

Justice et sécurité informatique



Laboratoire de
CYBERJUSTICE
Laboratory



Dépôt

Des procédures, pièces, autorités



Hébergement

Du dossier de la cour



Présentation

De documents lors du procès



Archivage

Du dossier de la cour

Plan de la présentation...



Identification et authentification



Cybersécurité



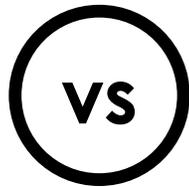
Sécurité de l'information

L'identification





IDENTIFICATION



AUTHENTIFICATION

« Opération qui consiste, pour une personne ou pour toute autre entité demandant l'accès au système informatique, à communiquer à ce dernier l'identité dont elle se réclame.

« Procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel.



IDENTIFICATION

AVEC CONTRÔLE D'ACCÈS



INFRASTRUCTURE À CLÉ
PUBLIQUE



IDENTIFICATION VIA NOM
D'UTILISATEUR /MOT DE PASSE
AVEC VÉRIFICATION PRÉALABLE

SANS CONTRÔLE D'ACCÈS



INFORMATION PERSONNELLE
ET\OU SPÉCIFIQUE



IDENTIFICATION VIA NOM
D'UTILISATEUR /MOT DE PASSE
SIMPLE



IDENTIFICATION VIA COURRIER
ÉLECTRONIQUE



INFRASTRUCTURE À CLÉ PUBLIQUE



IDENTIFICATION VIA NOM
D'UTILISATEUR /MOT DE PASSE
AVEC VÉRIFICATION
PRÉALABLE



IDENTIFICATION VIA NOM
D'UTILISATEUR /MOT DE PASSE
SIMPLE



INFORMATION PERSONNELLE
ET\OU SPÉCIFIQUE

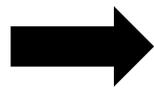


IDENTIFICATION VIA COURRIER
ÉLECTRONIQUE





AUTHENTIFIER SEULEMENT LORSQUE NÉCESSAIRE



LE NIVEAU D'AUTHENTIFICATION DOIT S'ÉVALUER
PAR RAPPORT AUX DIFFÉRENTS BESOINS DE SÉCURITÉ



AUTHENTIFIER SEULEMENT LORSQUE NÉCESSAIRE

Nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont il a la gestion.

Un organisme public peut toutefois recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune. [...]

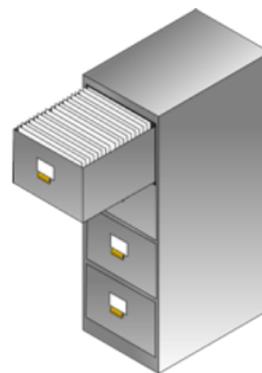
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1



