ATELIER 9

Protection + renseignements confidentiels = une recette technologique parsemée d'ingrédients de saison

Me Patrick Gingras
Avocat et agent de marques de commerce, ministère de la Justice du Québec

Me Éloise Gratton
Avocate associée, McMillan LLP

Plan de la présentation

- 1) Cadre légal canadien en matière de protection et sécurité des RP
- 2) Prévention et gestion d'employés
- 3) Sécurité lors de la transmission de RP (et destruction)
- 4) Exigences légales lors de transfert de RP à des tiers (impartition et exigences contractuelles)
- 5) Bris de sécurité
- 6) Utilisation des informations obtenues par l'entremise des médias sociaux ou autres technologies de surveillance.

mcmillan 2

1) Cadre légal canadien en matière de protection et sécurité des RP

mcmillan 3

Cadre légal canadien (secteur privé)

- *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, c. 5), «LPRPDE» (fédéral) 2004
- Lois provinciales « substantiellement similaires »:
  - Québec (1994)
  - Colombie-Britannique (2003)
  - Alberta (2003)

mcmillan 4

Mesures de sécurité

- Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.
- **LPRPDE, annexe 1:**

  « 4.7.3. 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. »

mcmillan 5

Mesures de sécurité

– *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1), «LPRPSP» :

« 10. 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 concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1) :

« 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.»

et 34 LCCJTI:

mcmillan

6

Mesures de sécurité

– *Personal Information Protection Act* (S.A. 2003, c. P-6.5), «PIPA» :

«34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction. »

– *Personal Information Protection Act* (S.B.C. 2003, c. 63), «PIPA» :

« 34 An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks. »

mcmillan

7

Mesures de sécurité « raisonnables »

- Peut contrevenir à la loi même s'il n'y a pas de bris de sécurité :
  - « Section 34 of PIPA requires organizations to make reasonable security arrangements to protect personal information in their custody or control. Organizations that have not made reasonable security arrangements will be in contravention of the Act, whether or not an incident occurs. »
    - Alberta. Office of the Information and Privacy Commissioner. *Guide: PIPA Advisory #8, Implementing Reasonable Safeguards*. Calgary: the Office. P. 2 [en ligne]
- Peut ne pas contrevenir à la loi même si présence de bris de sécurité :
  - « […] Personal information security breaches may still occur, even where reasonable safeguards have been implemented. Instead, the reasonableness standard requires organizations to take into account all relevant circumstances in determining what safeguards to implement. »
    - Alberta. Office of the Information and Privacy Commissioner. *Guide: PIPA Advisory #8, Implementing Reasonable Safeguards*. Calgary: the Office. P. 2 [en ligne]
  - This standard acknowledges that reasonable "does not mean perfect."
    - British Columbia. Office of the Information and Privacy Commissioner. *Investigation Report F06-01: Sale of Provincial Government Computer Tapes containing Personal Information.* Vancouver: the Office' 2006. P. 14 [en ligne]

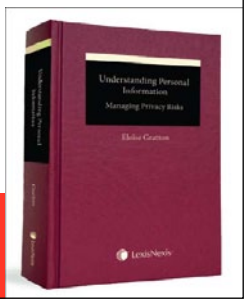
mcmillan 8

Quand un renseignement personnel est-il « sensible »?

mcmillan 9

Sensibilité du renseignement personnel

- Divulgation – le critère « identifiable » doit prendre également deux autres critères en considération :
  - La disponibilité des renseignements
  - La nature « intime » des renseignements
- Utilisation (le critère « identifiable » est moins pertinent, peut-être même désuet)
  - Critère : les renseignements seront-il utilisés contre l'individu ? Dans l'affirmative, les renseignements doivent être :
    - de qualité
    - pertinents



mcmillan

Qu'est-ce que des mesures de sécurité « raisonnables »?

mcmillan

11

Mesures de sécurité « raisonnables »

– « In determining what is "reasonable," section 2 of PIPA identifies the standard to be applied as what a reasonable person would consider appropriate in the circumstances. »
  - Alberta. Office of the Information and Privacy Commissioner. *Guide: PIPA Advisory #8, Implementing Reasonable Safeguards*. Calgary: the Office. P. 2 [en ligne]

mcmillan

12

Ottawa

Les données de 5000 Canadiens perdues par un fonctionnaire

Première publication **28 décembre 2012 à 14h45**

TVA Nouvelles

Par **Randy Richmond et Scott Taylor** | Agence QMI

Un **dispositif de stockage** contenant les **renseignements personnels** de près de 5000 Canadiens a été perdu par le ministère fédéral responsable des programmes de pensions et d'emploi.

Un employé de **Ressources humaines et Développement des compétences Canada** a égaré une clé USB qui comprenait des numéros d'assurance sociale, des dossiers médicaux et d'autres informations.

Le ministère a confirmé avoir perdu ces renseignements vendredi et a dit continuer à chercher la clé en question.

Des avocats spécialisés en vie privée sont d'avis que ce type de renseignements ne devraient jamais être extraits des bases de données principales du gouvernement.

Il y a eu, entre 2005 et 2008 en Amérique du Nord, 976 pertes ou vols de données personnelles touchant 313 millions de dossiers. Plus de la moitié de ces incidents sont attribuables à des vols de matériel informatique tels des ordinateurs portables ou à la négligence d'employés. Le piratage informatique ne constitue que 22,7 % des incidents.

Talvest perd des données sur un demi-million de clients

Une filiale montréalaise de la banque annonce avoir perdu un fichier informatique contenant des renseignements personnels sur près d'un demi-million de ses clients.

Vie privée: Des failles chez Winners et HomeSense, estiment les commissaires

Près de 600 000 citoyens touchés

Des renseignements personnels égarés par le fédéral

Agence QMI
12/01/2013 17h32

«Cet incident est inacceptable et aurait pu être évité», a indiqué la ministre Diane Finley.
Photo Reuters / Archives

OTTAWA - Un disque dur externe contenant des renseignements personnels au sujet de 583 000 personnes ayant contracté un prêt d'études canadien entre 2000 et 2006, a été perdu par le gouvernement fédéral.

Le disque dur se trouvait dans les bureaux du ministère des Ressources humaines et Développement des compétences (RHDCC) à Gatineau. C'est un employé du ministère qui a signalé la disparition de l'équipement informatique, le 5 novembre 2012.

http://www.nouvelles.umontreal.ca/recherche/sciences-sociales-psychologie/plus-de-300-millions-de-dossiers-personnels-egares.html

mcmillan

13
Document #

Mesures de sécurité « raisonnables »

- 1. Quels sont les risques?
- 2. Quelle est la probabilité (réaliste) que les risques surviennent?

Example: A Union employee exported information from the organization's member database for unauthorized purposes. Although the risk of unauthorized access by an employee had been foreseen, the Union could not have reasonably foreseen the extent and method of a data breach by a long-term employee who had legitimate access to personal information to perform his duties. The Union had appropriate policies and confidentiality agreements in place which the employee had understood, acknowledged, and then ignored. The Union was found to have implemented reasonable technical and administrative safeguards, despite the fact a breach occurred (OIPC Investigation Report #P2006-IR-004).

mcmillan 14

Mesures de sécurité « raisonnables »

- 3. Les dommages potentiels sont-il importants?
  - « The seriousness of harm may be very low if the personal information that is compromised is not very sensitive, or if only a few individuals are affected. Harm may be very serious if the personal information is sensitive medical or financial information that can be used to commit fraud or identity theft. Organizations should also consider that they may be harmed by a personal information security breach through negative publicity, loss of customer business, or the time and money required to respond to a breach. »
- 4. Quels sont les coûts pour l'implantation d'un système de sécurité?

mcmillan 15

Mesures de sécurité « raisonnables »

- 5. Quels sont les standards dans l'industrie?
  - «(…) Be aware, however, that compliance with established practice will not necessarily be deemed to be reasonable. Influencing factors include:
    - the longevity of the practice,
    - its universality,
    - the status and reputation of those who have implemented the standard (e.g. professionals, the type of industry),
    - the technical difficulty of implementing the safeguard (safeguards that are complex, scientific or highly technical may not be reasonable), and
    - whether the organization relied only on established practice without considering other precautions that may have been available.»

