cai.gouv.qc.ca

# L’impact d’un incident de sécurité pour le citoyen et l’entreprise

**Me Jean Chartier**

Président

Carrefour de l’industrie de la sécurité

21 octobre 2013 - La Malbaie (Québec)

Commission d’accès à l’information du Québec

cai.gouv.qc.ca

# Présentation générale

La Commission a **deux missions:**

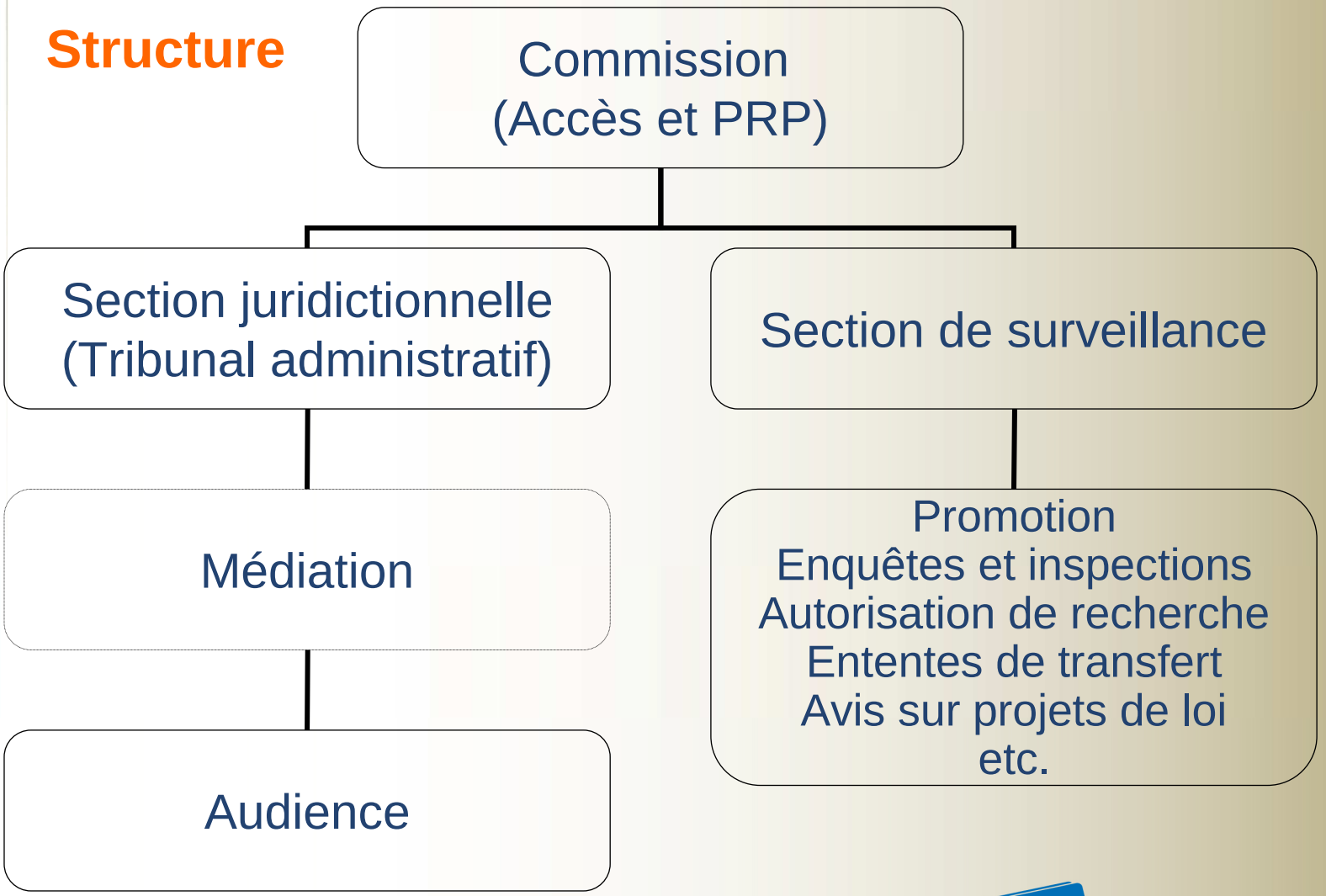
- Assurer le respect et la promotion de l'accès aux documents des organismes publics
- Assurer le respect et la promotion de la protection des renseignements personnels tant dans le secteur public que dans le secteur privé

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Présentation générale

## Structure




Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Protection des renseignements personnels

- Définition de la notion de RP

  « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier »

- RP détenus par les organismes publics et les entreprises (1525 C.c.Q.)