LE NIVEAU D'AUTHENTIFICATION DOIT S'ÉVALUER PAR RAPPORT AUX DIFFÉRENTS BESOINS DE SÉCURITÉ

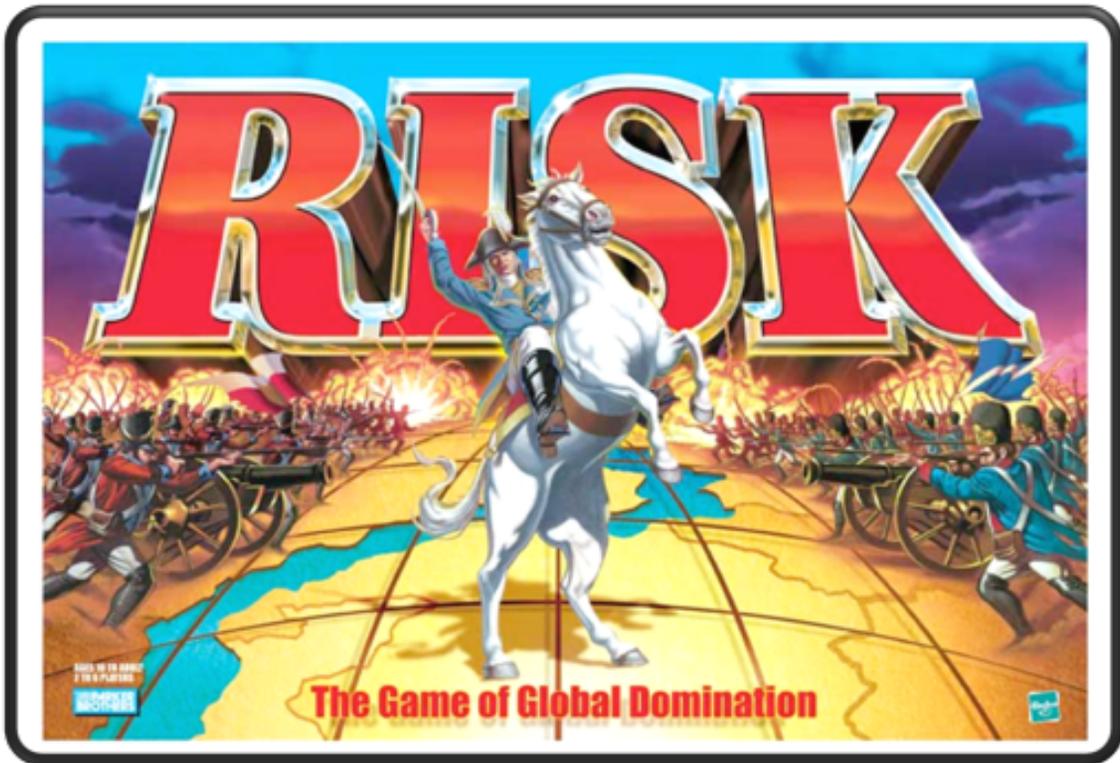


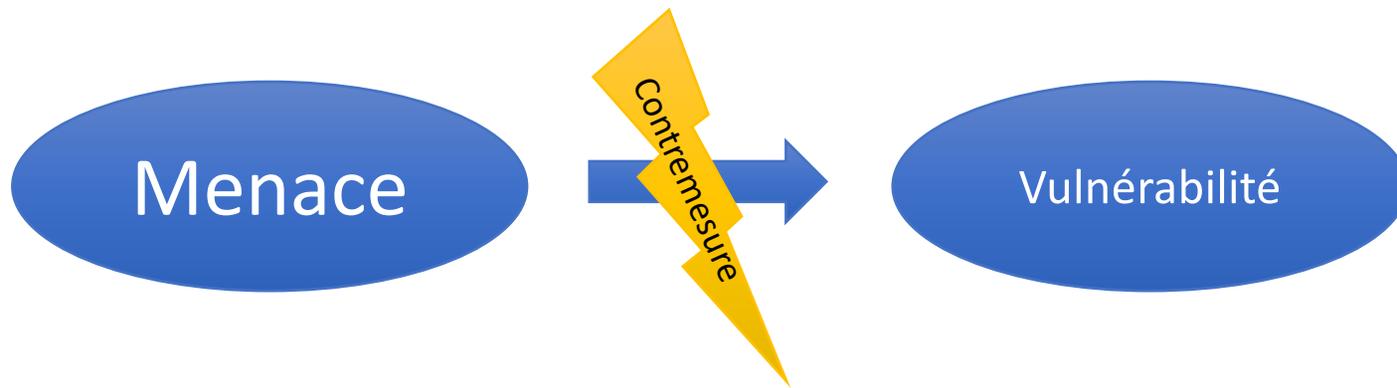
≈





La sécurité



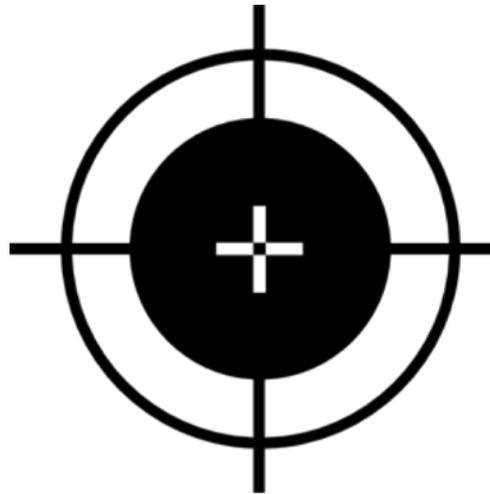




Peut être...



La menace...