Example: An organization's laptop computer with personal information of approximately 8,000 individuals was stolen from a vehicle. The organization relied on its employee to follow policies and not leave the laptop unattended in the vehicle. Information on the laptop was protected only by a log-on password. These safeguards were found to be insufficient. Instead, a combination of administrative, physical and technical safeguards - including encryption, which can be relatively inexpensive and has become a computing standard - would have been reasonable in the circumstances (OIPC Investigation Report #P2006-IR-005).

16

Mesures de sécurité raisonnables

- S'assurer que les endroits d'entreposage soient sécurisés (verrouillés et accès limité)
  - Ex: Garder des documents contenant des RP dans une classeur non verrouillé est contraire aux dispositions de la loi en matière de sécurité. (*Stacey c. Sauvé Plymouth Chrysler (1991) inc.* (C.Q., 2002-05-14), SOQUIJ AZ-50129243, J.E. 2002-1147, [2002] R.R.A. 654, [2002] R.J.Q. 1779.)

Example: Cell phone contracts containing customer personal information were recovered in a police investigation. The cell phone service dealer reported several previous incidents of staff theft. An OIPC investigation found that employee access to sensitive customer data was not restricted within the organization. Further, records containing personal information were stored in the accounting office and inventory storage areas, accessible to all of the organization's staff (OIPC Investigation Report #P2005-IR-003).

- Attention aux déménagements

Example: A collection agency's debt collection account records were found by police in the possession of unauthorized individuals. The agency had recently moved to new premises and a number of gaps in the organization's security measures were exploited, resulting in a breach. Records containing personal information were left behind and not secured, and were at times accessible to unsupervised third parties; shredding bins were not secured, the premises alarm system was not always activated (OIPC Investigation Report #P2005-IR-002).

mcmillan

17

Un exemple…

« Au cours de la période allant du 26 octobre au 8 novembre 2007, a fait défaut d'agir avec professionnalisme et a **fait preuve de négligence en hébergeant, sur le site Web du cabinet Assurances Kotliaroff & Associés, les liens informatiques, codes d'utilisateur et mots de passe** […], **alors que l'accès à ceux-ci n'était pas protégé, permettant ainsi, notamment à tout visiteur, aux employés du cabinet et à lui-même, d'y avoir accès**, sans le consentement de Promutuel Deux-Montagnes, société mutuelle d'assurance générale, et d'avoir accès à des renseignements personnels de plus de 12 000 clients de Promutuel Deux-Montagnes […]; »

(*Chambre de l'assurance de dommages* c. *Kotliaroff* (C.D.C.H.A.D., 2008-04-16 (culpabilité) et 2008-04-16 (sanction)), SOQUIJ AZ-50488063)

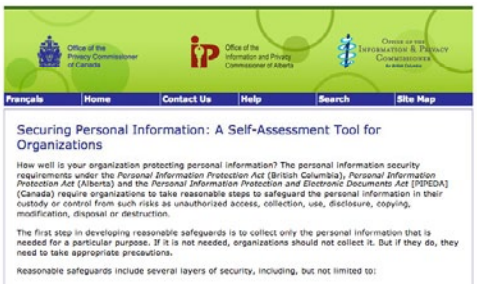
mcmillan 18

2) Prévention et gestion d'employés

mcmillan 19

Évaluer les risques

- « Privacy Impact Assessment »
  - Identifier les besoins et les risques et développer un programme en utilisant le modèle d'évolution des pratiques en matière de PRP de l'AICPA- ICCA et les lois applicables aux activités et à l'entreprise



20

Adoption de politiques

- Adoption de politiques en matière de protection de renseignements personnels et en matière de sécurité (rétention, destruction), communication des politiques aux employés et partenaires et mises à jour.

- En dehors des lieux du travail :
  - «It may be necessary for an organization to develop policies that specifically address the security of personal information outside the workplace - whether stored in paper files, or on laptops or other devices such as PDAs. »

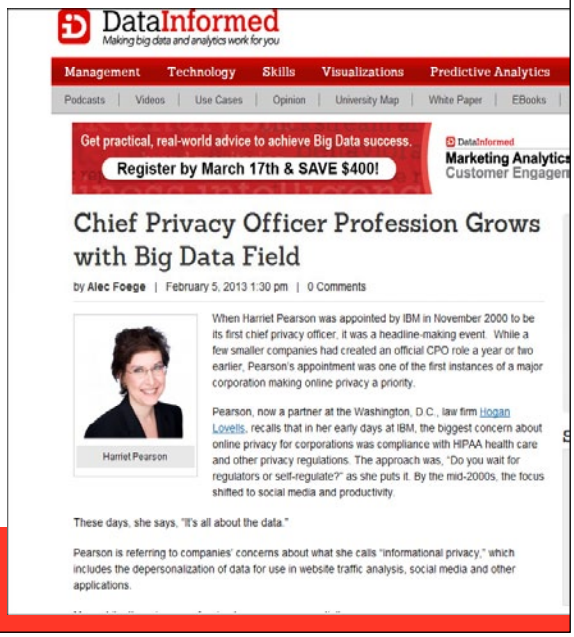
Example: A laptop computer was stolen from the home of an employee of a health region. Although the laptop had a locking cable to secure it to a desk or table, this mechanism was not in force. The laptop had more health information than was required stored on its hard drive. The health information was not encrypted (OIPC Investigation Report #H2006-IR-002).

  - Information & Privacy Commissioner for British Columbia. *Protecting Personal Information Outside the Office,* February 2005.

mcmillan

Nommer un chef de la protection de RP

- Nommer une personne en charge des questions de protection de RP
  - Obligation légale à venir : Québec. Commission d'accès à l'information. *Technologies et vie privée à l'heure des choix de société.* Rapport quinquennal 2011. Québec: la Commission, 2011. 112 p. [en ligne], propose aussi des amendements aux lois québécoises allant dans ce sens


DataInformed
Making big data and analytics work for you

Management | Technology | Skills | Visualizations | Predictive Analytics

Podcasts | Videos | Use Cases | Opinion | University Map | White Paper | EBooks

Get practical, real-world advice to achieve Big Data success.
Register by March 17th & SAVE $400!

DataInformed Marketing Analytics Customer Engagem

Chief Privacy Officer Profession Grows with Big Data Field

by Alec Foege | February 5, 2013 1:30 pm | 0 Comments

Harriet Pearson

When Harriet Pearson was appointed by IBM in November 2000 to be its first chief privacy officer, it was a headline-making event. While a few smaller companies had created an official CPO role a year or two earlier, Pearson's appointment was one of the first instances of a major corporation making online privacy a priority.

Pearson, now a partner at the Washington, D.C., law firm Hogan Lovells, recalls that in her early days at IBM, the biggest concern about online privacy for corporations was compliance with HIPAA health care and other privacy regulations. The approach was, "Do you wait for regulators or self-regulate?" as she puts it. By the mid-2000s, the focus shifted to social media and productivity.

