JSSI 2008

Obligations de protection des données personnelles et de la vie privée pour un opérateur mobile

Patrick CHAMBET – Alain VERDIER

Bouygues Telecom

Sommaire

- Panorama des obligations concernant les données
  - Informatique et libertés
  - Effacement/conservation des données de trafic/connexion - navigation
  - Sollicitations commerciales
- Mesures de protection des données
  - Risques sur les données
  - Moyens de protection
  - Mise en œuvre des moyens de protection

Contexte

Dispositif d'effacement /conservation des données de trafic / navigation	Dispositif de protection des personnes contre les sollicitations commerciales

Loi informatique et libertés

Quelles obligations Informatique et libertés ?

Déclarer !

Doit être déclaré à la CNIL, **avant son exploitation:**

– Tout traitement automatisé ou non automatisé de données à caractère personnel (directes ou indirectes) figurant dans des fichiers

Informer !

Information des personnes (« Clause CNIL ») dont les données font l'objet d'une collecte

Obligations CNIL

Sécuriser !

Le responsable du traitement doit garantir la protection des données, en **interne et en externe :**

– pas d'altération, déformation des données

– pas de divulgation des données

Purger !

La conservation doit garantir un « droit à l'oubli » (purge dans les systèmes)

Conservation / effacement des données de trafic - navigation

Sécurité Quotidienne (2001)

- Champ d'application de la loi :

Opérateurs de communication électroniques
Données de trafic

- Principe : Effacer les données de trafic dès la fin de la communication

- Exception : conservation des données selon une durée variable dans 4 cas

Sécurité intérieure (2003)

- **Champ d'application de la loi :**
  - -Opérateur de télécommunication
  - - Pages consultées par un internaute

- **Principe posé par la loi :**
Préserver pour une durée ne dépassant pas 12 mois le contenu des pages consultées

⇒ Mise à disposition des données dans un fichier spécifique ou par un accès temporaire et limité aux bases des entités concernées

Conservation

Effacement

Lutte contre le terrorisme, sécurité et contrôles frontaliers (2006)

- Champ d'application de la loi :
- Opérateur de communication électroniques
- Données de connexion

- Principe posé par la loi : Élargissement de la définition d'un opérateur de communication électroniques (cybercafés….)

Confiance en l'économie numérique (2004)

- Champ d'application de la loi :
-Personnes offrant un accès à des services de communication au public
- Personnes assurant pour une mise à disposition le stockage de sons, écrits etc.….

- Principe posé par la loi : Préserver toute donnée permettant d'identifier une personne ayant contribué à la création d'un contenu

Sollicitations commerciales

Confiance en l'économie numérique (2004)

- Champ d'application de la loi : Prospection commerciale via automate d'appel, télécopieur, courrier électronique

- Principe : Prospection interdite si la personne n'a pas exprimé **préalablement** son consentement à la réception de tels messages

- **Exception** : Possibilité de se passer du consentement préalable pour la prospection **électronique**

Informatique et Libertés (1978 loi modifiée en 2004)

- **Déclaration Cnil** pour tout traitement (collecte adresses électroniques..) permettant l'envoi de sollicitations commerciales

Sollicitations commerciales

Directive 12/07/2002

Communications non sollicitées

Sommaire

- Panorama des obligations concernant les données
  - Informatique et libertés
  - Effacement/conservation des données de trafic/connexion - navigation
  - Sollicitations commerciales
- Mesures de protection des données
  - Risques sur les données
  - Moyens de protection
  - Mise en œuvre des moyens de protection

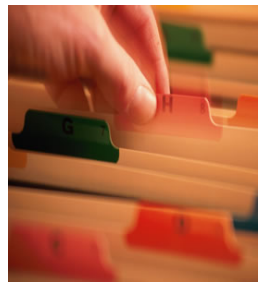
Les risques sur les données personnelles

- Quelques faits divers remarquables…
  - Grande-Bretagne
    - ➔ Disparition de CD-ROMs du HMRC (HM Revenue and Customs) envoyés par TNT -> 25 millions de données de citoyens britanniques
    - ➔ 600 000 données sensibles du personnel de la Royal Navy et de la Royal Air Force
  - Etats-Unis
    - ➔ Affaire TJX
      - Plus de 94 millions de numéros de CB potentiellement compromis
      - Transaction de 41 M$ avec les banques
    - ➔ Plus de 8 millions de dossiers clients détournés et revendus par un DBA
    - ➔ TD Ameritrade: détournement de plus de 6 millions de dossiers bancaires
  - France
    - ➔ SMS…

Moyens de protection des données

- Que disent les normes ?
  - SOX ? ISO 27000 ? PCI-DSS ?
  - Utilisation des meilleures pratiques de l'ISO 27002 et de PCI-DSS

- Première étape: identifier et recenser les informations personnelles qui circulent sur le SI
  - Listes d'appels (vocaux, data, SMS)
  - Données de localisation des clients
  - Tickets de taxe
  - Et bien sûr, données à caractère personnel traditionnelles (noms, adresses, etc...)



