Commission Juridique Eurocloud France

Olivier Iteanu – Avocat

L'obligation de notification des failles de sécurité

14 Octobre 2011

L'ordonnance du 24 août 2011

- A valeur de Loi
- Transposition du 2nd Paquet Télécom de 2008
  - Directive 2002/58 du 12 Juillet 2002 « vie privée et communications Électroniques »
    - « Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur (…) informe les abonnés de ce risque … »
  - Directive 2009/136/EC du 25 Novembre 2009 du Parlement européeen
    - Introduit la notion de « violation de données à caractère personnel » (art. 2 c) 3) et « violations intervenant dans le secteur des communications électroniques » (considérant 59)
- Existe aux USA depuis 2002 [California Security Breach Notification Act – désormais dans 40 Etats]

La mise en œuvre, qui, quoi ?

- « traitements mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux … »
- « Toute violation de la sécurité entraînant accidentellement ou de manière illicite » une violation des données à caractère personnel »

- Limité aux « opérateurs » ou à tous ?
  - Le terme opérateur défini à l'article L 32 15℃(Chap. Ier Définitions) *« On entend par opérateur toute personne (…) exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques »*
  - Communiqué CNIL *« Seuls les fournisseurs (…) c'est-à-dire **essentiellement** les opérateurs déclarés à l'ARCEP … »*
  - Directive 2009 *« les violations intervenant dans le secteur des CE … » (considérant 59)*
  - Création de l'art. 34 Bis dans la Loi Informatique et Libertés de 1978
  - Le sens de l'histoire
- Violation et pas simple risque ni tentative
- Plus que la faille ?

Comment ?

- « le fournisseur avertit, sans délai, la CNIL »
- « Lorsque cette violation peut porter atteinte aux données (…) d'un abonné ou d'une autre personne physique , le fournisseur avertit également, sans délai, l'intéressé »
- Tenir un registre « des violations (…) notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et le conserve à la disposition » de la CNIL

- Avertir ou notifier (Lettre recommandée) ?
- « Sans délai » [dès connaissance] Qu'en pense la Police ?
- Contenu de la notification
  - Description de la faille ?
  - Moyens d'y remédier OUI
- Notification aux Clients et … aux autres
  - Exception à la notification: art. 34 Bis II avant dernier § « les données incompréhensibles » - promotion de la cryptologie

Les sanctions – la double peine

- Ne pas procéder à la notification
  - 5 ans d'emprisonnement et 300K€ d'amende (art. 226-17-1 du Code Pénal)
- « Mise en demeure » de la Cnil et les sanctions associées (article 34Bis II dernier §)
  - Sanctions pécuniaires (jusqu'à 150K€ ou 300K€)
  - Publicité

En conclusion

Cette obligation de notification est une brèche dans l'omerta traditionnelle française (une révolution culturelle)

A terme, il est certain que tout détenteur de données à caractère personnel développant une activité « on line » est concerné

On reste dans l'attente de « guidelines » par la CNIL

Les nouvelles sanctions pénales vont pousser au développement de la pratique des délégations de pouvoir au sein de l'entreprise

Olivier ITEANU

Avocat à la Cour d ’Appel de Paris

contact@iteanu.com -
www.iteanu.com

blog.iteanu.com