These days, she says, "It's all about the data."

Pearson is referring to companies' concerns about what she calls "informational privacy," which includes the depersonalization of data for use in website traffic analysis, social media and other applications.

mcmillan

Formation des employés

- Sensibiliser le personnel qui gère des RP (RH, marketing, TI, médias sociaux, gestion documentaire, etc.) aux questions de sécurité des RP :
  - Environ 80 décisions du CVPC mentionnent l'importance de former les employés qui vont gérer des RP dans le cadre de leurs fonctions;
  - « Provide information privacy and security education and training for staff at the time of hire, and regularly throughout the duration of employment »;
  - Les entreprises doivent effectuer des formations d'employés sur quand et comment ils peuvent communiquer des documents concernant des RP à des tiers afin de se conformer aux obligations de sécurité de la loi.
    - *Centre financier aux entreprises Desjardins Grandes-Seigneuries--Vallée-des-Tisserands et Syndicat des employées et employés professionnels et de bureau, section locale 575 (Pierre Laflèche)* , T.A., 2008-06-16), SOQUIJ AZ-50507770, D.T.E. 2008T-715, [2008] R.J.D.T. 1349

mcmillan

3) Sécurité lors de la transmission de RP

mcmillan

24

Loi concernant le cadre juridique des technologies de l'information (RLRQ, c. C-1.1)

34. Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication.

La documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuve, le cas échéant.

mcmillan

25

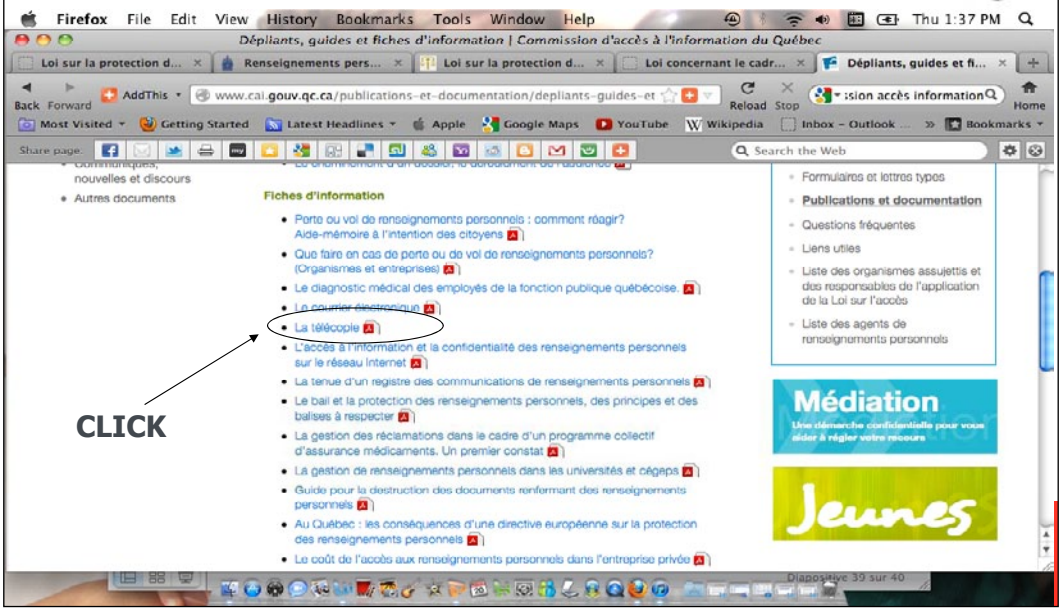
Mesures de sécurité lors du transfert (télécopie)

- Mesures jugées inacceptables par le CVPC (suite) :
  - Envoyer un document contenant des RP à une personne **sans vérifier l'identité du receveur** (CVPC Résumé #2007-374);
  - Envoyer un document contenant des RP à la **mauvaise personne** (CVPC Résumé #2006-332);
  - Envoyer un document contenant des RP (incluant le NAS d'un employé) sur la **page couverture d'un fax** (CVPC Résumé #2005-317).

mcmillan

26

Mesures de sécurité lors du transfert (télécopie)



Mesures de sécurité lors du transfert (télécopie)

- **Le télécopieur ou l'ordinateur doit :**
  - être installé dans un endroit surveillé qui n'est pas accessible au public
  - être utilisé seulement par les personnes autorisées
- **En tout temps, l'utilisateur doit :**
  - vérifier (avant transmission) si les RP qu'il contient peuvent en être extraits
  - remplir un formulaire d'accompagnement indiquant le nom, l'adresse et le numéro de téléphone du destinataire et le numéro de téléphone de l'expéditeur
  - s'assurer, après avoir composé le numéro du télécopieur du destinataire, qu'il n'y a pas d'erreur de composition
  - vérifier le rapport de transmission et communiquer avec le destinataire pour s'assurer qu'il a bien reçu les documents

mcmillan 28

Mesures de sécurité lors du transfert (télécopie) - suite

- **Lors de la transmission de RP par télécopieur, l'individu doit :**
  - vérifier l'urgence de communiquer des renseignements personnels
  - indiquer visiblement leur caractère confidentiel
  - informer le destinataire de l'heure de la transmission et s'assurer de sa présence au moment de la réception
  - obtenir confirmation de la personne autorisée à recevoir les renseignements

mcmillan 29

Transmission de RP par télécopie

– Alberta. Office of the Information and Privacy Commissioner. *Guidelines on Facsimile Transmission*. Vancouver: the Office [en ligne]

> ***Example:*** A collection agency faxed a Verification of Employment (VOE) form to a debtor's place of employment. The fax was received on a non-confidential fax machine, and was collected by an unauthorized individual instead of the intended recipient. The organization did not have adequate policies or procedures in place to mitigate risks associated with faxing personal information (OIPC Investigation Report #P2006-IR-003).

– British Columbia. Office of the Information and Privacy Commissioner. *Faxing and Emailing Personal Information*. Vancouver: the Office, February 2005 [en ligne]

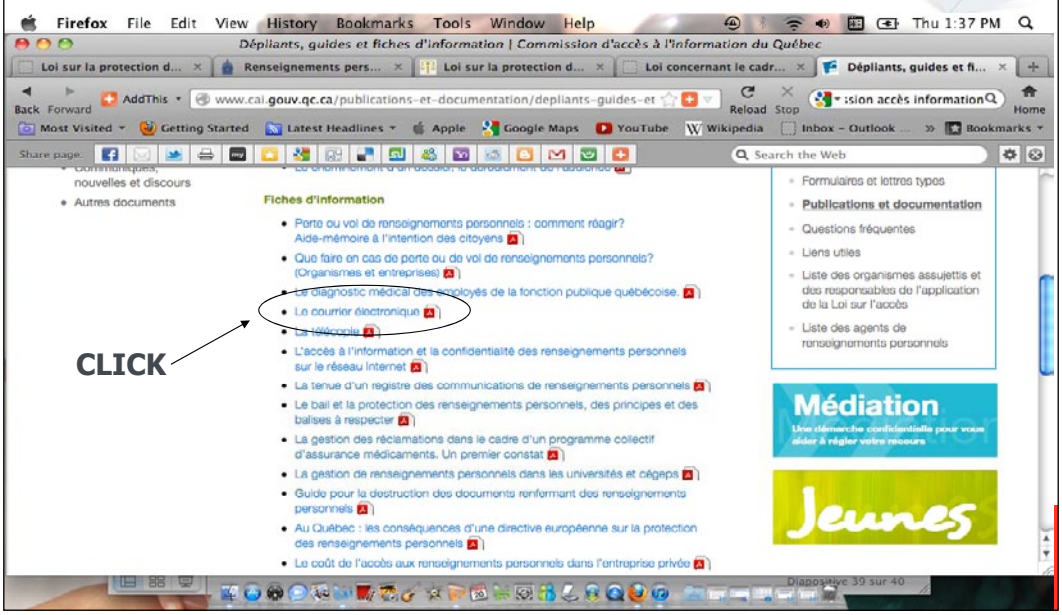
mcmillan 30

Mesures de sécurité lors du transfert (courriel)

