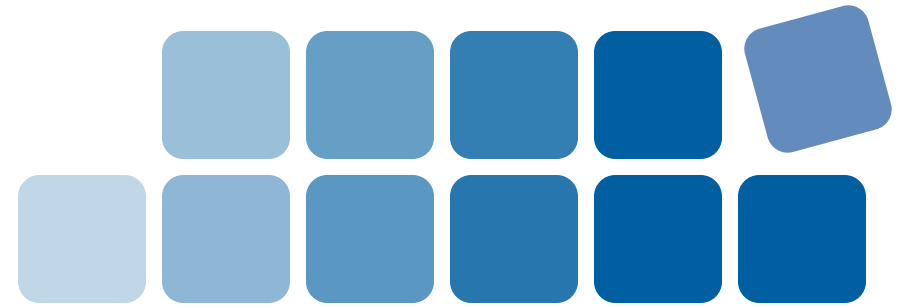


Pédophilie

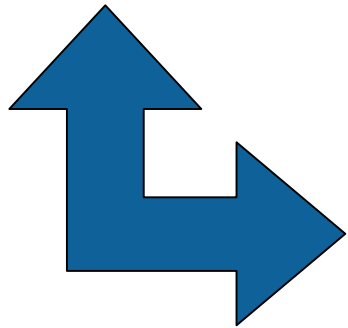


méfais

Méfait



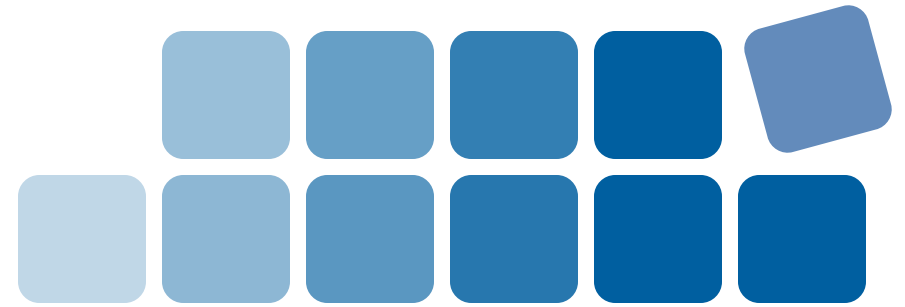
Méfait informatique



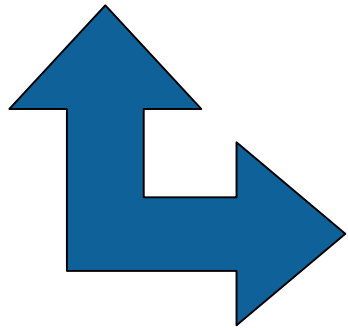
Atteinte aux données

- Destruction / Modification / Corruption
- Accès illicite
- Limiter l'accès

Méfait

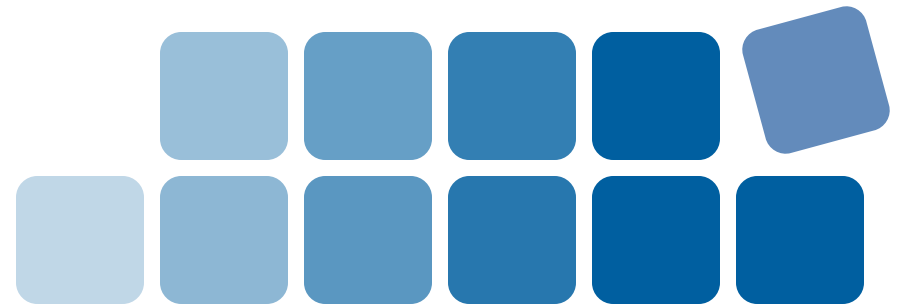


Méfait informatique



Atteinte à la sécurité
De l'information...

