CRIM

CENTRE DE
RECHERCHE INFORMATIQUE
DE MONTRÉAL

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DE VOS CLIENTS : QUELLES SONT VOS OBLIGATIONS ?

Dr. Fehmi Jaafar

crim.ca

PRINCIPAL PARTENAIRE FINANCIER

Économie et Innovation Québec

CRIM

Le CRIM est un centre de recherche appliquée et d'expertise en technologies de l'information qui rend les organisations plus performantes et compétitives par le développement de technologies innovatrices et le transfert de savoir-faire de pointe, tout en contribuant à l'avancement scientifique.

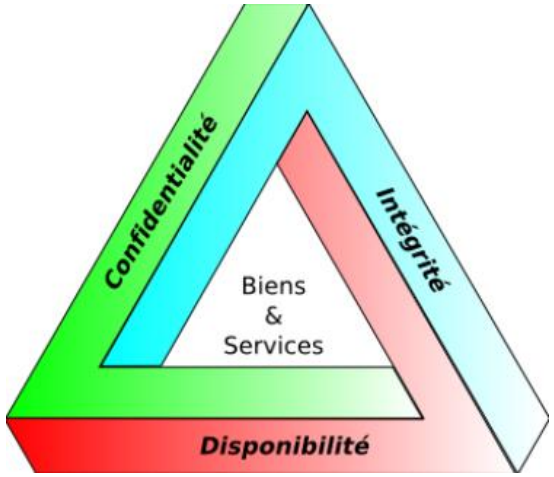
TABLE DES MATIÈRES

1. LA SÉCURITÉ DE L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENT PERSONNELS

1. LA SÉCURITÉ DE L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENT PERSONNELS

LES OBJECTIFS DE LA SÉCURITÉ INFORMATIQUE :

- **L'intégrité** : garantir que les données sont bien celles que l'on croit être ;
- **La confidentialité** : assurer que seules les personnes autorisées aient accès aux données échangées ;
- **La disponibilité** : maintenir le bon fonctionnement du système d'information et l'accès aux services et données ;



"Confidentialité-Intégrité-Disponibilité". Ljean 2008.

1. LA SÉCURITÉ DE L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENT PERSONNELS

MÉTHODES FORMELLES POUR LES SYSTÈMES LOGICIELS SÉCURISÉS :

- Une **donnée à caractère personnel** (couramment « **données** personnelles ») correspond à toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement.
    - Un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.
    - Peu importe que ces informations soient **confidentielles ou publiques**.

1. LA SÉCURITÉ DE L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENT PERSONNELS

- Pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.
- Il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.

2. LES OBLIGATIONS AU CANADA

2. LES OBLIGATIONS AU CANADA

LPRPDE ?

- La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) est la loi fédérale sur la protection de la vie privée à laquelle sont assujetties les organisations du secteur privé.
- La LPRPDE s'applique aux organisations du secteur privé qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales.
- Toutes les entreprises qui exercent des activités au Canada et qui traitent des renseignements personnels qui vont au-delà des frontières provinciales ou nationales sont assujetties à la LPRPDE.

2. LES OBLIGATIONS AU CANADA

LES « RENSEIGNEMENTS PERSONNELS » AUX TERMES DE LA LPRPDE ?

- L'âge, le nom, un numéro d'identification, le revenu, l'origine ethnique ou le groupe sanguin.
- Une opinion, une évaluation, un commentaire, le statut social ou une mesure disciplinaire.
- Le dossier d'un employé, un dossier de crédit ou de prêt, un dossier médical, l'existence d'un différend entre un consommateur et un commerçant, le projet d'une personne (l'intention d'acquérir des biens ou des services ou de changer d'emploi, etc.).

2. LES OBLIGATIONS AU CANADA

QU'EST-CE QUI N'EST PAS « RENSEIGNEMENTS PERSONNELS » ?

- Les coordonnées d'affaires, comme le nom, le titre, l'adresse professionnelle, le numéro de téléphone ou l'adresse courriel **de l'employé**, recueillis, utilisés ou communiqués uniquement dans le but de contacter la personne pour les besoins de son **emploi ou de sa profession**;

2. LES OBLIGATIONS AU CANADA

VOS RESPONSABILITÉS EN VERTU DE LA LPRPDE ?

- **Les entreprises doivent respecter les dix principes :**

1. **Responsabilité**
2. **Détermination des fins de la collecte des renseignements**
3. **Consentement**
4. **Limitation de la collecte**
5. **Limitation de l'utilisation, de la communication et de la conservation**

2. LES OBLIGATIONS AU CANADA

VOS RESPONSABILITÉS EN VERTU DE LA LPRPDE ?

- **Les entreprises doivent respecter les dix principes :**

6. **Exactitude**
7. **Mesures de sécurité**
8. **Transparence**
9. **Accès aux renseignements personnels**
10. **Possibilité de porter plainte à l'égard du non-respect des principes**

2. LES OBLIGATIONS AU CANADA

VOS RESPONSABILITÉS EN VERTU DE LA LPRPDE ?

- **Les entreprises doivent :**
  - Nommer une personne chargée de la conformité de l'organisation à la LPRPDE, et fournir son nom ou son titre à l'interne et à l'externe.
  - Élaborer un programme de gestion de la protection de la vie privée (des protocoles de gestion des incidents).
  - Passer régulièrement en revue le programme de gestion de la protection de la vie privée.
  - Élaborer, documenter et offrir une formation appropriée sur la protection de la vie privée à l'intention des employés.