– Les entreprises ne doivent pas utiliser un ordinateur dans un endroit accessible au public permettant à n'importe qui d'accéder à des renseignements sensibles sans mots de passe.
  – CVPC Résumé #2003-177, *Bank leaves computer logged on in public area; customer obtains sensitive personal account information without password*, 5 juin 2003.
– En cas de bris de sécurité (relatif à des RP sensibles, numéro de permis de conduire et informations financières) que le fait que RP n'étaient pas encryptés d'être une cause de responsabilité.
  – CVPC Résumé #2008-395, *Commissioner initiates safeguards complaint against CIBC*, janvier 2008;
  – Voir aussi Report of Findings – TJX Companies Inc. / Winners Merchant International L.P., 25 septembre 2007.

mcmillan 31

Mesures de sécurité lors du transfert (courriel)



Mesures de sécurité lors du transfert (courriel)

Le courrier électronique offre à peu près le même degré de confidentialité qu'une carte postale.

- **Les mesures de protection :**
  - Appliquer les correctifs proposés par les fournisseurs de logiciels
  - Utiliser un antivirus à jour
  - Utiliser un logiciel de chiffrement
  - Gérer le mot de passe
- **Conservation et destruction des messages**
  - L'administrateur d'un système de courrier électronique doit fixer des délais de conservation des messages.

mcmillan

33

Mesures de sécurité lors du transfert (courriel)

- **Politique d'utilisation du courrier électronique en entreprise :**
  - Les règles de gestion et d'utilisation du courrier électronique dans l'entreprise doivent être claires et connues de tous les usagers (qui peut avoir accès aux boîtes postales et dans quelles circonstances cet accès est autorisé).
  - « En milieu de travail, il est raisonnable de s'attendre que l'employeur contrôle l'utilisation des moyens de communication qui lui appartiennent. Toutefois, l'employé a droit au respect de sa vie privée dans l'exercice de ce contrôle. Les employés doivent ainsi être informés des motifs de contrôle et des mécanismes de contrôle dont ils peuvent être l'objet. Ils doivent être clairement informés de leurs obligations et de leurs droits. »

mcmillan 34

Mesures de sécurité lors du transfert (courriel)

- **Des précautions élémentaires:**
  - À chaque boîte postale devrait correspondre un mot de passe connu seulement de l'employé autorisé à y accéder et géré par lui.
  - (…) Le système informatique devrait exiger que l'usager modifie son mot de passe régulièrement, disons chaque mois, et rejeter les mots de passe utilisés antérieurement.
  - Aucune donnée personnelle ne doit être expédiée, à moins d'être chiffrée.

Mots de passe : « Require staff to use strong passwords (e.g. a minimum of 8 characters, use of both upper and lower case letters, numbers and symbols (…).»

mcmillan 35

Mesures de sécurité lors du transfert (courrier)

- Mesures de sécurité inacceptables :
  - La perte de RP de clients lorsque ces derniers étaient contenus dans des documents envoyés par la poste (**entre deux endroits**)
    - CVPC Résumé #2001-11, *Bank loses customer's personal information*, 7 septembre 2001.
  - Défaut de **bien cacheter une enveloppe** qui contient de RP avant de la mettre à la poste
    - CVPC Résumés #2003-154 et #2003-197.
- Mesures de sécurité acceptables :
  - Livrer un document contenant des RP à un destinataire dans un **enveloppe cachetée** qui garde les documents sur le bureau de la réceptionniste (non accessibles à n'importe qui).
    - CVPC Résumé #2003-237, *Individual accuses employer of disclosing personal information to co-workers*, 20 novembre 2003.

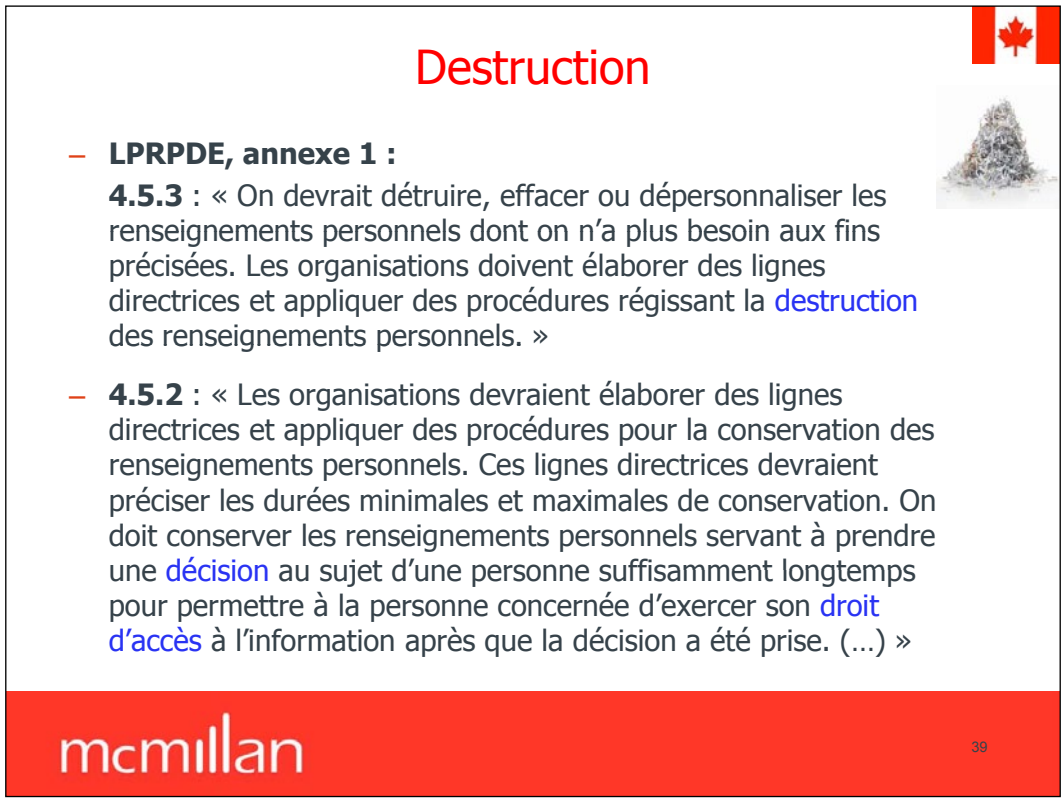
mcmillan 36

Mesures de sécurité lors du transfert (courrier)