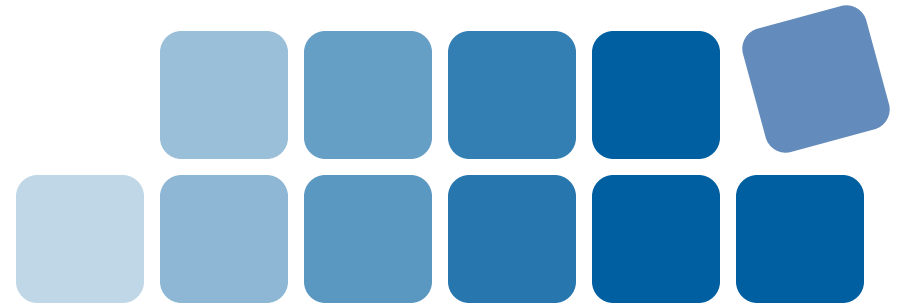
Sécurité de l'information



« 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. »

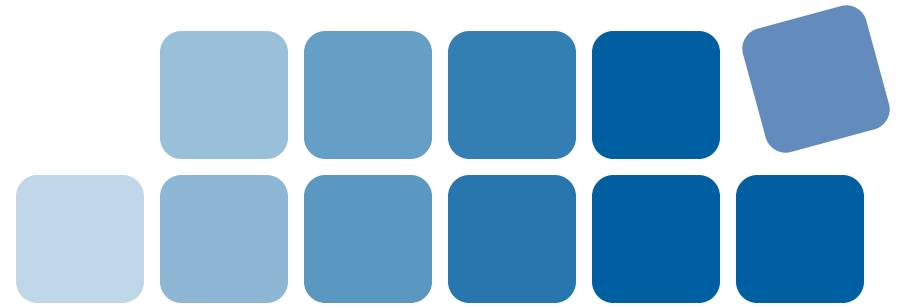
OFFICE DE LA LANGUE FRANÇAISE, *Grand Dictionnaire terminologique*

Loi concernant le cadre juridique des technologies de l'information



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.

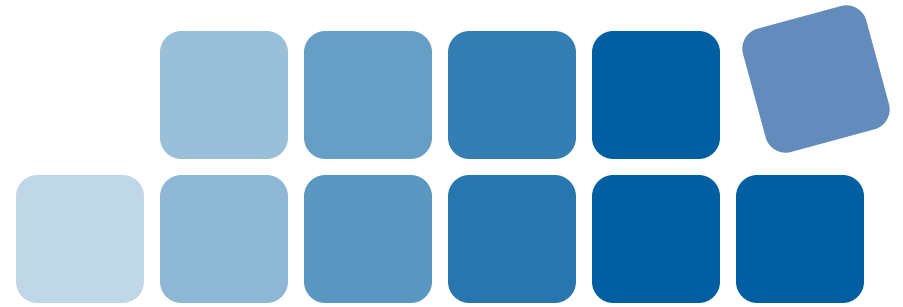
Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en **assurer la sécurité**, en préserver l'**intégrité** et, le cas échéant, en protéger la **confidentialité** et en interdire l'**accès** 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.



confidentialité

intégrité
accès

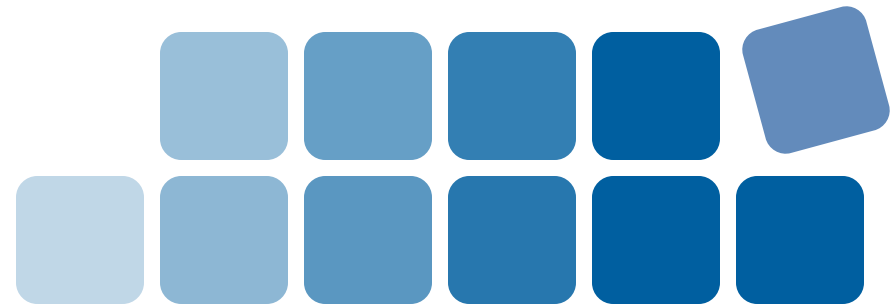
Donnée



« données » Représentations d'informations ou de concepts qui sont préparés ou l'ont été de façon à pouvoir être utilisés dans un ordinateur.