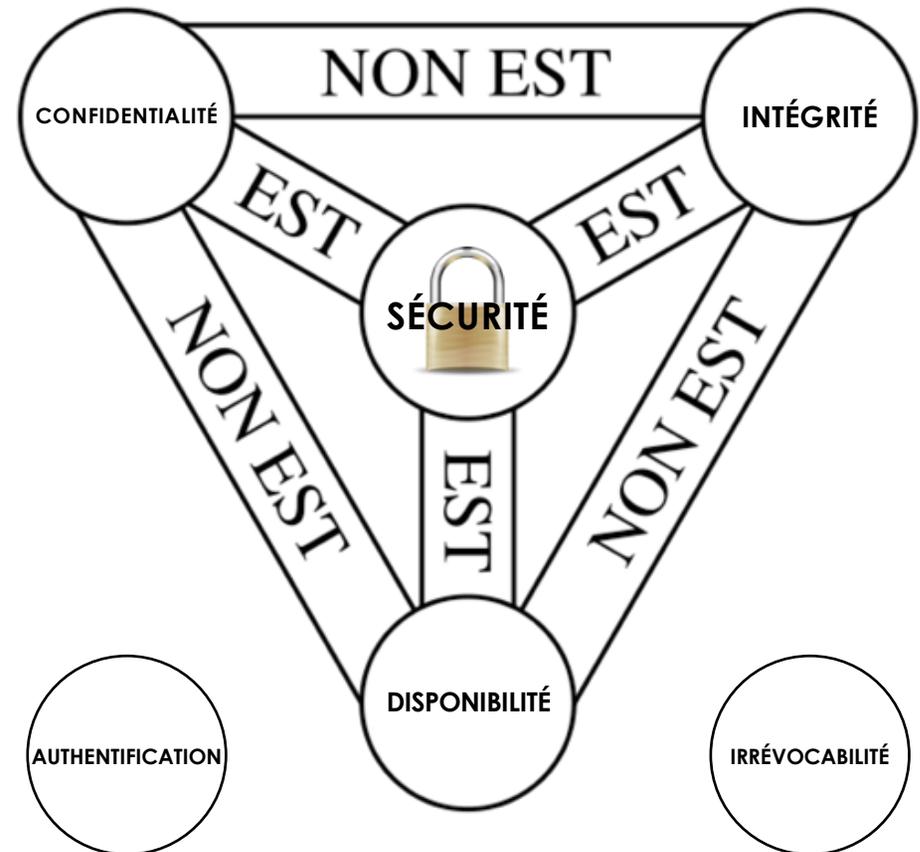
La vulnérabilité...



La contremesure

« There are really only six bad things that can happen to data. It can be disclosed, destroyed or modified, either accidentally or intentionally.

Peter S. BROWNE, "Computer Security – A Survey", (1972) 4(3) *Database* 1



26. [...]

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.

Recueil des politiques de gestion

Pour information, consultez la table téléphonique pour le numéro 11 à la page 11 0 0 1.

Document 7-2014 du 15 janvier 2014

DIRECTIVE SUR LA SÉCURITÉ DE L'INFORMATION GOUVERNEMENTALE

Loi sur la gouvernance et la gestion des ressources informatiques des organismes publics et des entreprises du gouvernement, chapitre G-1.03, s. 30

OBJET

1. La présente directive a pour objet d'assurer la sécurité de l'information qu'un organisme public diffuse dans l'exercice de ses fonctions, que la conservation de cette information, d'après appeler l'information gouvernementale, soit assurée par lui-même ou par un tiers.