- « Implement standards for shipping personal information outside of the workplace e.g. require that files be transported in a sealed envelope marked "confidential"; use only trustworthy, bondable courier companies; document the shipment (date, time, contents, name of courier company), confirm receipt. »

mcmillan 37


Barreau du Québec
ACCUEIL
Guide des TI
Gestion et sécurité des technologies de l'information pour l'avocat et son équipe
Chiffrement
Dernière mise à jour : 8 novembre 2011
23 questions pour évaluer votre utilisation des TI
Introduction
SECTION 1 - Sécurité des communications
SECTION 2 - Protection de l'accès aux données
Mot de passe
Chiffrement
Gestion du départ d'un employé
Entente avec les fournisseurs
Sécurisation des bureaux, des salles et des équipements
Mise au rebut ou recyclage du matériel informatique
SECTION 3 - Gestion des documents électroniques
Lexique
Réalisation du Guide
Dans cette page :
1. Pourquoi le chiffrement?
2. Qu'est-ce que le chiffrement?
Pourquoi le chiffrement?
L'homme a toujours ressenti le besoin de dissimuler de l'information, et ce, bien avant l'apparition des premiers ordinateurs et des machines à calculer.
Depuis sa création, le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication. Cependant, cette communication met de plus en plus en jeu des problèmes stratégiques liés à l'activité des entreprises sur le Web. Les transactions effectuées à travers le réseau peuvent être interceptées. C'est le chiffrement qui se charge de garantir la sécurité de cette information.
Qu'est-ce que le chiffrement?
Le mot chiffrement est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre incompréhensibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffrer.
Les données enregistrées sur des supports amovibles, tels une clé USB, un disque dur externe ou un iPod peuvent être interceptées (trouvées ou volées) et devraient par conséquent être chiffrées. De plus, les messages transmis par courrier électronique et les données enregistrées sur les téléphones intelligents devraient également faire l'objet de chiffrement.
Dans certaines circonstances, le chiffrement permet non seulement de préserver la confidentialité des données mais aussi d'en garantir l'intégrité et l'authenticité.
Vous avez une question ou vous désirez nous faire part d'un commentaire ou d'une suggestion? C'est par ici!


Destruction
– LPRPDE, annexe 1 :
4.5.3 : « On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels. »
– 4.5.2 : « Les organisations devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels. Ces lignes directrices devraient préciser les durées minimales et maximales de conservation. On doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne concernée d'exercer son droit d'accès à l'information après que la décision a été prise. (…) »
mcmillan
39

Destruction

- CVPC : les entreprises qui n'ont pas établi de période de rétention et n'ont pas adopté de politiques en matière de destruction de RP en place agissent en contravention aux principes 4.5.2 et 4.5.3 de LPRPDE.
  - CVPC Résumé #2009-008, *Report of Findings : CIPPIC v. Facebook Inc.* – July 16, 2009.
  - CVPC Résumé #2002-52, *Company accused of failing to safeguard information of online contest entrants*, June 13, 2002.

mcmillan 40

Destruction

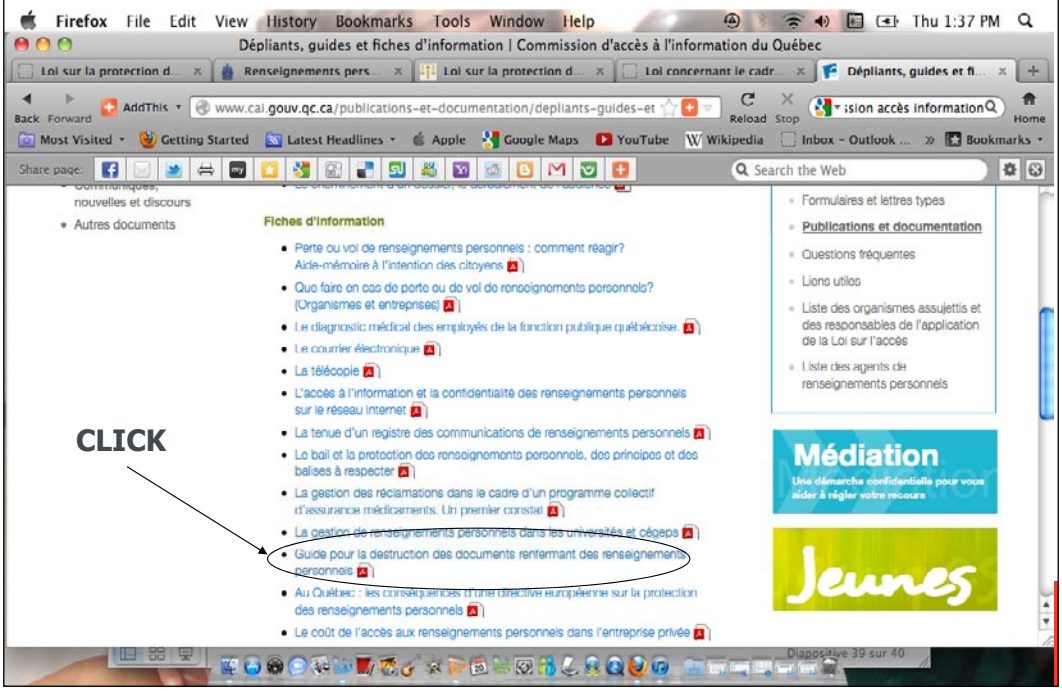
- LRPRDE, annexe 1 :

  4.7.5 « Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3). »

- CVPC a pris la position qu'une entreprise qui a laissé un document contenant les informations bancaires de l'un de ses employés dans un bac de recyclage est en défaut de cette obligation de protection. (CVPC Résumé #2006-356, *Customer's banking personal information found in a recycling bin*, October 23, 2006.)

mcmillan 41

Destruction



Destruction

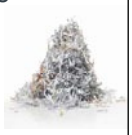
- Au sein de l'organisme ou de l'entreprise, il est important que chaque employé, à son poste de travail, se sente responsable d'assurer la protection des renseignements personnels qu'il traite. C'est ainsi qu'il ne doit pas jeter au rebut les documents, disquettes, cartouches ou rubans magnétiques qui en contiennent sans s'être assuré au préalable que leur contenu ne peut être reconstitué.
- Le déchiquetage demeure la meilleure méthode de destruction des documents confidentiels.
- Si les spécifications techniques de la déchiqueteuse de l'entreprise ne répondent pas au volume des documents à détruire, il faut les entreposer dans un endroit fermé à clé avant de les confier à une entreprise spécialisée de récupération de papier.

mcmillan

43

Destruction

- Contrat écrit est nécessaire en cas de sous-traitance de la destruction des documents contenant des RP, lequel devrait contenir, au minimum, les éléments suivants :
  - le procédé utilisé pour la destruction des documents;
  - la nécessité d'un accord préalable entre les parties avant de confier la destruction des documents confidentiels à un autre sous-contractant;
  - les pénalités aux dépens de l'entreprise de récupération si elle ne respecte pas ses engagements;
  - l'entreprise de récupération devrait :
    - reconnaître que les documents sont de nature confidentielle;
    - faire signer un engagement à la confidentialité à toute personne qui aura à manipuler ces documents; (…)
    - faire rapport au client lors de la destruction des documents reçus.



mcmillan 44

Destruction

- Contenu des appareils (incluant disques durs, disquettes, CDs, etc.) effacés si en réparation ou recyclés – si pas possible, destruction.

Example: Staff of a beauty supply organization disposed of customer personal information in a dumpster. The organization did not provide adequate direction regarding the confidential and secure disposal of records, and staff only tore the records by hand instead of shredding them (OIPC Investigation Report #P2006-IR-003).