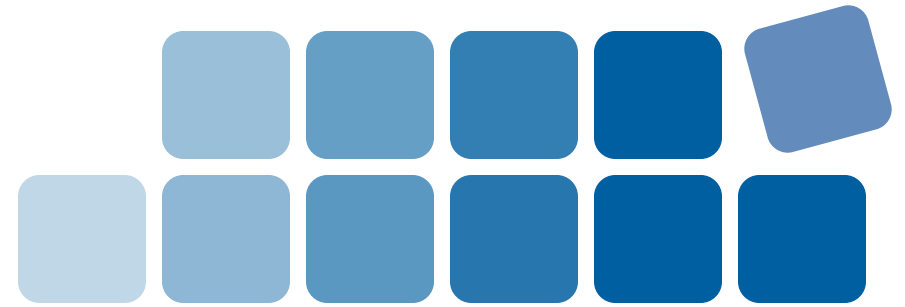
Code criminel, art. 342.1

*Loi concernant le cadre juridique
des technologies de l'information*



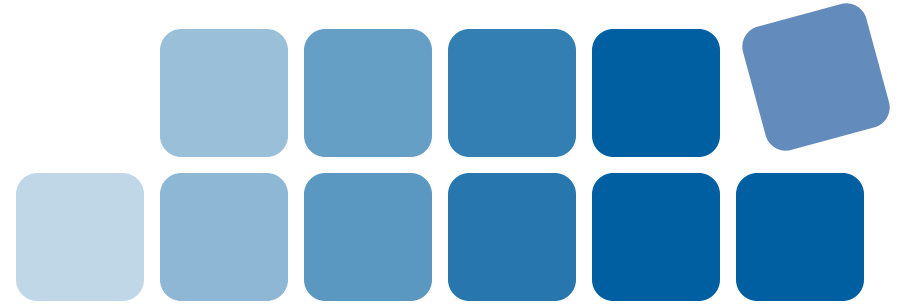
25. La personne responsable de l'accès à un document technologique qui porte un **renseignement confidentiel** doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche 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.

Donnée



Donnée $\stackrel{?}{=}$ Renseignement
confidentiel

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. (Telle que citée dans *Institut de zoothérapie du Québec Inc. c. Rioux*, 2005 CanLII 10507 (QC C.S.), par. 34.



« [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. »

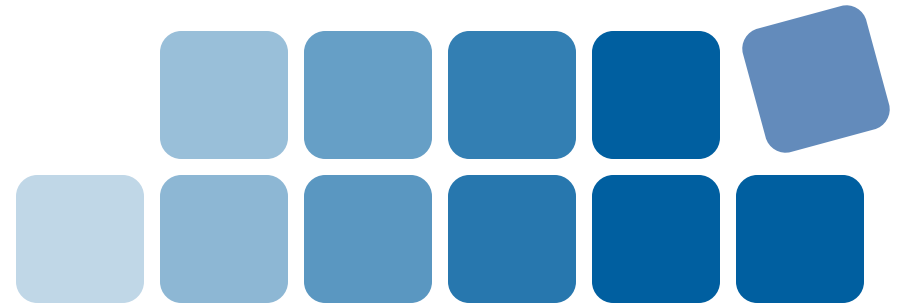
Renseignements personnels



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. (**Loi sur la protection des renseignements personnels dans le secteur privé, art. 10**)

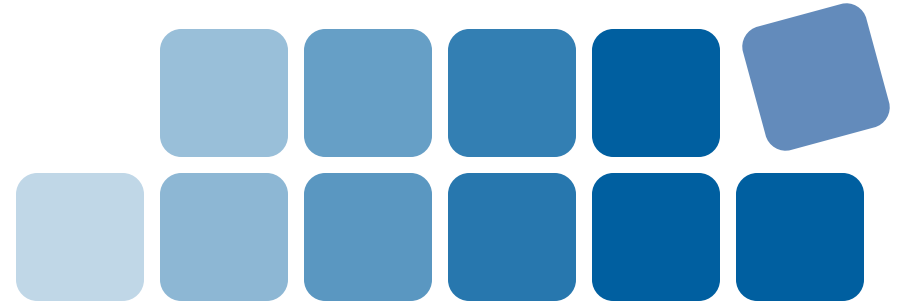
Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. (**Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, art. 63.1**)