Moyens de protection des données

- Contrôle d'accès aux données
  - Habilitation des utilisateurs d'après des profils métiers définis
    - ➔ Gestion des Identités, Gestion des Habilitations
  - Authentification et contrôle d'accès aux applications
    - ➔ IAM, RBAC
  - Affichage sélectif: « ne montrer que ce qui est nécessaire »
    - ➔ Masquage des informations dans les IHM
    - ➔ Là encore, en fonction des profils utilisateurs
  - Traçabilité des accès aux données
    - ➔ En modification
    - ➔ Mais aussi en lecture !
      - « Qui a recherché quoi parmi les données sensibles ? »

Moyens de protection des données

- Chiffrement des données
  - Dans les bases de données
    - ➔ Oracle
      - Oracle >= 9i : TDE (Transparent Data Encryption)
      - Oracle 8 : Obfuscation Toolkit
    - ➔ MS SQL Server
      - EncryptByPassPhrase / DecryptByPassPhrase (Transact-SQL)
    - ➔ Quelques limitations
      - Recherche dans une colonne chiffrée -> comparaison des hashes seulement
      - Gestion des clés…

```
UPDATE Cust.CreditCard
SET CardNumber_Encrypted =
EncryptByPassPhrase(@Passphrase,
CardNumber, 1,
CONVERT(varbinary, CreditCardID))
WHERE CreditCardID = '1234'
```

  - Dans les flux d'échanges entre applications / entre partenaires
    - ➔ Protocoles chiffrés (HTTPS, SSH, SFTP, IPSEC, …)
    - ➔ Attention aux flux externes échangés avec des partenaires sans VPN !

Moyens de protection des données

- Anonymisation
  - Lors du transfert de données à l'extérieur de l'entreprise
  - Lors de la sortie de données de production (jeux de tests par ex.)
  - Utilisation d'applications spécialisées avec règles d'anonymisation complexes
    - ➔ Conservation de la « non qualité » des données notamment
    - ➔ Ex: Compuware, Princeton Softech (-> IBM)
- Purge (au-delà de la période de rétention légale)
  - Parfois difficile (contraintes d'intégrité dans les bases)
  - Revient parfois à anonymiser les « vieux » enregistrements

Moyens de protection des données

- Et bien sûr… protection du domaine bureautique !
  - Le poste de travail: l'éternel point faible, source de fuites d'informations personnelles
    - ➔ Lutte contre le vol (souvent ciblé) de portables et de médias
    - ➔ Supports et périphériques mobiles (clés USB, i-pods, PDA, …)
    - ➔ Pas de transport dans des pays à risque pour les données (USA, Chine, …)

  - Protection contre les chevaux de Troie
    - ➔ Anti-virus/anti-spam, pare-feu personnel, anti-malwares
  - Fourniture d'outils individuels de chiffrement des données
    - ➔ Disques, fichiers (ex: BitLocker, EFS, SecurityBox, ZoneCentral, …)
    - ➔ E-mails (S/MIME)
  - Outils de DLP (Data Leak Prevention)
    - ➔ Un secteur à la mode mais pas encore tout-à-fait mature

      -> Il faut savoir calmer un commercial chaud comme une baraque à frites

Mise en œuvre des moyens de protection

- De nombreux processus et acteurs de l'entreprise sont impliqués (pas seulement concernés)
  - MOAs, métiers: identification des données à protéger
  - DSI, MOEs, bureautique, réseau: conception et mise à disposition des moyens de protection
  - Gestion des risques: suivi des risques de divulgation
- La problématique doit être prise en compte le plus en amont possible
  - Doit être intégrée au processus de gestion de la sécurité dans les projets et les applications

Conclusion

- La protection des données personnelles est un sujet incontournable sur la plupart des SI
- Les risques pesant sur ces données sont devenus très importants
- C'est une obligation légale qui a un coût non négligeable
- Un grand nombre d'acteurs sont impliqués, de bout en bout des processus de l'entreprise

Questions