

# Protection des données personnelles

Pierre-Yves Bonnetain  
py.bonnetain@ba-consultants.fr

B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

24 mars 2011

- Cabinet de conseil en sécurité informatique créé en 1996.
- Conseils, suivi et assistance en sécurité informatique.
- Audits de sécurité, de configurations, de code. . .
- Tests d'intrusion, tests d'applications (boîte blanche, boîte noire)
- Analyses de risques, gestion des risques sur l'information
- Ingénierie de la sécurité informatique, recherche de solutions
- Formations à la sécurité informatique
- Expertise judiciaire (civile ou pénale) et expertises privées

## Première partie I

Des données personnelles ? Où ça ?

# Pour faire simple

Une donnée personnelle, c'est

Toute bribe d'information permettant d'identifier un individu.

C'est donc, par exemple,

- des photos ou vidéos,
- des adresses électroniques, des numéros de téléphone,
- des SMS, des discussions sur des forums, des listes d'appels téléphoniques
- les notes d'un blog, des pages personnelles, des e-mails,
- les recherches réalisées sur un moteur de recherche, les traces de navigation sur le web,
- des traces GPS, des traces de migration d'antennes mobiles.

## Attention

Ne confondez pas **données personnelles** avec **données privées**. Les secondes sont **incluses** dans les premières, mais n'y sont pas égales.

# Vie privée, vie personnelle et données

Une personne devrait toujours se poser quelques questions :

- Où sont ses données personnelles et ses données privées ?
- Qui en est responsable ?
- Qui y a accès ?
- Quelles sont les règles d'engagement de ces données ?
- Qu'arrivera-t-il si ces données deviennent publiques ?

## Par exemple

Les photos « privées » téléchargées sur un compte Facebook, les informations associées à une fiche « client » (parfois très intrusives ou instructives), etc.

## Garder à l'esprit

Ces questions, et les réponses inappropriées qui peuvent y être apportées par les entreprises, sont autant de risques opérationnels et juridiques.

# Obligations du responsable de traitement

Peuvent être résumées comme suit :

**Obligation de sécurité des fichiers** Adopter les mesures de sécurité physique (locaux) et logique (système d'information) **adaptées à la nature des données et aux risques** présentés par le traitement.

**Obligation de confidentialité des données** Seules les **personnes autorisées** peuvent accéder aux données personnelles contenues dans un fichier.

**Obligation d'information des personnes** Permettre aux personnes concernées par des informations détenues d'exercer pleinement leurs droits. Communiquer : identité du responsable, finalité du traitement, caractère obligatoire ou facultatif des réponses, destinataires des informations, existence de droits et modalités d'exercice, transmissions envisagées.

**Obligation de péremption des informations** Fixer une durée de conservation raisonnable en fonction de l'objectif du fichier. S'assurer que les données sont détruites dès leur péremption.

**Obligation d'autorisation préalable** Traitements informatiques de données personnelles **qui présentent des risques particuliers d'atteinte aux droits et aux libertés** doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL.

**Obligation de finalité** Objectif précis du fichier constitué. Informations exploitées cohérentes par rapport à l'objectif du fichier. **Ne peuvent pas être réutilisées** de manière incompatible avec la finalité pour laquelle elles ont été collectées.

## Telcos' data breach notification amendment is passed

OUT-LAW News, 03/11/2009

The European Council has approved a data breach notification rule for Europe's telecoms firms. The amendment to an EU Directive will force telcos to tell customers if they lose their data.

The European Parliament and Commission have already approved the amendments, which will become law after it has been published in the EU's Official Journal and signed by the President of the Council and President of the European Parliament.

The amendments, though, do not extend data breach notification duties to non-telecoms firms, despite the Parliament's earlier demands that it include providers of 'information society services' such as online banks or health services providers.

- Apparition progressive d'une **obligation d'information quant aux atteintes aux données personnelles.**
- France : projet de loi Détraigne-Escoffier

## Conséquences

- Etre capable de détecter l'incident (quelles données perdues ?)
- Etre en mesure d'identifier sa portée (qui est touché ?)



Dès lors qu'il y a collecte d'informations personnelles. . .

- Comment leur propriétaire peut-il y avoir accès ?
- Où et comment sont-elles stockées, archivées, sauvegardées ?
- Qui en a la responsabilité technique ? opérationnelle ?
- Qui peut y avoir accès au sens opérationnel et au sens technique ?
- Dans quelles situations ces données peuvent-elles être utilisées ? Transmises à des tiers ?
- Quelles sont les règles de conservation et d'effacement de ces données ? Comment sont-elles appliquées ?

Bien trop souvent

Aucune de ces questions ne reçoit de réponse pertinente la première fois qu'on les pose.

## Deuxième partie II

Questions ?