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. (**Loi sur la protection des renseignements personnels et les documents électroniques, Annexe 1, art. 4.7**)



« 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, respecter 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» »

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

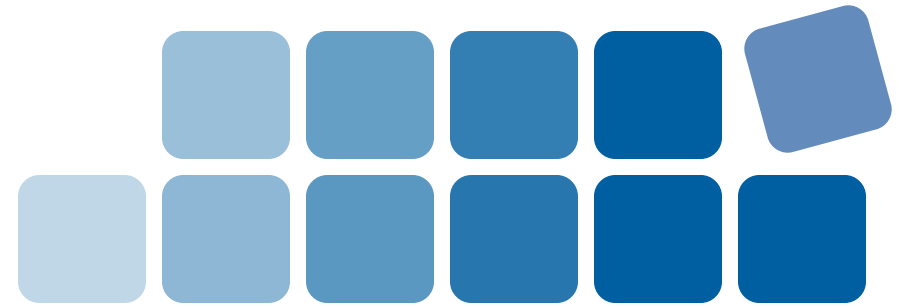


● Critères:

- 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.

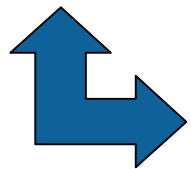
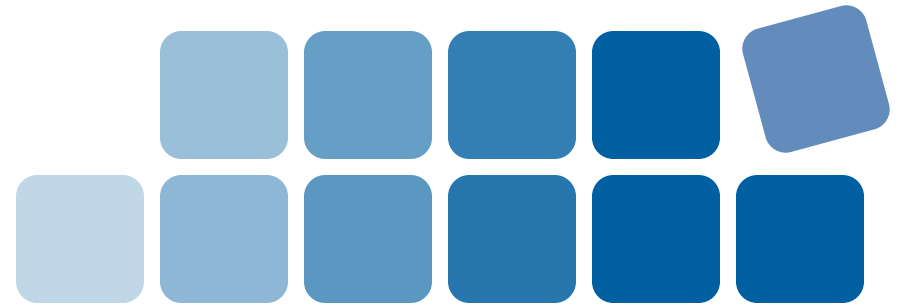
Pharand Ski Corp. c. Alberta, 1991 CarswellAlta 85 (ABQB), citant *Ansell Rubber Co. c. Allied Rubber Industries Pty. Ltd.*, [1967] V.R. 37 et *Deta Nominees Pty. Ltd. c. Viscount Plastics Products Pty. Ltd.*, [1979] V.R. 167.

Donnée

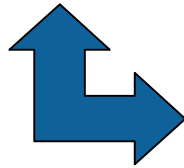




Donnée > Renseignement
confidentiel

Responsabilité civile vs. Responsabilité pénale



Donnée

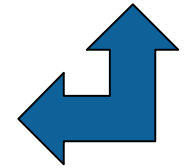
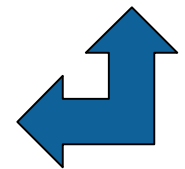




- 430(1.1) C.cr. 
- 1457 C.c.Q. 
- 1457 C.c.Q. ABC inc.



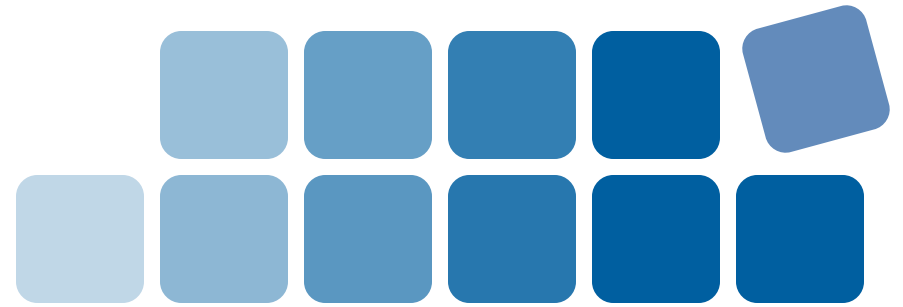
ABC inc.

