PROTECTION DES DONNEES PERSONNELLES

FICHE 7 | concept de La Protection des Données Personnelles

CONTEXTE

Au cours des années 70, des projets d'identification ont été lancés pour la création de fichiers d'identification des personnes. Mais ces projets ont suscité une vive émotion de l'opinion publique et montraient le danger de certaines utilisations de l'informatique.

La protection des données personnelles se détache comme une problématique au cœur de la confiance et du développement des usages de l'informatique. Son apparition de plus en plus fréquente dans l'actualité n'en fait pas pour autant un thème facile à appréhender, même par des spécialistes. L'analyse de ces questions est rendue difficile par le fait que l'on ne dispose pas d'un recul suffisant face à des technologies en cours d'introduction dans un contexte d'identification de masse (outils biométriques, mobilité, sans fil, etc.).

Avec l'accroissement des échanges de données personnelles à travers les frontières nationales, il est nécessaire d'assurer la protection effective des droits de l'homme et des libertés fondamentales, et en particulier du droit à la vie privée par rapport à de tels échanges de données personnelles.

Qu'est-ce qu'une donnée personnelle?

Par ce terme, il faut comprendre toutes les informations qui se rapportent à une personne physique ou morale, identifiée ou identifiable.

Exemple de données personnelles :

- Adresse
- Date de naissance
- CV
- Numéro de téléphone
- Revenu
- Santé
- Casier judiciaire
- Éléments biométriques
- Etc.

La réglementation

En France, la loi Informatique et Liberté du 6 janvier 1978, modifiée le 6 août 2004, précise les principes et les modalités du traitement informatique de données à caractère personnel ainsi qu'au traitement non automatisé de telles données dès lors qu'elles sont contenues dans un fichier informatique.

La loi introduit et précise une notion de responsables des données personnelles ainsi que de destinataire.

Elle instaure la Commission Nationale de l'Informatique et des Libertés (CNIL) en tant qu'autorité administrative indépendante et en précise les missions.
Les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la CNIL, et certains doivent faire l'objet d'une autorisation préalable.
En Europe, la directive Protection des données personnelle du 24 octobre 1995 intervient également et précise notamment des obligations en matière de flux de données à caractère personnel transfrontalier, notamment vers les États situés hors de l'Union Européenne.

Les normes en matière de protection des données personnelles
Dans le domaine de la protection personnelle des données, différentes approchent sont envisagées et peuvent s'avérer complémentaires :

1 – Des normes de management des données personnelles, éventuellement certifiables
Dans les pays n'ayant pas de dispositions réglementaires de type CNIL, cette approche a été mise en place. C'est le cas du Japon et du Canada :

Canada : CAN/CSA – Q380 : Code type sur la protection des renseignements personnels
Japon : JIS Q 15001 : Compliance Program on Personal Information Protection

2 – Les bonnes pratiques
En matière de sécurité de l'information, la protection des données à caractère personnel peut être envisagée en tant que sous-ensemble d'une politique de management.

Les bonnes pratiques s'adressent aux entreprises et organisations qui ont mis en place un service pour la gestion des données personnelles. Elles intéresseront tout particulièrement le correspondant à la Protection des données à caractère personnel et lui aideront à implémenter la réglementation en interne, y compris dans l'aménagement de clauses contractuelles avec des partenaires.

CWA 15499-1
Personal Data Protection Audit Framework (EU Directive EC 95/46)
Part I: Baseline Framework - The protection of Personal Data in the EU

CWA 15499-2
Personal Data Protection Audit Framework (EU Directive EC 95/46)
Part II: Checklists, questionnaires and templates for users of the framework - The protection of Personal Data in the EU

CWA 15292
Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)

3 – Les normes d'audit portant sur la sécurité des systèmes d'information

ISO 27002 (renumérotation de ISO 17799)

Code de pratique pour le Management de la sécurité – *une partie de cette norme est consacrée à la protection des données personnelles* –:

Référentiel de bonnes pratiques Z67-002 (nov 2003)

Qualité des services internet – Sites de commerce et échange de services sur internet (e-business) – spécifications des critères et évaluation de la qualité des services offerts

4 – Les approches technologiques basées sur des concepts d'architectures à faible transfert de connaissance

Ces approches ont pour objectifs de s'assurer d'une gestion optimisée des informations à caractère personnel susceptible d'être véhiculées.

Les architectures PETs (*Privacy Enhancing Technologies*) assurent les fonctions :
- Gestion d'identités multiples : Réduire les liens entre une personne et les données la concernant, accès personnalisés / privilégiés
- Protection des adresses IP : PET : affectation dynamique des adresses IP, routeurs d'anonymat
- Accès anonyme à des services : Relais d'anonymat unidirectionnels ou bidirectionnels, serveurs de pseudonymes
- Autorisation respectant la vie privée : les credentials (certificats multiples, certificats restreints)
- Gestion des données personnelles : minimisation des données personnelles, auto-détermination, négociation – Accès aux données : principe du moindre privilège, politique de sécurité et mécanisme de protection, données critiques (dossiers médicaux), anonymisation

Autres perspectives :

Ajout de fonctions d'effacement des puces RFID en sortie de magasin (EPC Global)
Modèle de gestion à faible connaissance (analogie avec le ticket de métro ou le billet de banque)

Documents de référence sur les architectures à faible transfert de connaissance :

Accord européen CWA 15263

Analysis of Privacy Protection Technologies, Privacy-Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization

Fascicule de documentation sur l'anonymisation de données personnelles (s'applique à l'Informatique de santé)

FD S97-560 Septembre 2000 - Anonymisation - Glossaire et démarche d'analyse et expression du besoin

La standardisation en protection des données personnelles

Ils existent plusieurs instances qui traitent ce sujet :

- L'atelier européen CEN ISSS sur la protection des données personnelles et de la vie privée

- Le comité international ISO/CEI JTC1 SC 27 Sécurité IT constitué comme ceci:
  WG1 sur le management de la sécurité et la définition des contrôles (normes 27000 + normes Télécoms UIT)
  WG2 sur les techniques et mécanismes de sécurité
  WG3 sur l'évaluation de la sécurité (dont l'évaluation biométrie)
  WG4 sur l'implémentation des contrôles sécurité (le PCA est inclus dedans)
  WG5 sur les techniques de gestion d'id et de données personnelles (privacy)

- Comité technique International ISO JTC1 SC 37 sur la biométrie

- Comité technique européen CEN TC 224 : signature électronique et la carte ECC (European Citizen Card)

- Le consortium W3C traite aussi du sujet sur la protection des données personnelles avec la recommandation P3P : Platform for Privacy Preferences (P3P) V1.0 – recommandation d'avril 2002

- Le consortium Liberty Alliance traite également de ces questions du point de vue de la protection contre le vol d'identité numérique sur les réseaux.

Autre source d'information : PRIME (*Privacy and Identity Management for Europe*) Standardisation Workshop: www.prime-project.eu