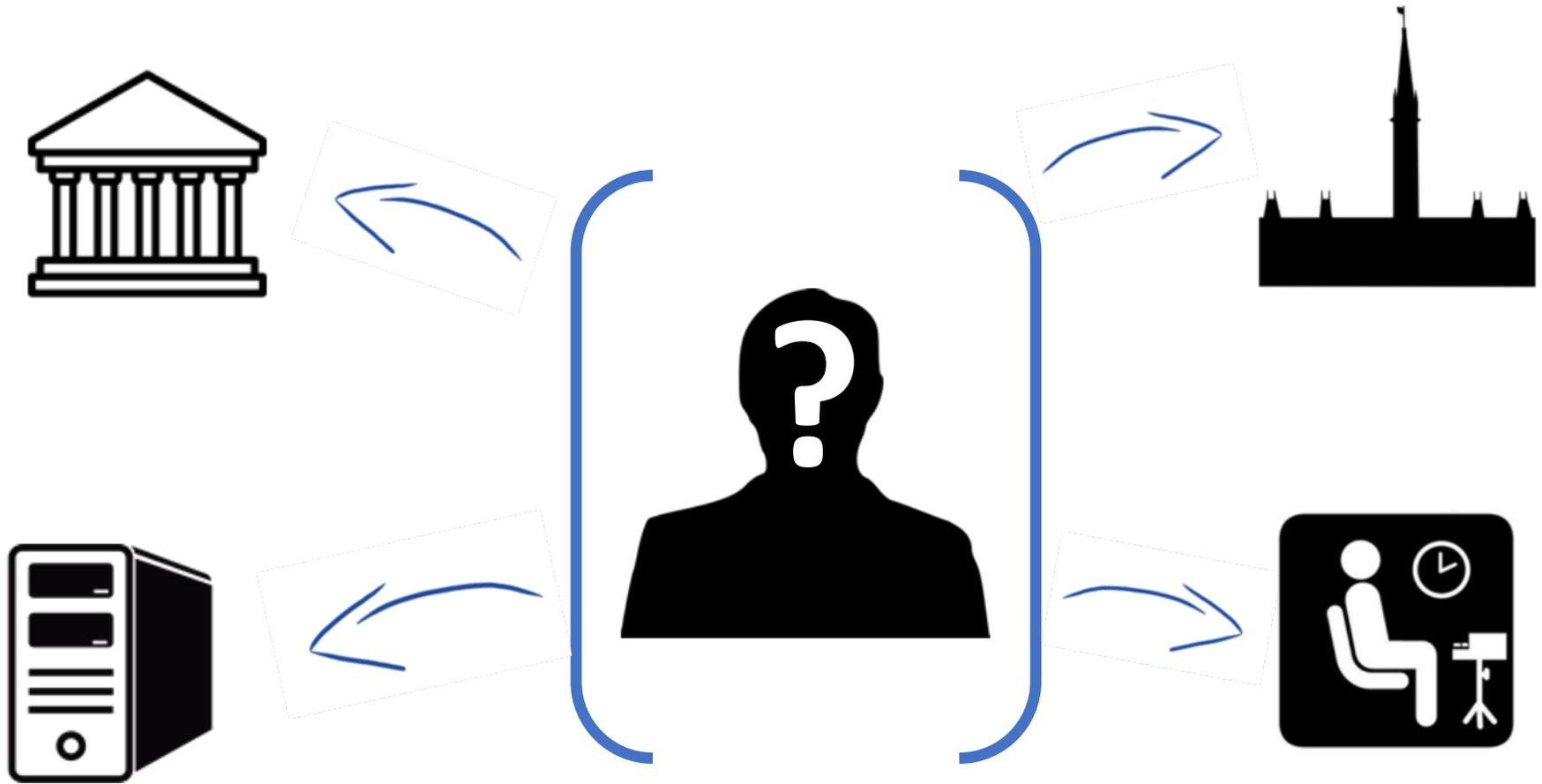
Elle fixe les objectifs à atteindre, énonce les principes directeurs devant être appliqués et décrit les obligations du dirigeant principal de l'information et des organismes publics pour assurer la sécurité de l'information gouvernementale tout au long de son cycle de vie. Elle est appuyée par un cadre gouvernemental de gestion de la sécurité de l'information, un cadre de gestion des risques et des incidents à pertes gouvernementales et une approche stratégique triennale 2014-2017 de sécurité de l'information.