Renseignement
confidentiel



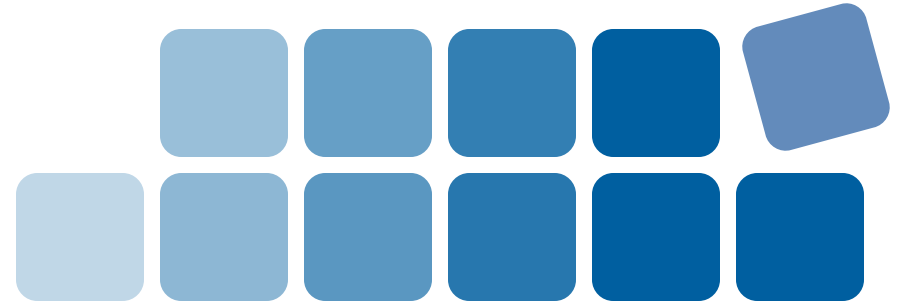
- 430(1.1) C.cr. 
- 1457 C.c.Q. 
- 25 Lccjti ABC inc.

Méfais ?



- ~~Pourriel (Spam)~~ (*R. v. Hamilton, 2002 ABQB 0015*)
- Vol de données ??? (*R. c. Alexander, 2006 CanLII 26480*)
- Virus / vers / chevaux de Troie
- Hameçonnage / Harponnage (Phishing / spearphishing)
- Logiciels espions (spyware)
- Bidouillage (Hacking)

Critères



342.1 (1) Quiconque, **frauduleusement** et **sans apparence de droit** :

a) directement ou indirectement, obtient des services d'ordinateur;

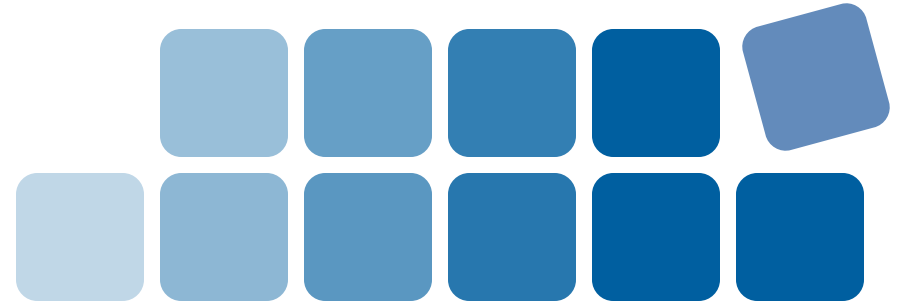
b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;

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,

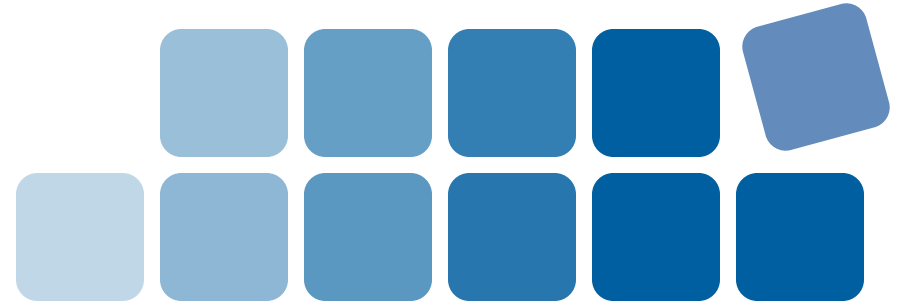
est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Critères