- Règle de la confidentialité

- Devoirs des détenteurs d'assurer la protection des RP / d'adopter des mesures de sécurité

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Protection des renseignements personnels

## Mesures de sécurité

Tout **organisme public** et toute **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.**

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Protection des renseignements personnels

## Mesures de sécurité et documents technologiques

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

**art. 25** – **personne responsable** de l'accès à un document technologique portant un renseignement confidentiel = **prendre des mesures de sécurité propres à assurer la confidentialité** (contrôle d'accès, mot de passe, procédé de visibilité réduite, etc.)

**art. 26** – document technologique confié à un **prestataire de services**

- **Obligation du mandant** : **informer préalablement de la protection que requiert le document** en ce qui a trait à la confidentialité de l'information et des personnes habilitées à en prendre connaissance
- **Obligation du prestataire**: veiller à ce que les moyens technologiques en place permettent d'**assurer la sécurité**, de **préserver l'intégrité**, de **protéger la confidentialité** et d'**interdire l'accès non autorisé** aux documents confiés

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Protection des renseignements personnels

La **sécurité**

- est un principe fondamental en matière de protection des RP

**Toutefois** le **risque zéro n'existe pas** en matière de sécurité.

Les entreprises et les organismes publics ne sont donc pas à l'abri d'un **incident de sécurité**, à savoir:

- un manquement dans la mise en œuvre et l'application des mesures de sécurité
- qui peut provenir d'une simple erreur ou négligence humaine.

Commission d'accès à l'information du Québec

# Incidents de sécurité

## **Enjeux** liés aux incidents de sécurité

**- Pour une entreprise**:

- atteinte à la réputation / marque de commerce
- perte de confiance des clients
- perte du chiffre d'affaires
- coûts financiers de gestion de l'incident
- risque de poursuites civiles si dommages causés
- etc.

**- Pour le citoyen**:

- vol d'identité / fraude
- stress
- démarches à effectuer pour s'assurer que ses renseignements personnels ne sont pas utilisés à son détriment
- risque d'être tenu responsable des dettes contractées en son nom
- etc.

cai.gouv.qc.ca

# Incidents de sécurité

**Défis qui s'imposent aux entreprises et aux organismes publics:**

- AVANT: Élaboration et application de mesures de sécurité efficaces et efficientes, révisées de façon continue (**prévention**)
- APRÈS: Circonscrire rapidement la faille pour minimiser les conséquences pour les personnes concernées (**réaction**)

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité

-La **déclaration** des incidents de sécurité à la Commission n'est **pas obligatoire** car ce n'est pas prévu dans la loi.

- **Néanmoins**, la Commission **encourage** les entreprises et les organismes publics à lui déclarer, sur une **base volontaire**, les incidents de sécurité.

- ***Rapport quinquennal 2011***: la Commission a recommandé au législateur que la déclaration des incidents de sécurité soit obligatoire.

  **Recommandation:** Imposer aux organismes publics et aux entreprises une obligation de déclaration des incidents de sécurité impliquant des renseignements personnels à la Commission.

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité: comment réagir ?

La Commission propose une **procédure à suivre**

- pour les organismes publics et les **entreprises**

  COMMISSION D'ACCÈS À L'INFORMATION, *Aide-mémoire à l'intention des organismes publics et des entreprises en cas de perte ou de vol de renseignements personnels*.

- pour les **citoyens**

  COMMISSION D'ACCÈS À L'INFORMATION, *Aide-mémoire à l'intention des citoyens en cas de perte ou de vol de renseignements personnels*.