CHAMP D'APPLICATION

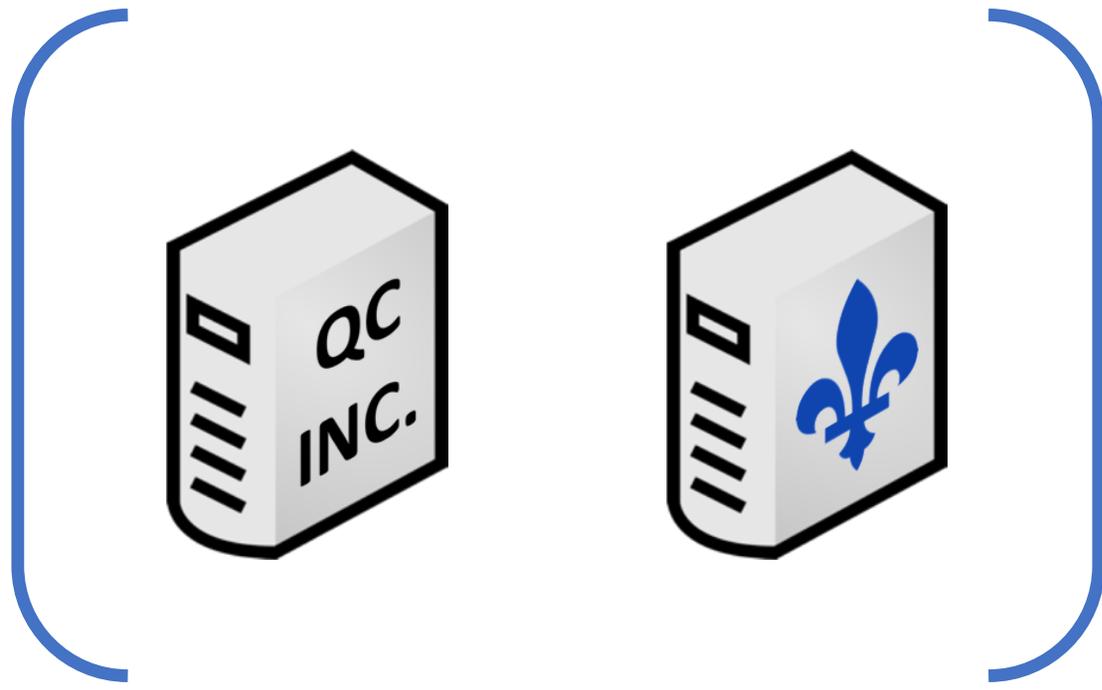
2. Cette directive s'applique aux organismes publics visés à l'article 2 de la Loi sur la gouvernance et la gestion des ressources informatiques des organismes publics et des entreprises du gouvernement (chapitre G-1.03), d'après appeler la Loi.

Les mesures de sécurité doivent être proportionnelles à la valeur de l'information gouvernementale à protéger. Elles sont établies en fonction des risques, de leur probabilité d'occurrence et de leurs conséquences. Plus particulièrement, ces mesures visent à :

- a) Assurer la **disponibilité** de l'information gouvernementale de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée.
- b) Assurer l'**intégrité** de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues.
- c) Limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte **confidentialité**.
- d) Permettre de **confirmer l'identité** d'une personne ou l'identification d'un document ou d'un dispositif.
- e) Se **prémunir contre le refus d'une personne de reconnaître** sa responsabilité à l'égard d'un document ou d'un autre objet, dont un dispositif d'identification avec lequel elle est en lien.



66. Le secrétariat des tribunaux et **la gestion de l'information et des documents** nécessaires à leur fonctionnement de même que la garde des registres, des dossiers, des ordonnances et des jugements sont **assurés par les greffes** [...]





La disponibilité

Disponibilité

- « Propriété d'une information ou d'une ressource informationnelle d'être accessible en temps voulu et de la manière requise par une personne autorisée.

GOUVERNEMENT DU QUÉBEC, « Guide relatif à la catégorisation des documents technologiques en matière de sécurité », Québec, 2003, p. 4.

Disponibilité



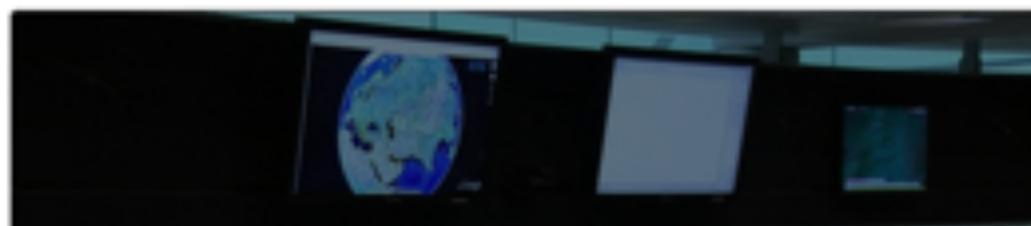
- « the stenographer tasked to record the trial had deleted primary records held on a 'memory disc' used in the stenography process before the electronic backup made to a PC was also destroyed after an unspecified malware infection
- « A convicted murderer has been granted a retrial after a stenographer's backup record of his trial was apparently destroyed by a malware infection.