Example: A retail office supply store re-sold a computer that had been returned to the store. The new owner found personal information of the previous owner on the computer's hard drive. The organization contravened PIPA by failing to thoroughly eradicate the previous owner's personal information from the hard drive before reselling the computer (OIPC Investigation Report #P2006-IR-001).

mcmillan 45

4) Exigences légales lors de transfert de RP à des tiers (impartition et exigences contractuelles)

mcmillan

46

Restrictions - Impartition

– **LPRPDE, annexe 1 :**

«4.1.3 Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie. »

– **LPRPSP** :

« **20**. Dans l'exploitation d'une entreprise, un renseignement personnel n'est accessible, sans le consentement de la personne concernée, à tout préposé, mandataire ou agent de l'exploitant ou à toute partie à un contrat de service ou d'entreprise qui a qualité pour le connaître qu'à la condition que ce renseignement soit nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat ou de son contrat.»

mcmillan

47

Restrictions - Impartition

- **PIPA :**

  « 5 (2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act. »

- **PIPA :**

  « 4 (2) An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization. »

mcmillan 48

Transfert de renseignements « nécessaires »

- Au niveau de la *collecte* :
  - « 5. La personne qui recueille des renseignements personnels afin de constituer un dossier sur autrui ou d'y consigner de tels renseignements ne doit recueillir que les renseignements nécessaires à l'objet du dossier. […] »
- Au niveau du *transfert* :
  - « 13. Nul ne peut communiquer à un tiers les renseignements personnels contenus dans un dossier qu'il détient sur autrui ni les utiliser à des fins non pertinentes à l'objet du dossier, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie. »
  - « 20. Dans l'exploitation d'une entreprise, un renseignement personnel n'est accessible, sans le consentement de la personne concernée, à tout préposé, mandataire ou agent de l'exploitant ou à toute partie à un contrat de service ou d'entreprise qui a qualité pour le connaître qu'à la condition que ce renseignement soit nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat ou de son contrat.»

mcmillan 49

Impartition: nécessité d'un contrat

- *X c. La Métropolitaine* (C.A.I., 1995-03-31), SOQUIJ AZ-95151504, A.I.E. 95AC-46, [1995] C.A.I. 364 (rés.). La CAI prend la position que La Métropolitaine ne peut pas mettre le fardeau de protection sur son mandataire (Equifax Canada) et qu'une entente aurait dû être signée par mesure de sécurité.

- *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. […] »

mcmillan 50

Responsable du traitement *vs* Sous-traitant

Commission européenne. Direction général sur la Justice. Groupe de Travail « Article 29 » sur la Protection des Données, *Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant»*, Adopté le 16 février 2010 [en ligne]

- Responsable du traitement : « En effet, un organisme qui n'exerce ni influence de droit ni influence de fait pour déterminer la manière dont les données à caractère personnel seront traitées ne saurait être considéré comme un responsable du traitement. »

- Sous-traitant : « Par conséquent, les deux conditions fondamentales pour agir en qualité de sous-traitant sont, d'une part, d'être une entité juridique distincte du responsable du traitement et, d'autre part, de traiter les données à caractère personnel pour le compte de ce dernier. »

mcmillan 51

5) Bris de sécurité

mcmillan

52

Obligation de notifier en cas de bris de sécurité

- Obligations légales :
  - Alberta PIPA, en cas de « real risk of significant harm to an individual »
  - À venir :
    - Fédéral : La *Loi protégeant les renseignements personnels des Canadiens*, Projet de loi C-12, 41e législature, 1re session, 2011, et la *Loi modifiant la Loi sur la protection des renseignements personnels et documents électroniques (pouvoir de rendre des* ordonnances), Projet le loi C-475, 41e législature, 1re session, 2013, proposent des amendements à la LPRPDE
    - Québec. Commission d'accès à l'information. *Technologies et vie privée à l'heure des choix de société.* Rapport quinquennal 2011. Québec: la Commission, 2011. 112 p. [en ligne] propose aussi des amendements aux lois québécoises allant dans ce sens

mcmillan

53

Obligation de notifier en cas de bris de sécurité

– Québec. Commission d'accès à l'information. *Technologies et vie privée à l'heure des choix de société.* Rapport quinquennal 2011. Québec: la Commission, 2011. P. 77 [en ligne]:

Recommandation 7 : La Commission recommande que la *Loi sur l'accès* et la *Loi sur la protection dans le secteur privé* soient modifiées par l'ajout d'une obligation de lui déclarer les failles de sécurité qui surviennent dans les organismes publics et les entreprises et qui impliquent des renseignements personnels.

Recommandation 8 : La Commission recommande que soient déterminées les conditions et les modalités conduisant à déclarer des failles de sécurité impliquant des renseignements personnels.

Recommandation 9 : La Commission recommande que lui soit confié le pouvoir d'ordonner aux organismes publics et aux entreprises d'aviser, aux conditions qu'elle déterminera, les personnes concernées d'une faille de sécurité impliquant leurs renseignements personnels et de prendre les mesures qu'elle jugera nécessaires pour assurer une protection adéquate de leurs renseignements personnels.

mcmillan

Alberta : obligation légale

Notification of loss or unauthorized access or disclosure

PIPA :

– «**34.1(1)** An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.
– **(2)** A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.»

mcmillan

55

Obligation de notifier en cas de bris de sécurité

- Entre-temps, chaque juridiction a adopté un guide:

- **Fédéral :** Commissariat à la protection de la vie privée du Canada. *Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée* [en ligne]

- **Colombie-Britannique :** Office of the Information and Privacy Commissioner for British Columbia, *Key Steps for Organizations in Responding to Privacy Breaches* (June 2008).

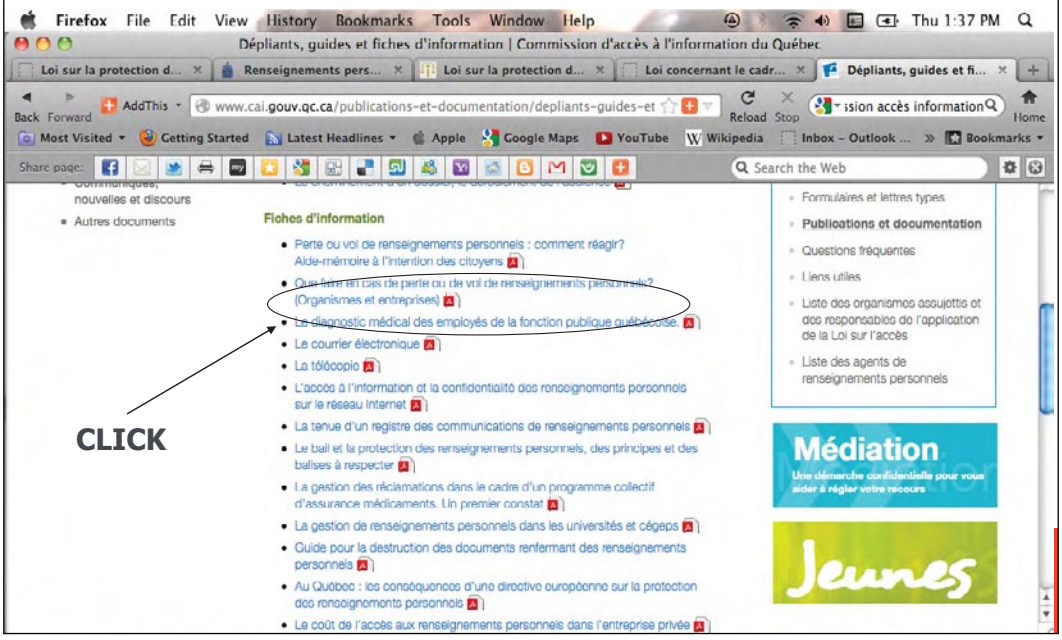
- **Alberta :** Office of the Information and Privacy Commissioner, Alberta, *Key Steps in Responding to Privacy Breaches* (2007).