2. LES OBLIGATIONS AU CANADA

VOS RESPONSABILITÉS EN VERTU DE LA LPRPDE ?

- **Les entreprises doivent :**
  - Déterminer et documenter les fins de la collecte des renseignements personnels et obtenir les consentements.
  - Préciser aux clients la raison de la collecte de leurs renseignements personnels avant ou au moment de la collecte et obtenir à nouveau leur consentement si il y a une nouvelle fin.
  - S’assurer que les processus de consentement soient conviviaux et généralement compréhensibles (mineurs, retirement, etc.)

2. LES OBLIGATIONS AU CANADA

VOS RESPONSABILITÉS EN VERTU DE LA LPRPDE ?

- **Les entreprises doivent :**
  - Protéger tous les renseignements personnels contre leur perte, leur vol ou tout accès non autorisé, leur communication, leur copie, leur utilisation ou leur modification.
  - Protéger les renseignements personnels d'une manière appropriée à l'importance de leur nature délicate.
  - Sur demande, informer les personnes des renseignements personnels les concernant détenus par l'organisation (comment les renseignements sont obtenus, utiliser, communiquer, etc.) dans délai de 30 jours.

3. LES OBLIGATIONS À L'ÉCHELLE INTERNATIONALE

3. LES OBLIGATIONS À L'ÉCHELLE INTERNATIONALE

LE RÈGLEMENT DE L'UNION EUROPÉENNE SUR LA PROTECTION DES DONNÉES (RGPD)

- À compter du 25 mai 2018, toutes les entreprises qui traitent des données personnelles liées à des citoyens européens devront respecter le RGPD.
- En cas de non-respect du RGPD, plusieurs sanctions peuvent être appliquées aux entreprises.

3. LES OBLIGATIONS À L'ÉCHELLE INTERNATIONALE

Six étapes pour s'adapter au RGPD selon la CNIL	
Etape	Détail
Etape 1 : Nommer un délégué à la protection des données	Disposer d'un pilote est indispensable pour gérer les données personnelles collectées par une entreprise. Celui-ci est chargé d'un rôle d'information, de conseil et de contrôle interne.
Etape 2 : Recenser les traitements des données	Un registre des traitements des données personnelles est une documentation qui permet de faire le bilan sur l'effet du règlement.
Etape 3 : Définir les actions correctives	Afin de respecter les règles en matière de droits et libertés personnels, il est nécessaire de déterminer quelles sont les actions prioritaires à mettre en œuvre. La priorisation est déterminée en fonction du niveau de risque et grâce au registre des traitements.
Etape 4 : Analyser les risques	Il convient de gérer au mieux les risques pouvant avoir des conséquences sur la sécurité des données.
Etape 5 : Établir des procédures internes	Les procédures internes permettent de constamment assurer la protection des données personnelles. Il faut ici anticiper les événements éventuels pouvant impacter les traitements en cours.
Etape 6 : Tenir une documentation	La documentation permet de justifier la conformité d'une entreprise au règlement. Il est également essentiel de fréquemment reconsidérer et ajuster les actions et documents afin de garantir une protection des données durable.

3. LES OBLIGATIONS À L'ÉCHELLE INTERNATIONALE

EN CAS DE NON-RESPECT DU RGPD, PLUSIEURS SANCTIONS PEUVENT ÊTRE APPLIQUÉES AUX ENTREPRISES :

- Étape 1 : Avertissement ou mise en demeure de l'entreprise accompagné d'un rappel des règles concernant la mise en conformité ;
- Étape 2 : Injonction, ordre de cessation immédiate des violations constatées ;
- Étape 3 : Limitation ou suspension temporaire des traitements ou des flux de données ;
- Étape 4 : Sanctions administratives pour les entreprises qui n'ont pas respecté l'injonction.
- Étape 5 : Sanctions pénales applicables peuvent atteindre jusqu'à **300 000 € d'amende** et entrainer jusqu'à **5 ans d'emprisonnement**.

4. LES BONNES PRATIQUES DE LA SÉCURITÉ DES DONNÉES PERSONNELLES

4. LES BONNES PRATIQUES DE LA SÉCURITÉ DES DONNÉES PERSONNELLES

- **Sensibiliser les utilisateurs** : faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée.
- **Gérer les habilitations** : limiter les accès aux seules données dont un utilisateur a besoin.
- **Tracer les accès et gérer les incidents** : journaliser les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).
- **Sécuriser les postes de travail** : prévenir les accès frauduleux, l'exécution de virus ou la prise de contrôle à distance, notamment via Internet.
- **Sécuriser l'informatique mobile** : anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile.

4. LES BONNES PRATIQUES DE LA SÉCURITÉ DES DONNÉES PERSONNELLES

- **Sécuriser les sites web** : S'assurer que les bonnes pratiques minimales sont appliquées aux sites web.
- **Encadrer la maintenance et la destruction des données** : Garantir la sécurité des données à tout moment du cycle de vie des matériels et des logiciels.
- **Gérer la sous-traitance** : Encadrer la sécurité des données avec les sous-traitants.
- **Sécuriser les échanges avec d'autres organismes** : Renforcer la sécurité de toute transmission de données à caractère personnel.

Fehmi Jaafar, Ph. D.
Chercheur en cybersécurité

fehmi.jaafar@crim.ca

WWW.CRIM.CA

405, avenue Ogilvy, bureau 101, Montréal (Québec) H3N 1M3
514 840-1234 / 1 877 840-2746