IN|FIDEM

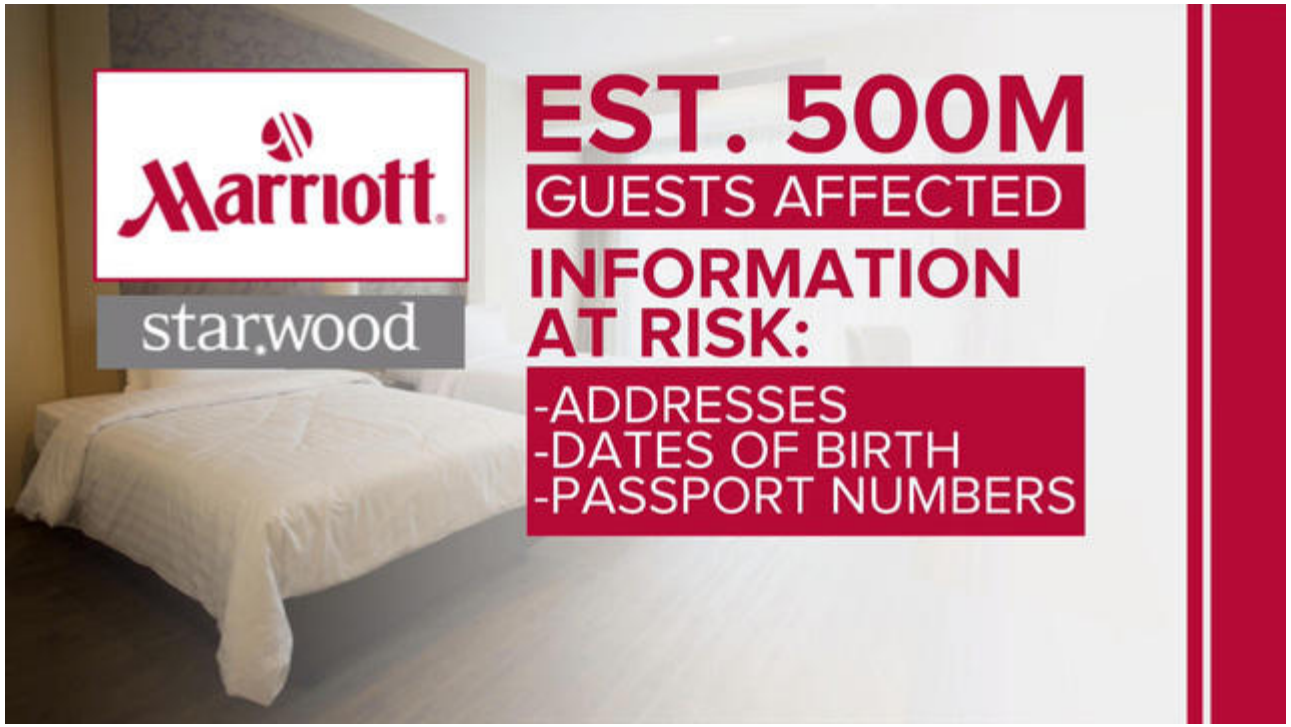
La protection de la vie privée dès la conception des systèmes d'information

ISACA®
Section de Québec

David Henrard, CISA, CISM, CGEIT, CRISC

Le 5 décembre 2018 – Université Laval

Actualité



INFIDEM

Actualité (suite)

INFIDEM

Actualité (ancienne…)

INFIDEM

Cas vécu

INFIDEM

Les 7 facettes de la protection de la vie privée

The Seven Categories of Privacy That Every Enterprise Must Address, ISACA

INFIDEM

Qu’est-ce qu’un renseignement personnel?

- Un renseignement qui concerne une personne physique et qui permet de l’identifier.

- Art. 4 du règlement général sur la protection des données (personnelles)
  - "toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu’un nom, un numéro d’identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