- **Québec :** Commission d'accès à l'information du Québec. *Que faire en cas de perte ou de vol de renseignements personnels?* (2009) [en ligne]

mcmillan

56

Obligation de notifier en cas de bris de sécurité



Principales étapes à suivre lors d'une perte ou d'un vol de RP

ÉTAPE 1 : ÉVALUATION PRÉLIMINAIRE DE LA SITUATION

- **1. Définir sommairement le contexte de la perte ou du vol de renseignements personnels :**
  - Identifier les RP touchés ainsi que leur support;
  - Identifier les personnes (clients, employés) touchées et leur nombre;
  - Établir le contexte des événements (date, heure, lieu, etc.);
- **2. Informer les autorités externes concernées** (Police, CAI, etc.)
- **3. Désigner une équipe responsable de la gestion de la situation.**
- **4. Informer les intervenants concernés à l'interne :**
  - Dirigeants de l'organisme ou de l'entreprise, responsable de la protection des RP, Conseiller juridique;
  - Direction des communications (gestion médias et appels clientèle).

mcmillan 58

Principales étapes à suivre lors d'une perte ou d'un vol de RP

ÉTAPE 2 : LIMITER L'ATTEINTE À LA VIE PRIVÉE

- L'organisme ou l'entreprise doit prendre sans tarder des mesures adéquates pour limiter les conséquences pour les personnes concernées d'une possibilité d'utilisation malveillante de leurs renseignements personnels, de l'usurpation ou du vol de leur identité :
- **1. Prendre des mesures afin de limiter immédiatement les conséquences d'une perte ou d'un vol de renseignements personnels en s'assurant de mettre fin à la pratique non conforme le cas échéant;**
- **2. Récupérer les dossiers physiques ou numériques, selon le cas;**
- **3. Révoquer ou modifier les mots de passe ou les codes d'accès informatiques;**
- **4. Contrôler les lacunes dans les systèmes de sécurité.**

mcmillan 59

Principales étapes à suivre lors d'une perte ou d'un vol de RP

ÉTAPE 3 : ÉVALUER LES RISQUES

- **1. Compléter une évaluation préliminaire des risques** (sensibilité RP);
- **2. Déterminer le contexte de l'incident incluant** (cause, le caractère délibéré ou non, auteurs connus, l'étendue de la situation)
- **3. Évaluer la possibilité que les RP fassent l'objet d'une utilisation préjudiciable pour les personnes concernées;**
- **4. Évaluer le caractère réversible ou non de la situation;**
- **5. Évaluer si les mesures immédiates prises étaient adéquates pour limiter l'atteinte et les compléter si nécessaire;**
- **6. Déterminer les préjudices potentiels** (possibilités d'utilisation future des RP)
- **7. Déterminer les priorités et identifier les actions à prendre à partir des résultats de l'évaluation de ces risques.**

mcmillan 60

Principales étapes à suivre lors d'une perte ou d'un vol de RP

ÉTAPE 4 : AVISER LES ORGANISATIONS ET PERSONNES CONCERNÉES

- **1. Déterminer qui doit être mis au courant de la perte ou vol de RP en fonction de l'évaluation des risques**
  - Service de police, personnes concernées, CAI, agences de crédit, un cocontractant, un syndicat, un assureur, un ordre professionnel, etc. Toutefois, ne pas aggraver le préjudice que pourraient subir les personnes concernées.
- **2. Désigner les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone);**
- **3. Le cas échéant, identifier et consigner les motifs à l'origine de la décision de ne pas aviser les personnes concernées et les autres intervenants.**

mcmillan 61

Ne pas oublier que…

- Les lois étrangères (ex. certains États américains) peuvent nécessiter une notification pour leurs résidants, peu importe la juridiction où se trouvent ces informations.
- Les individus peuvent s'attendre à recevoir une notification même si la loi n'oblige pas une telle notification (ex. disparition de 470 000 dossiers personnels appartenant à des clients de la banque CIBC en janvier 2007).
- Est-ce que l'obligation légale en matière de responsabilité civile (1457 C.C.Q.) peut s'appliquer?
- Au moins deux lois canadiennes en matière de santé obligent à notifier.

mcmillan 62

6) Utilisation des informations obtenues par l'entremise des médias sociaux ou autres technologies de surveillance

mcmillan 63

Éléments de preuve provenant de réseaux sociaux

Renaud et Ali Excavation inc., (C.L.P., 2009-06-19), 2009 QCCLP 4133, SOQUIJ AZ-50562109

- Confirmation par la Commission des lésions professionnelles d'une révision par la CSST. Mise en preuve de statuts Facebook.
- « [33] La page «facebook» du travailleur est produite. Nous y retrouvons, notamment, les mentions suivantes (année?) :
  - 26 janvier : JE VIENS ARRIVER DU DOCTEUR COOL JAI EU CE QUE JE VOULAIS [sic]
  - 3 février : je relax une autre grosse journe demain [sic]
  - 4 février : VIENS DE FINIR JE RELAX [sic]
  - 9 février : peinture dans maison [sic]

  […]
- [42] Finalement, sans s'attarder sur cet élément de preuve, la Commission des lésions professionnelles trouve étonnante l'inscription du travailleur faite sur sa page «facebook», le 3 février (année?), indiquant qu'il a une «autre» grosse journée demain. L'explication du travailleur n'est pas convaincante (a fait quelques boîtes), d'autant plus que, le lendemain, il inscrit qu'il vient de finir. »

mcmillan

Éléments de preuve provenant de réseaux sociaux

Garderie Les «Chat» ouilleux inc. et Marchese (C.L.P., 2009-10-26), 2009 QCCLP 7139, SOQUIJ AZ-50581454

- Une employée s'est fait couper ses prestations d'assurance invalidité par son assureur à l'automne. Des photos sont produites par l'employeur et l'avocat de l'employée ne s'y objecte pas.
- « [59] […] De plus, certaines photographies produites à l'audience montrent la travailleuse en vacances en République Dominicaine, en janvier 2008, dans des positions peu compatibles avec une souffrance lombaire aussi importante que ce qu'elle décrit à ses médecins à la même période (…) Cela aussi vient entacher sa crédibilité. »

mcmillan

Éléments de preuve provenant de réseaux sociaux

Brisindi c. STM (Réseau des autobus), (C.L.P., 2010-06-04), 2010 QCCLP 4158, SOQUIJ AZ-50645213

- L'employé, qui est chauffeur d'autobus, prétend avoir subi une lésion professionnelle au bras. Des photos mises en ligne sur son profil Facebook sont introduites en preuve et viennent affecter sa crédibilité, et sa demande est rejetée.

- «[25] Durant les mois de juillet et août 2008, le travailleur participe à quatre biathlons et triathlons, soit les 12 juillet 2008, 27 juillet 2008, 10 août 2008 et 16 août 2008, tel qu'il appert des documents déposés par l'avocat de l'employeur et provenant du site « Facebook » du travailleur. [...]
- [46] Tous les documents déposés par l'avocat de l'employeur et provenant du propre site « Facebook » du travailleur démontrent que celui-ci est un sportif accompli, de haut niveau, qui participe à des compétitions très exigeantes et qui, de plus, obtient de bons résultats dans la période pendant laquelle il est en arrêt de travail. Le fait qu'il n'ait parlé à personne de ces activités sportives de haut niveau entache sérieusement sa crédibilité.»

mcmillan

Campeau et Services alimentaires Delta Dailyfood Canada inc. (C.L.P., 2012-11-28), 2012 QCCLP 7666, SOQUIJ AZ-50918073, 2013EXP-74, 2013EXPT-1, [2012] C.L.P. 673

- **Faits :** Une employée est blessée et doit s'absenter du travail. Ses blessures la déprime. Pour tester si sa dépression est vraie, l'employeur a créé un compte fictif au nom de Veronica Miles. Elle a pris soin de créer un profil qui allait attirer l'attention de la travailleuse. Ainsi, son profil indique qu'elle travaille au Cirque du Soleil, qu'elle étudie à l'Université McGill (comme la travailleuse) ainsi que ses préférences musicales, de lecture, de cinéma, etc.