* Documents disponibles sur le site Internet de la Commission

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité et entreprises

## Principales étapes à suivre en cas d'incidents de sécurité:

1. Évaluation préliminaire de la situation
2. Limiter l'atteinte à la vie privée
3. Évaluer les risques
4. Aviser les organisations et personnes concernées
5. Évaluation approfondie de la situation et prévention
6. Suivi

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité et entreprises

## Étape 1: Évaluation préliminaire de la situation

1. Définir sommairement le contexte de l'incident de sécurité (perte, vol, etc.);

2. Informer les autorités externes concernées (par ex. service de police, banques, Commission);

3. Désigner une personne ou une équipe responsable de la gestion de la situation;

4. Informer les intervenants concernés à l'interne.

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité et entreprises

## Étape 2: Limiter l'atteinte à la vie privée

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.

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité et entreprises

## Étape 3: Évaluer les risques

1. Déterminer le contexte de l'incident;

2. Déterminer les préjudices potentiels (vol d'identité)

3. Déterminer les priorités et identifier les actions à prendre à partir des résultats de l'évaluation de ces risques.

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité et entreprises

## Étape 4: Aviser les organisations et les personnes concernées

1. Déterminer qui doit être mis au courant de l'incident ;

2. Désigner les personnes responsables ainsi que le moment et le moyen (lettre, courriel, téléphone);

3. Le cas échéant, identifier et consigner les motifs si on décide de ne pas aviser les personnes concernées et les autres intervenants.

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité et entreprises

## Étape 5: Évaluation approfondie de la situation et prévention

1. Approfondir l'analyse des circonstances de l'incident de sécurité et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés.
2. Répertorier et examiner les normes, politiques ou directives internes en place au moment de l'incident et, vérifier si elles ont été suivies par les personnes impliquées - identifier les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant;
3. S'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;
4. Évaluer la nécessité d'élaborer une politique en matière de traitement d'une perte ou d'un vol de renseignements personnels au sein de l'organisme ou de l'entreprise;
5. Formuler les recommandations relatives aux solutions à moyen et long termes et aux stratégies de prévention;
6. S'assurer de la réelle nécessité, pour l'organisme ou l'entreprise, de la collecte des renseignements personnels concernés et, le cas échéant, adopter des mesures de conservation adéquate;
7. Prévoir le suivi devant être accordé.

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité et citoyens

**Quelques conseils** à donner aux personnes concernées par un incident de sécurité

- Pour diminuer les **risques de pertes financières** ou autres:
  - Aviser les institutions financières / les agences de crédit
  - Aviser les services de police
  - Aviser les organismes émetteurs et demander le remplacement du document

Dans tous les cas, conserver les documents pertinents relatifs à vos démarches auprès des différents organismes et entreprises contactés,  faire une demande d'accès à vos renseignements personnels et, le cas échéant, une demande de rectification.

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité:
## Comment la CAI peut vous aider ?

Rôle de la Commission: accompagnement des entreprises pour les aider à mettre en œuvre les différentes étapes précitées.

Déclaration d'un incident = examen de l'incident par l'un des analystes de la section de surveillance

- prise de contact avec l'entreprise;
- demande de complément d'informations si nécessaire;
- évaluation des risques au regard de la sensibilité des RP / du nombre de personnes visées / des protections en place et prises depuis l'incident, etc.;
- recommander d'éventuelles mesures à prendre immédiatement et pour l'avenir.

Commission d'accès à l'information du Québec

cai.gouv.qc.ca

# Incidents de sécurité:
## exemples d'incidents déclarés à la CAI

### Perte / Vol

- perte de renseignements personnels de clients ou d'employés au sein d'un organisme public ou d'une entreprise ou lors de déplacements
- perte ou vol de différents supports (ordinateurs, disques durs, documents papiers, clés USB, chèques)
- perte de données lors de transferts entre organismes publics ou entreprises

### Accès / Divulgation

- divulgation non autorisée de renseignements personnels concernant des clients (dossiers de crédit, carte de crédit)
- accès non autorisé à des renseignements personnels via Internet, des courriels ou des bases de données (piratage, hameçonnage, etc.)
- envoi, par la poste ou par courriel, de documents contenant des renseignements personnels au mauvais destinataire
- informations visibles par la fenêtre de l'enveloppe / lettres non cachetées

### Conservation / Destruction

- mise aux rebuts non sécuritaire de matériel contenant des renseignements personnels
- documents contenant des renseignements personnels mis dans des poubelles publiques

cai.gouv.qc.ca

# Merci de votre attention

http://www.cai.gouv.qc.ca

Commission
d'accès à l'information
du Québec