INFIDEM

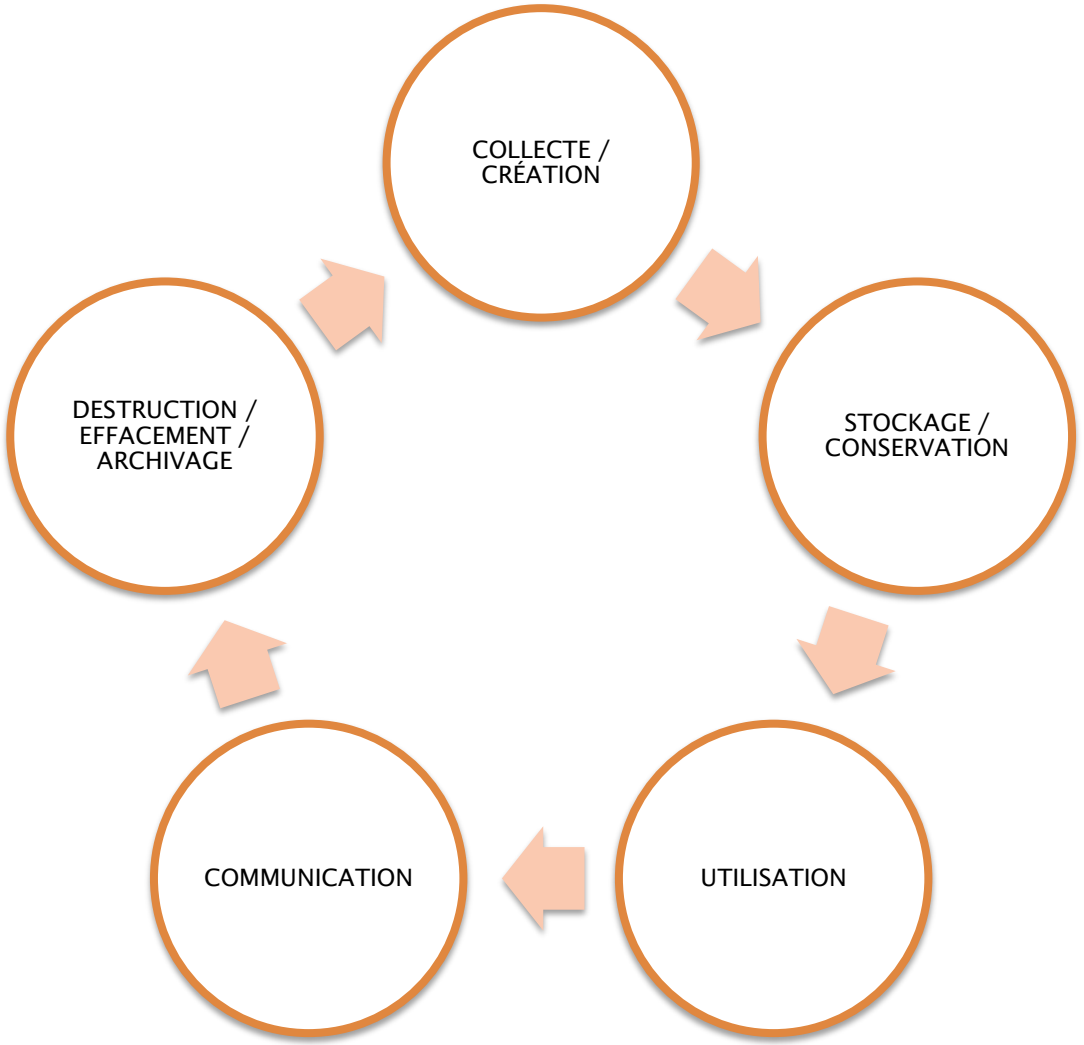
Les catégories de renseignements personnels

- Internes
  - Connaissance et croyance
  - Authentifiant
  - Préférence
- Externes
  - Identifiant
  - Appartenance ethnique
  - Sexualité
  - Comportement
  - Informations démographiques
  - Informations médicales et de santé
  - Caractéristiques physiques
- Suivi
  - Dispositif informatique
  - Contacts
  - Localisation

- Historique
  - Vécu
- Financier
  - Compte
  - Propriétés
  - Transactions
  - Crédit
- Social
  - Professionnel
  - Criminel
  - Vie publique
  - Famille
  - Réseautage social
  - Communications

INFIDEM

Protection tout au long du cycle de vie du renseignement personnel



INFIDEM

1. LA PROTECTION LORS DE LA COLLECTE

- Objectif poursuivi
  - Licite et conforme à la mission de l'organisation
- Nécessité de la collecte
- Consentement éclairé
  - Qui? Pourquoi? Où?
- Collecte sécuritaire (par un moyen assurant la protection)

2. LA PROTECTION LORS DE LA CONSERVATION

- Protection adéquate compte tenu de la sensibilité des renseignements
- Maintien de l'intégrité – absence d'altération
- Gestion et contrôle des accès
- Responsabilité même si les renseignements sont confiés à un tiers

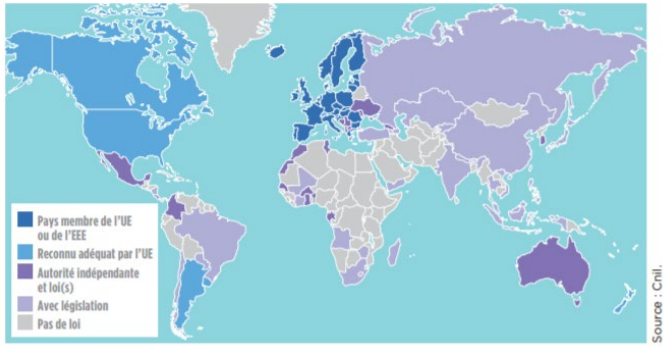
INFIDEM

3. LA PROTECTION LORS DE L'UTILISATION

- Limitation de l'utilisation
- En lien avec l'objet pour lequel il a été collecté
- Contrôle de l'utilisation
  - Journalisation, dépersonnalisation, anonymisation
- Sensibilisation des utilisateurs