- La travailleuse l'accepte comme amie, ce qui donne à la représentante de l'employeur l'accès à l'ensemble du dossier *Facebook* de la travailleuse. Elle en tire toutes les conversations et interventions que la travailleuse a eues durant les 12 derniers mois. À l'audience, la travailleuse mentionnera qu'elle a été attirée par le fait que le pseudonyme de la représentante étudie à la même université qu'elle et qu'elle semblait être dans une position pour l'aider.

- La travailleuse affirme qu'elle a pris soin d'activer la protection privée sur son profil ce qui est d'ailleurs confirmé par le témoignage de la représentante de l'employeur, qui affirme avoir dû demander à la travailleuse, via son pseudonyme, la permission pour devenir son amie.

mcmillan

67

Campeau et Services alimentaires Delta Dailyfood Canada inc. (C.L.P., 2012-11-28), 2012 QCCLP 7666, SOQUIJ AZ-50918073, 2013EXP-74, 2013EXPT-1, [2012] C.L.P. 673

- **Faits (suite) :** Les deux conditions doivent être remplies pour qu'une preuve soit exclue en vertu de cette disposition. Ainsi, une preuve obtenue par des moyens illégaux mais qui ne porte pas atteinte aux droits et libertés fondamentaux ne sera pas exclue, pas plus qu'une preuve obtenue de façon à enfreindre ces mêmes droits mais qui n'a pas pour effet de déconsidérer l'administration de la justice.
- **Décision :** Le tribunal est d'avis que l'unique but de la démarche de l'employeur était d'espérer trouver de façon fortuite un élément de preuve qu'il ne soupçonnait pas.
- Le tribunal est donc d'avis, dans les circonstances particulières de cette affaire, que les informations obtenues n'auraient pas pu l'être par d'autres moyens.
- Eu égard à tout ce qui précède, le tribunal est d'avis que la preuve tirée du profil *Facebook* de la travailleuse est irrecevable en l'espèce.

mcmillan 68

Pneus Touchette Distribution inc. c. Pneus Chartrand inc. (C.S., 2012-07-10), 2012 QCCS 3241, SOQUIJ AZ-50873800, 2012EXP-2875, J.E. 2012-1529

- **Faits :** La demanderesse, Pneus Touchette, poursuit monsieur Campeau et d'autres personnes pour concurrence déloyale, soutenant que, lorsque monsieur Campeau était à l'emploi de Touchette, il aurait transmis à la défenderesse, Joanne Daemen, des informations confidentielles appartenant à son employeur. Selon la demanderesse, madame Daemen aurait par la suite communiqué ces informations à Pneus Chartrand, une société concurrente de Touchette.
- L'enquête a révélé que monsieur Campeau aurait envoyé plusieurs courriels de son ordinateur du bureau à son adresse courriel personnelle «Hotmail».
- CompuQuest a par la suite employé un logiciel afin de déceler le mot de passe de monsieur Campeau, afin d'accéder à son compte Hotmail. Une fois dans son compte, CompuQuest a pu déterminer que monsieur Campeau aurait transmis de son compte Hotmail, à madame Daemen et à d'autres adresses courriels, des documents appartenant à Touchette.
- Monsieur Campeau allègue qu'en accédant à sa boîte de courriel personnelle CompuQuest a violé son droit à la vie privée tel que protégé par les articles 3, 35 et 36 paragraphe 6 C.C.Q. Monsieur Campeau demande donc le rejet du rapport.

mcmillan 69

Pneus Touchette Distribution inc. c. Pneus Chartrand inc. (C.S., 2012-07-10), 2012 QCCS 3241, SOQUIJ AZ-50873800, 2012EXP-2875, J.E. 2012-1529

- **Question :** Est-ce qu'une personne raisonnable, objective et bien informée de toutes les circonstances serait d'avis que la mise en preuve des courriels provenant de la boite personnelle Hotmail de monsieur Campeau, lesquels ont été obtenus à son insu par son ancien employeur, remettait en question les principes d'équité et de transparence qui sont inhérents au processus judiciaire?
- Le juge doit décider dans chaque cas s'il doit faire primer la recherche de la vérité ou la protection des droits fondamentaux. Pour ce faire, il tient compte notamment de la gravité de la violation, de la nature du litige, de la bonne foi des parties et de l'importance de l'élément de la preuve. [Les tribunaux] sont également portés à recevoir un élément de preuve pour empêcher la victime de la violation d'un droit fondamental de commettre une fraude.
- Gravité de la violation dans cette cause : Touchette avait un intérêt légitime à vouloir examiner le contenu de la boîte de courriel Hotmail de monsieur Campeau. Touchette savait qu'un des ses employés transmettait des informations confidentielles à son concurrent. À titre de directeur de l'informatique chez Touchette, monsieur Campeau avait accès à l'ensemble des fichiers informatiques de la compagnie. Sans explication, monsieur Campeau avait envoyé des courriels à partir de son poste de travail à son adresse Hotmail pendant ses heures de travail.

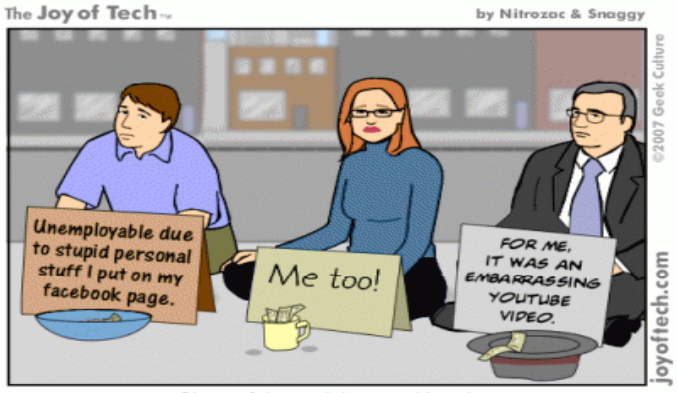
mcmillan 70

Pneus Touchette Distribution inc. c. Pneus Chartrand inc. (C.S., 2012-07-10), 2012 QCCS 3241, SOQUIJ AZ-50873800, 2012EXP-2875, J.E. 2012-1529

- **Décision :** Puisque monsieur Campeau a transmis les courriels en question pendant qu'il était au travail, il ne pouvait raisonnablement s'attendre à ce que ses communications demeurent strictement privées.
- Il faut reconnaître le caractère essentiel de la preuve en question. Sans la production en preuve des courriels, Touchette aurait fort à faire pour contredire la dénégation de monsieur Campeau et son action pourrait être sérieusement compromise.
- Le Tribunal est d'avis qu'une personne raisonnable, objective et bien informée conclurait que l'administration de la justice serait déconsidérée si la preuve des courriels était exclue.

mcmillan 71

Questions?



Signs of the social networking times.

Eloïse Gratton
McMillan LLP
eloise.gratton@mcmillan.ca

mcmillan