« À la lecture de l'article 342.1, la poursuite doit démontrer que l'accusé a, non seulement **sans apparence de droit** mais également **frauduleusement**, obtenu des services d'ordinateur. Il est admis qu'il n'y avait aucune apparence de droit. L'obtention frauduleuse des services d'ordinateur doit donc être prouvée par la poursuite. La conduite de l'accusé n'est pas frauduleuse simplement parce qu'elle n'est pas autorisée. Elle doit aussi posséder des caractéristiques malhonnêtes et moralement mauvaises. »

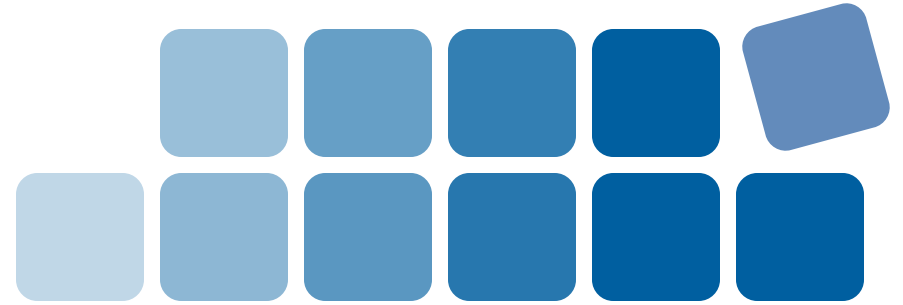
Exemples (1.0)



- *R. c. Parent* (2010 QCCQ 82)
 - Un policier utilise son mot de passe pour entrer dans le système informatique de la GRC et obtenir des renseignements personnels qu'il **remet** à un tiers (crime organisé).
 - Pas contraire à 342.1.
- *R. c. Martineau* (2003 CanLII 29509)
 - Des employés d'un mandataire de la S.A.A.Q. utilisent son mot de passe pour entrer dans le système informatique de la S.A.A.Q. et obtenir des renseignements personnels qu'ils **vendent** aux Hell's Angels. (Attenta contre Michel Auger)
 - Contraire à 342.1.



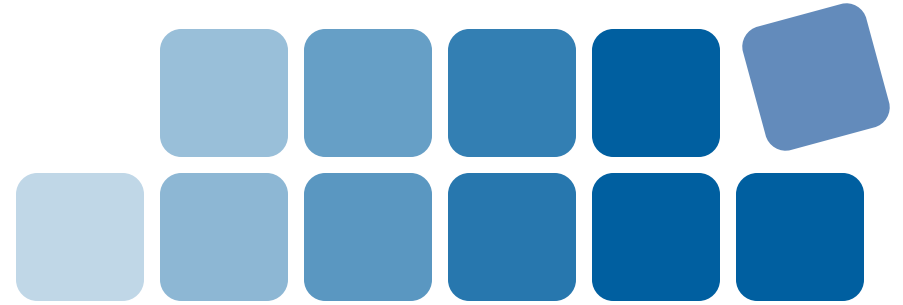
Exemples (1.1)



- *Sûreté du Québec c. Bergeron*, (2008 QCCS 1771)

« monsieur Coulombe, alors à l'emploi de la Sûreté municipale de Port-Cartier, utilise l'ordinateur du poste de police relié au Centre de renseignements policiers du Québec (le CRPQ) pour des fins personnelles, i.e. pour obtenir des renseignements sur son ex-épouse, leur fils et son ex-belle-mère »

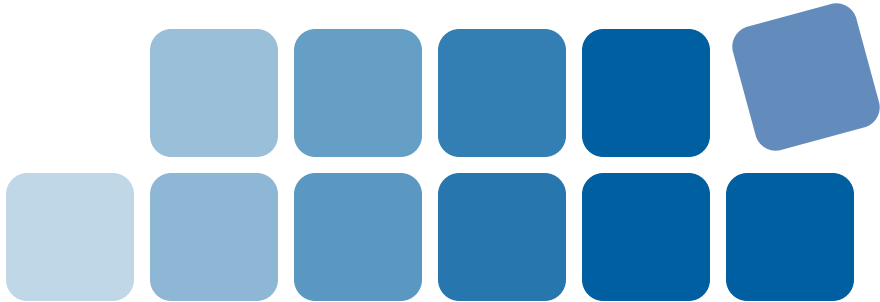
Exemples (1.2)