4. LA PROTECTION LORS DE LA COMMUNICATION

- Moyen de communication assurant la protection
- Cadre contractuel (entente)
- Prévue lors de la collecte
- Communication à l'extérieur du Québec
  - Nécessité d'un régime de protection équivalent
  - Obligation d'informer la personne



INFIDEM

5. LA PROTECTION LORS DE LA DESTRUCTION

- Lorsque l'objectif pour lequel il a été collecté est accompli
  - Sous réserve du respect des règles d'archivage

- Par un moyen sécuritaire et irréversible

Privacy by Design (Pbd)
Sa provenance et sa signification

- Approche développée dans les années 1990 par Dr. Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario
- Consiste à intégrer la protection de la vie privée dès la conception, l'opération et la gestion d'un système d'information ou d'un processus d'affaires
- Repose sur l'adoption de 7 principes fondamentaux

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

INFIDEM

Les 7 principes fondamentaux du PbD

- Prendre des mesures proactives et non réactives, des mesures préventives et non correctives
- Assurer la protection par défaut de la vie privée
- Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques
- Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle
- Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements
- Assurer la visibilité et la transparence
- Respecter la vie privée des utilisateurs

Les nouveaux enjeux

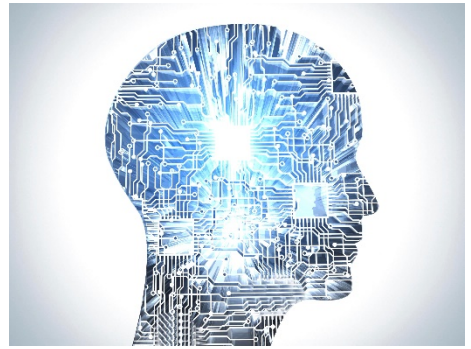
L'identité numérique

La mobilité

Les objets connectés

L'infonuagique

Les données massives



L'intelligence artificielle

INFIDEM

LA DÉCLARATION DE MONTRÉAL POUR UN DÉVELOPPEMENT RESPONSABLE DE L'INTELLIGENCE ARTIFICIELLE – 4 décembre 2018

3- PRINCIPE DE PROTECTION DE L'INTIMITÉ ET DE LA VIE PRIVÉE

- La vie privée et l'intimité doivent être protégées de l'intrusion de SIA et de systèmes d'acquisition et d'archivage des données personnelles (SAAD).

  1) Des espaces d'intimité dans lesquels les personnes ne sont pas soumises à une surveillance, ou à une évaluation numérique, doivent être protégés de l'intrusion de SIA ou de systèmes d'acquisition et d'archivage des données personnelles (SAAD).
  2) L'intimité de la pensée et des émotions doit être strictement protégée de l'usage de SIA et de SAAD susceptible de faire du tort, en particulier de l'usage visant à juger moralement des personnes ou de leur choix de vie.
  3) Les personnes doivent toujours avoir le choix de la déconnexion numérique dans leur vie privée et les SIA devraient explicitement offrir le choix de la déconnexion à intervalle régulier, sans inciter à rester connecté.
  4) Les personnes doivent avoir un contrôle étendu sur les informations relatives à leurs préférences. Les SIA ne doivent pas construire de profils de préférences individuelles pour influencer le comportement des personnes concernées sans leur consentement libre et éclairé.
  5) Les SAAD doivent garantir la confidentialité des données et l'anonymisation des profils personnels.
  6) Toute personne doit pouvoir garder un contrôle étendu sur ses données personnelles, en particulier par rapport à leur collecte, usage et dissémination. L'utilisation par des particuliers de SIA et de services numériques ne peut être conditionnée à l'abandon de la propriété de ses données personnelles.
  7) Toute personne peut faire don de ses données personnelles aux organismes de recherche afin de contribuer au progrès de la connaissance.
  8) L'intégrité de l'identité personnelle doit être garantie. Les SIA ne doivent pas être utilisés pour imiter ni modifier l'apparence physique, la voix et d'autres caractéristiques individuelles dans le but de nuire à la réputation d'une personne ou pour manipuler d'autres personnes.

IN|FIDEM

Merci !

David Henrard, CISA, CISM, CGEIT, CRISC