Ciberataques em larga escala atingem empresas no mundo e afetam Brasil

Ataques ocorreram em ao menos 74 países, com 'vírus de resgate' que exige dinheiro, diz empresa de segurança. No Brasil, sites de empresas e órgãos públicos saíram do ar. Hospitais na Inglaterra foram atingidos no início do ataque.



Por G1
12/05/2017 11h45 - Atualizado 15/05/2017 13h23



Disponibilité... pour qui ?



11. La justice civile administrée par les tribunaux de l'ordre judiciaire est publique. **Tous peuvent** assister aux audiences des tribunaux où qu'elles se tiennent et **prendre connaissance des dossiers et des inscriptions aux registres des tribunaux** [...]

Disponibilité

19. **Toute personne doit**, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité et **voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible** et de l'utiliser aux fins auxquelles il est destiné.

23. **Tout document** auquel une personne a droit d'accès **doit être intelligible**, soit directement, soit **en faisant appel aux technologies de l'information** [...]

Le choix d'un support ou d'une technologie tient compte de la demande de la personne qui a droit d'accès au document, sauf si ce choix soulève des difficultés pratiques sérieuses, notamment en raison des coûts ou de la nécessité d'effectuer un transfert.

Disponibilité

- « failure to accommodate the public's evolving expectations of access to public process threatens the court's ability not only to secure justice, but also to satisfy the appearance of justice. The way people receive information is undergoing one of the greatest transformations in the history of information technology. In today's media climate, an open courtroom not only means letting people into the building, but letting information out as well.



Quelle
information ?

Disponibilité

Archives judiciaires :

Tout renseignement ou document recueilli, reçu, entreposé, conservé ou archivé par un tribunal en rapport avec ses instances judiciaires. Le terme comprend notamment les :

- a) dossiers judiciaires;
- b) plunitifs;
- c) procès-verbaux des audiences;
- d) calendriers des audiences;
- e) index des dossiers;
- f) registres des actions;
- g) tout document relatif aux instances judiciaires.

La définition ne comprend pas d'autres documents recueillis par les employés de la cour mais qui ne sont pas liés à une instance, notamment les registres fonciers ou concernant des permis. L'expression exclut les renseignements qui ne visent que la gestion et l'administration du tribunal, notamment les programmes de formation des juges; l'horaire des juges et des des procès ainsi que les statistiques concernant l'activité judiciaire. Elle ne vise pas non plus les notes, notes de service, ébauches et autres documents ou renseignements semblables préparés et utilisés par les juges, les fonctionnaires judiciaires et les autres employés de la cour.

Disponibilité





« commenter les activités
des tribunaux en tant
qu'aspect essentiel de
notre société
démocratique »

« pour connaître
les droits qu'ils
peuvent avoir »

« l'examen du
travail des
tribunaux »

Transparence

Société Radio-Canada c. Nouveau-Brunswick (Procureur général), [1996] 3 RCS 480, par. 26.

Edmonton Journal c. Alberta (Procureur général), [1989] 2 RCS 1326.



La confidentialité

Confidentialité

- « Propriété d'une information ou de renseignements personnels qui ne doivent pas être divulgués à des personnes ou à des entités non autorisées.

Confidentialité

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.

