La sécurité : une source abondante de sanctions CNIL

Workshop : Data privacy, an interdisciplinary overview after one year under GDPR

Julien Le Clainche - Avocat - Docteur en droit

julien@droit-ntic.com - @droitntic

9 octobre 2019

Aspects juridiques de la sécurité

ASPECTS JURIDIQUES DE LA SECURITE

Les obligations de sécurité et de confidentialité

Des obligation fondamentales

- *"'Un grand pouvoir implique une grande responsabilité"'* Benjamin Parker (Spiderman, 2002)
- Manquement à la sécurité = 2/3 des sanctions CNIL
- Parfois, sanction sans délai de mise en conformité pour les manquements les plus graves
- Personne n'est à l'abris

$\Rightarrow$ Disponibilité, intégrité, confidentialité des données

- Informatique, télématique, avènement des réseaux de communication

$\Rightarrow$ La sécurité prend une place de plus en plus importante

La place croissante de la sécurité en droit des données personnelles

Une obligation de plus en plus précise

- **À l'origine en 1978** → art. 44 : divulgation par imprudence ou négligence
- **Sanctions** : 1 an à 5 ans de prison et de 2 000 à 20 000 francs d'amende
- **En 2004 (transposition de la dir. 95/46)** → art. 34 : prendre toute précautions utiles pour préserver la sécurité et empêcher qu'elles soient **déformées ; endommagées** ou que des **tiers non autorisés** y aient accès
- **Obligation de moyen**
- **Sanctions** : 5 ans de prison, 300 000 euros d'amende

La place croissante de la sécurité en droit des données personnelles

RGPD → art. 121 de la loi 78-17 → analyse de risque

- **Type de risque** : confidentialité / intégrité
- **Type de menace** : interne / externe
- **Conséquences** dommageables prévisibles
- **Probabilité** de la survenance du risque
- **Gravité** du risque
- **Vraisemblance** du risque

⇒ On tient compte de la nature des données et des risques

Sanctions CNIL : 20 000 000 d'euros ou 4% du CA mondial

La place croissante de la sécurité en droit des données personnelles

L'approche par l'analyse de risque

- Analyse d'impact sur la **vie privée** $\Rightarrow$ Analyse d'impact sur la **protection des données**
- Protéger des personnes et des libertés, c'est plus que protéger des données
- **Quand faire une AIPD ?** si $\exists$ un risque élevé
- **Comment savoir si $\exists$ un risque élevé** ? en faisant une AIPD ô-Ô...

RGPD : La violation de données

La violation de données est :

- Une violation de la **sécurité**
- **Accidentelle ou illicite**
- entrainant la **destruction**, la perte, l'**altération**, la **divulgation** non autorisée de DCP

Qui doit être notifié ?

- Notification à la CNIL
- Si risque élevé pour les droits et libertés : notification aux personnes concernées

$\Rightarrow$ **Pb au niveau des droits de la défense**, la victime de la violation est aussi potientiellement coupable d'un manquement à l'obligation de sécurité

La CNIL de plus en plus prescriptrice dans le domaine de la sécurité

LA CNIL DE PLUS EN PLUS PRESCRIPTRICE DANS LE DOMAINE DE LA SECURITE

Où commence et où s'arrête le rôle de la CNIL ?

La sécurité logique

La sécurité logique

- Fermeture des sessions XD
- Logs des sessions
- Chiffrement des données
- Anti-virus, pare-feu et anti-espiogiciels. . .

Où commence et où s'arrête le rôle de la CNIL ?

Mots de passe : dél. 2017-01 et 2017-190

- Identifiant + mot de passe : 12 caractères
- Identifiant + mot de passe + restrictions : 8 caractères
- Identifiant + mot de passe + information complémentaire : 5 caractères
- Identifiant + mot de passe + token : 4 caractères

$\Rightarrow$ ça commence à devenir très précis !

Où commence et où s'arrête le rôle de la CNIL ?

La gestion de fichiers clients

- Authentification des personnes qui accèdent aux données
- Https
- Traçabilité des accès aux données relatives aux paiement
- Chiffrement des données en base
- Anonymisation, hash avec clé secrète
- Gestion des privilèges
- Mesures organisationnelles

Où commence et où s'arrête le rôle de la CNIL ?

Obligation de formation

La formation des personnels

- Les personnels doivent être formés aux obligations qui découlent de la loi
- À la sécurité
- Des condamnations ont pu être prononcées Ch.crim, 30 octobre 2001, gaz. pal., 23 octobre 2002, p.43, note : A. MOLE et H. LEBON

Les décisions CNIL les plus récentes

LES DECISIONS CNIL LES PLUS RECENTES

Les décisions CNIL les plus récentes

Le top 5 des hacks de sites web

- Mots de passe pas assez robustes
- Pas de règle d'authentification de compte
- URL incrémentale
- Pas de chiffrement
- Indexation par erreur dans un moteur de recherche

Les décisions CNIL les plus récentes

Sécurité et sanctions CNIL

Les sanctions récentes

- Dél. 2019-007 18 juillet 2019 : **Direct assurance**, **URLs incrémentales** $\Rightarrow$ **180 000 euros**
- La CNIL polonaise tient compte de la réactivité et de la coopération de Morele.net $\Rightarrow$ 640 000 euros tout de même
- Dél. 2019-005 28 mai 2019 : **SERGIC, URLs incrémentales** $\Rightarrow$ **400 000 euros**
- Dél. 2018-012 26 déc. 2018 : **Bouygues Télécom** ; (B and you), **URLs incrémentales** $\Rightarrow$ **250 000 euros**

Les décisions CNIL les plus récentes

La sécurité logique

Les sanctions récentes

- Dél. 2018-011 19 déc. 2018 : **Uber : Github pas d'authentifications forte, mot de passe ds le code, pas de filtrage IP $\Rightarrow$ 400 000 euros**
- Dél. 2018-010 6 sept. 2018 : **Alliance française, pas d'authentification $\Rightarrow$ 30 000 euros**
- Dél. 2018-008 24 juillet 2018 : **Dailymotion, pas de chiffrement, pas de filtrage IP $\Rightarrow$ 50 000 euros**
- Dél. 20108-003 21 juin 2018 : **Association pour le dév. des foyers, URLs incrémentales $\Rightarrow$ 75 000 euros**
- Dél. 2018-002 7 mai 2018 : **Optical center, URLs incrémentales $\Rightarrow$ 250 000 euros réduit à 200 000 euros par le CE**

Les décisions CNIL les plus récentes

La sécurité logique

Les sanctions récentes

- Dél. 2018-001 8 janvier 2018 : **DARTY, injection formulaire $\Rightarrow$ 100 000 euros**
- Dél. 2017-295 30 nov. 2017 : **jouets connectés "'My friend Cayla"' et "'I-que"' , appairage sans authentification$\Rightarrow$ mise en demeure (clôturée)**

Les enjeux actuels

Que retenir de la doctrine de la CNIL

Des acteurs inégauxs

- Grandes entreprises ⇒ RGPD favorise la diffusion des bonnes pratiques
- Les autres : la sécurité est le parent pauvre

La sous-traitance

- Des sous-traitants mal sensibilisés à la sécurité
- *"'C'est pas nous, pas nous"'* Nif Nif, Nouf Nouf, Naf Naf (Les 3 petits cochons, 1933)

Mais, . . . mais. . . ,c'est déjà fini ? ? ?

Place aux questions

.....

julien@droit-ntic.com - @droitntic - Linkedin