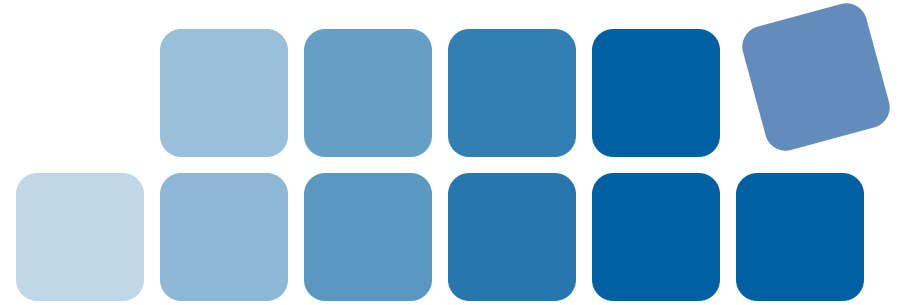
- *R. c. Singh Kainth*, (2003 CanLII 44369)

l'accusé s'adresse à un collègue de travail, Jack Castello, et lui demande de lui expliquer comment faire une recherche dans la base de données pour obtenir le nom de tous les clients qui paient par chèque. Après consultation de la banque, Castello lui dit qu'il y a vingt mille noms sous ce titre. L'accusé demande alors à Castello d'imprimer les noms et les informations qui sont contenus, à savoir les différents comptes de banque. Il faut préciser à ce point que l'accusé n'avait pas le mot de passe lui permettant d'accéder à ces informations et que c'est grâce au mot de passe de Castello qu'il peut y avoir accès.





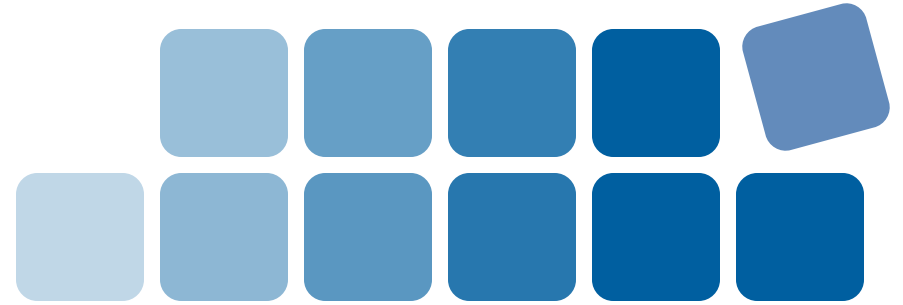
Loi sur la protection des renseignements personnels et les documents électroniques



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. **(Annexe 1, art. 4.7.3)**

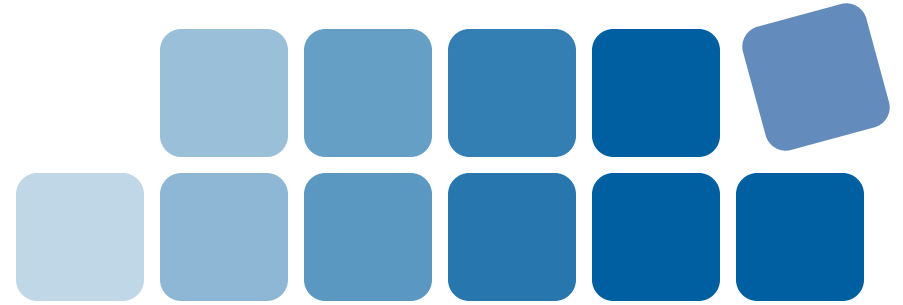
Exemples (2)



- *R. c. Lecompte*, (2004 CanLII 7889)

La Cour dans la présente affaire retient les faits suivants: toutes les transactions se sont faites sur les ordinateurs de l'accusé. C'est la victime elle-même qui a téléchargé le programme ICQ et les adresses correspondantes sur l'appareil de l'accusé. La victime, apparemment, y a laissé tous ses mots de passe et l'accusé s'est mis à recevoir des messages qui étaient destinés à madame Reid. [...] Les seules utilisations d'une des adresses électroniques de la victime que la preuve révèle sont ces quelques messages où celui-ci s'est servi de l'adresse électronique de la victime pour pouvoir communiquer avec son enfant et ceux de madame Reid. La Cour ne peut conclure, hors de tout doute raisonnable, que cette utilisation a été faite frauduleusement et sans apparence de droit.

