Compte-rendu de conférence WAQ 2019

Gestion de la confidentialité : revue de l'année 2018

Arnaud Hamelin-Lachapelle
Avocat, Sarailis Avocats

Gestion de la confidentialité : ordre du jour

- Développements récents (2018)
- Ce qui s'applique au Canada
- Réflexions d'un avocat
- Privacy by Design
- Q&A

Développements récents (2018)

17 Mars : Cambridge Analytica

Scandale : une entreprise de collecte de donnes et d'analyse psychologique ont eu accès a des données sur 87 millions d'utilisateurs Facebook et les ont utilisés pour la campagne de Donald Trump.

Le scandale est un écho de celui de Ted Cruz qui était exactement le même.

Tout part d'OpenGraph et de la gestion des utilisateurs (accès a tous les amis via une seule autorisation d'un utilisateur). Il n'y a pas seulement ce qui est publique mais vraiment tout le contenu Facebook.

Donc à partir de 300 000 participants d'une appli de gamification de 2013 ils sont arrivés à 87 millions.

Ils sont utilisé cette donnée pour vendre des profils psychologiques, notamment pour des études politiques.

15 Mai : RGPD

A partir du moment où on a une donnée personnelle (collecte ou traitement), on est régie par le règlement général pour tous les résidents européens.

Les exigences :

- Consentement libre et éclairé avant tout traitement. Optin obligatoire. Il faut donc un acte positif de consentement
- Droit d'accès
- Droit d'oubli
- Designer un DPO (responsable traitement des données)
- Politique de gestion des données, politique de confidentialité
- Désignation d'un représentant en Europe si une société externe traite de la donnée européenne.
- Informer toute brèche consciente de sécurité dans les 72h

Pénalités :

- Exemple. De 50 millions à Google pour non-respect.
- 91 amendes en Janvier.
- 4% du CA mondial.

28 juin : California Consumer Privacy Act

- Loi adoptée le 28 juin mais centre en vigueur le 1er janvier 2020.
- Même concept que le RGPD, même si des différences.
- Tout traitement de données de californien doit répondre aux exigences du CCPA

  Exigences :

- Droit d'accès
- Doit être informé d'un gain (financier) en rapport à sa donner
- Droit de refus de vente
- Droit de service égal et prix identique (même si on demande qu'il n'y ai pas de vente)
- Il faut un minimum de 50M$ de chiffre d'affaire.

Les amendes ne seront que de quelques milliers de dollars.

8 octobre : Google+ brèche #1

Les données des comptes Google + (de 500 000 personnes) ont été disponible a des développeurs tiers. Mais ça a été corrigé

10 décembre : Google+ brèche #2

Nouvelle brèche pour 52M de comptes accessibles a des développeurs tiers. Mais ça a été corrigé.

Ce qui s'applique au Canada

- Charte des droits et libertés de la personne qui donne un droit inaliénable a la vie privée (image, etc)
- Code civil du Québec
- Loi canadienne anti-pourriel (c-28) : On ne peut pas envoyer un message électronique (quel qu'il soit : message instantané, email, etc) a quelqu'un sans consentement de contact commercial. Les seules circonstances qui donnent droit : donner son nom, prévoir un mécanisme d'exclusion et mettre l'utilisateur au centre de sa réflexion.
- Loi sur la protection des renseignements personnels dans le secteur privé : consentement pour accès à une donnée personnelle (explicite ou tacite est OK)
- Règlement général de protection des données
- California Consumer Privacy Act

Réflexion d'un avocat

Qui est le méchant de 2018

On a vu beaucoup de ransomware, de hackers, etc avant en 2016/2017

En 2018 c'est différant, ce sont les entreprises qui nous offrent des services qui sont devenus des méchants en 2018. Exemple Facebook et Google. L'un a été conçu comme ça et Google par négligence

En 2020, comment on se prépare ? La responsabilité des entreprises est l'anticipation et le durcissement des lois, Beaucoup d'options, des audits de

pratique sont disponibles sur nos données et nos matières de collecte. Développer des processus interne d'analyse de conformité. Toujours se mettre à jour. Avoir des politiques corporatives écrites.

2030 : on conçoit les politiques d'internet de manière étatique alors qu'internet n'a pas de frontières. Peut-être que d'ici quelques années on devra avoir un représentant dans chaque état qui a ses propres lois, ça sera vraiment n'importe quoi et on aura des registres différents pour chaque état. Arnaud Hamelin-Lachapelle espère qu'on en viendra à une réflexion plus globale et logique et qu'elle portera ses fruits sur une entente entre les états et mettre sur pied les règlementations de base avec une adhésion étatique. Ce sera nécessaire. Sauf que quand ça va arriver, les pays qui font déjà accepterons pas de revenir en arrière. Donc il faut prendre le standard le plus haut.

Privacy by design

La conception de nos produits et services, en prenant en compte la confidentialité, est essentielle.

Les piliers du privacy by design :

1. Proactif et non réactif. Prévenir et non guérir. Avoir une réflexion de prévention de brèche, de traitement, de collecte sans raison et valeur ajoutée
2. Mode par défaut. Il faut optin partout, et si on veut un avantage on choisit un optin (car analyse de donne pour personnaliser)
3. Avoir les fonctionnalités complètes. Prévoir l'offre comme étant utile même sans la collecte. Avoir de la valeur sans traitement de donnée. L'utilisateur de toute façon va avoir un comportement naturel d'acceptation pour aller plus vite.
4. Transparence : la perte de confiance des utilisateurs est probante. Il faut éviter la dissonance de discours et être transparent dans ses pratiques. Réfléchir pourquoi on a besoin des données et expliquer simplement pourquoi.
5. Centré sur l'utilisateur : se mettre à sa place.

Si vous avez des questions et/ou voulez parler de cette conférence, venez me voir ! Jules.