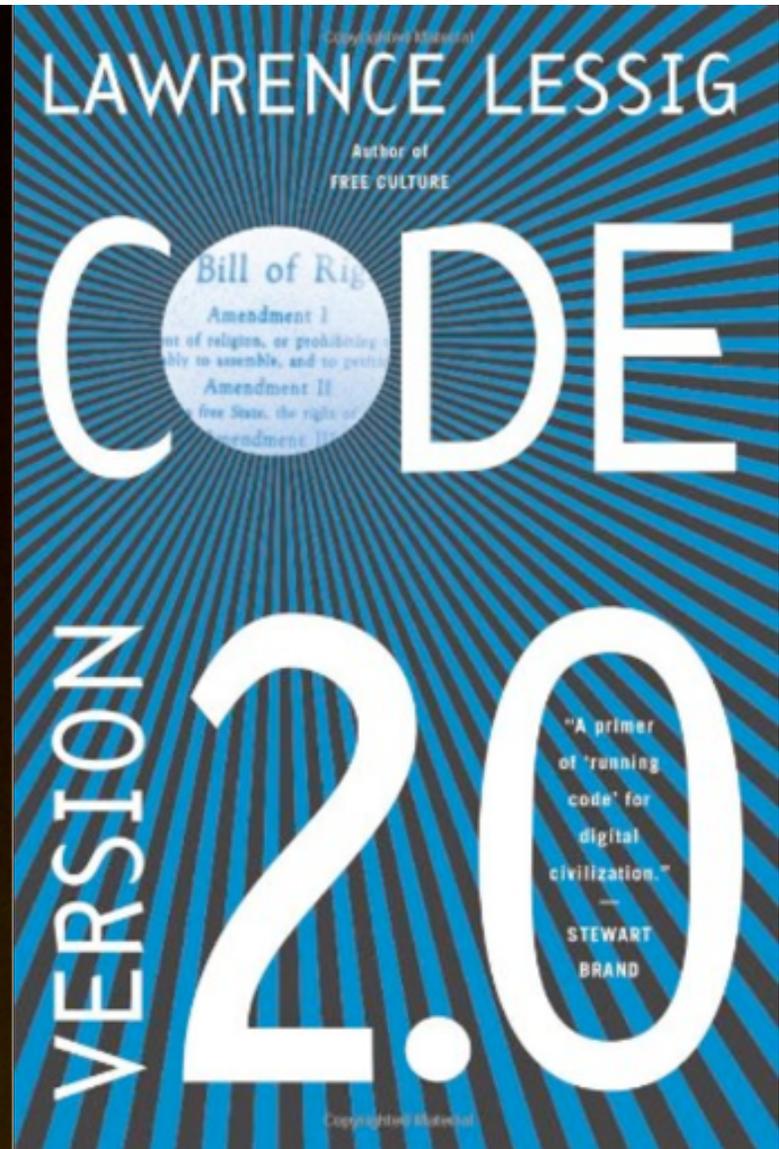
Confidentialité

11. **La justice** civile administrée par les tribunaux de l'ordre judiciaire **est publique**. Tous peuvent assister aux audiences des tribunaux où qu'elles se tiennent et prendre connaissance des dossiers et des inscriptions aux registres des tribunaux.

Confidentialité



« Dans le cas où les archives judiciaires sont en principe accessibles au public, mais où la capacité de recherche est réduite par la nécessité de repérer les dossiers dans les registres de la juridiction concernée et par le paiement de frais de recherche, **« l'opacité dans les faits » prévaut.** La transparence théorique est limitée par des barrières logistiques. Cependant, là où l'accès électronique existe, la définition de « public » s'élargira probablement.



Copyrighted Material
LAWRENCE LESSIG

Author of
FREE CULTURE

CODE

Bill of Rights
Amendment I
Congress shall make no Law
respecting an establishment
of religion, or prohibiting
the free exercise thereof;
or the right of the people
peaceably to assemble, and to
petition the Government
for redress of grievances.
Amendment II
A well regulated Militia,
being necessary to the
security of free States, the
right of the people to keep
and bear Arms, shall not
be infringed.

VERSION

2.0

"A primer
of 'running
code' for
digital
civilization."
—
STEWART
BRAND

Copyrighted Material

Confidentialité

69. [...] le gouvernement peut déterminer par règlement : [...] (2) des critères d'utilisation de fonctions de recherche extensive de renseignements personnels dans les documents technologiques qui sont rendus publics pour une fin déterminée ;

24. L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels et qui, pour une finalité particulière, est rendu public doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés. Elle peut en outre, eu égard aux critères élaborés en vertu du paragraphe 2° de l'article 69, fixer des conditions pour l'utilisation de ces fonctions de recherche.



L'intégrité



Intégrité

- « Propriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.

Intégrité

6. L'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.

L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction [...]

Intégrité

19. **Toute personne doit**, pendant la période où elle est tenue de conserver un document, **assurer le maintien de son intégrité** et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné.

Merci!

Nicolas Vermeys

Professeur agrégé - Faculté de droit

Directeur adjoint - Laboratoire de cyberjustice

Chercheur - Centre de recherche en droit public

nicolas.vermeys@umontreal.ca

Vermeys.com



**Faculté de droit
Université de Montréal**

**CENTRE DE
RECHERCHE EN
DROIT PUBLIC**



**Université 
de Montréal**



**Laboratoire de
CYBERJUSTICE
Laboratory**