Exemples (3)



- *Kochar c. University of Saskatchewan*, 1998 CanLII 13634
(un étudiant pirate le réseau de l'Université pour changer ses résultats aux examens)

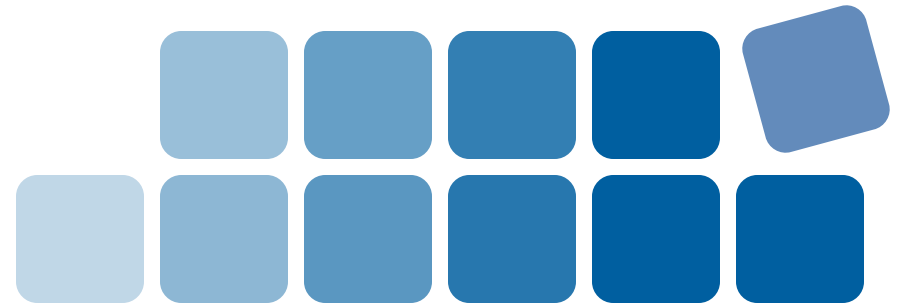
- *R. c. Plathier* (2009 QCCQ 2040)

« L'accusé était à l'emploi du *ministère de la Sécurité publique* [...] et a été congédié [...] l'accusé s'est **introduit dans le système informatique du ministère** [...] et a préparé un message ordonnant sa propre réintégration »

- *Iliescu c. Voicegenie Technologies Inc.* (2009 canlii 385)

As the litigation proceeded, affidavits of documents were exchanged. As a result of Mr. Iliescu's suspicions that VoiceGenie had not produced all of its documentation, Mr. Iliescu **surreptitiously accessed VoiceGenie's computer network and downloaded certain corporate documentation.**

Autres exemples



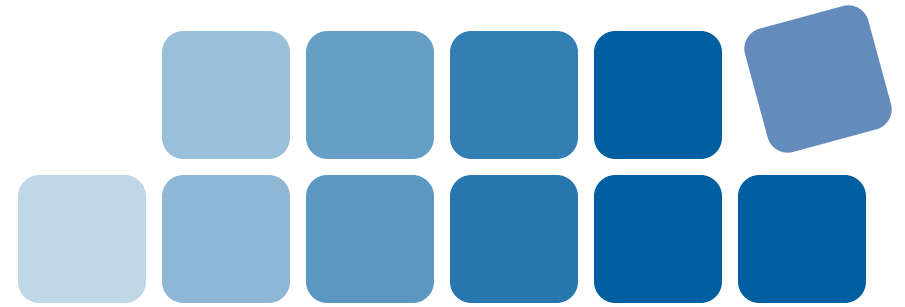
- Falsification ou clonage de cartes de débit / crédit (*R. v. Singh*, 2006 ABPC 156 ; *R. c. Rodrigue*, 2005 CanLII 22261; *R. c. Onose*, 2004 ABPC 44; *R. c. Ciocata*, 2004 ABPC 39; *R. v. Coman*, 2004 ABPC 18)
- Sites de piratage/de fabrication de bombes (*R. c. Lavoie*, 2000 CanLII 14437)
- Etc.



Responsabilité civile
et sécurité
informationnelle

NICOLAS W. VERMEYS

ÉDITIONS YVON BLAIS



Merci!

Nicolas Vermeys

Directeur adjoint

Laboratoire sur la cyberjustice

nicolas.vermeys@umontreal.ca