Sécurité et données personnelles

François PELLEGRINI
Professeur, Université de Bordeaux

francois.pellegrini@labri.fr

Des « informations nominatives » aux « données personnelles »

Du « croisement » à l'élevage en batterie

Données personnelles et contrôle (1)

- La collecte de données personnelles est une activité très ancienne
  - Concomitante à l'invention de l'administration
    - Collecte de l'impôt
  - Concomitante à l'invention de l'écriture !
- L'usage de ces données pour le contrôle des populations est également ancien
  - Revenus, hérédité et castes, religion, etc.

Données personnelles et contrôle (2)

- Le danger de la collecte massive des données personnelles est apparu avec l'automatisation de leur traitement
  - Fichage des populations au sein de « sommiers »
  - Utilisation de la mécanographie pour la mise en œuvre de tris *a posteriori*
    - Mention de la religion sur les cartes perforées individuelles aux Pays-Bas dans les années 1930

Données personnelles et contrôle (3)

- La puissance des outils numériques a encore accru les possibilités de contrôle des populations
  - « Croisements » entre fichiers et non plus seulement tris au sein d'un unique fichier déjà constitué
- Crainte d'une intrusion démesurée des États dans l'intimité des individus
  - À l'époque, seuls les États avaient la capacité de collecter des masses de données
    - Glissement ultérieur de la menace vers le secteur privé
    - Retour en force des États qui imposent d'accéder plus ou moins secrètement à ces gisements

Données personnelles et contrôle (4)

- Création de lois spécifiques
  - En France, loi « Informatique et libertés », en 1978
- Création d'organes de contrôle indépendants de l'exécutif et des administrations
  - Modèle juridique original d' « Autorités administratives indépendantes »
    - Ne peuvent appartenir aux autres pouvoirs en vertu même de la séparation des pouvoirs
  - En France, création de la CNIL (« Commission nationale de l'informatique et des libertés »)
    - 17 commissaires et ~180 personnes au sein des services

Missions de la CNIL

- Trois missions principales :
  - Autorisation
    - Étude des projets de traitements
    - Élaboration de doctrines relatives aux différents types de traitements
    - Élaboration de normes simplifiées et d'autorisations uniques
  - Contrôle
    - Réalisés par des équipes mêlant juristes et informaticiens
    - Contrôles en ligne depuis 2014
  - Sanction
    - Tribunal administratif spécialisé en matière de données personnelles

Critères d'autorisation

- L'autorisation d'un traitement de données personnelles est jugée selon les critères suivants :
  - Finalité
  - Responsable du traitement
  - Destinataire des données traitées
  - Durée de conservation
  - Mesures de sécurité de conservation
  - Conditions d'information, droit d'accès et de rectification
- Contrôles effectués :
  - Légitimité de la finalité
  - Proportionnalité des moyens mis en œuvre

Champ d'application de la loi « I&L » (1)

- Concerne exclusivement les personnes physiques
- S'appliquait aux « informations nominatives »
  - Directement associées au nom de l'individu
- Extension de son périmètre aux informations « indirectement » nominatives
  - Numéros de plaque d'immatriculation, de téléphone, etc.
- Extension aux « données personnelles »
  - Tout ce qui est, directement ou indirectement, rattaché aux personnes physiques
  - Biométrie, traces comportementales, etc.

Champ d'application de la loi « I&L » (2)

- Exemples de doctrines :
  - Existence d'identifiants distincts selon les secteurs
    - Séparation du NIR (le « numéro de sécu ») et du NUMEN
    - Mais extension passée du NIR au domaine de l'entreprise
  - Restriction de l'usage de la biométrie au contrôle d'accès
    - Mais autorisation pour les cantines
    - La biométrie n'est pas révocable !
  - Nécessité d'informer les personnes de l'usage de *cookies* à vocation publicitaire
    - Distinction entre les *cookies* « techniques » et les *cookies* « publicitaires »
    - Quid du *device fingerprinting* ?

Données personnelles et sécurité

Mieux vaut prévenir que guérir...

Obligations réglementaires

- Obligation de maintenir un niveau de sécurité adéquat pour les hébergeurs et opérateurs traitant des données personnelles
  - Obligation de certification de certains opérateurs
  - Obligation (transitive !) d'inclusion de dispositions contractuelles adéquates dans les contrats liant le responsable de traitement à ses sous-traitants.
- Obligation pour les opérateurs de communications électroniques de révéler les fuites de données personnelles à leurs clients et à la CNIL
  - Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques

Protection intégrée de la vie privée (1)

- Prendre en compte la protection de la vie privée dès la conception des dispositifs
- Sept principes :
  - Mesures proactives et non réactives
  - Protection implicite de la vie privée
  - Protection dès la conception des systèmes et pratiques
  - Fonctionnalité intégrale à somme positive, pas nulle
  - Sécurité de bout en bout tout au long de la conservation
  - Assurances de visibilité et de transparence
  - Respect des utilisateurs
- Assurance supplémentaire pour les responsables de traitements quant à leur conformité aux lois « I&L »

Protection intégrée de la vie privée (2)

- Obligation réglementaire future au sein de l'UE
  - Révision de la directive 95/46/CE du 24 octobre 1995
- Article 23 de la proposition de règlement 2012/0011 (COD) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
  - Uniformément applicable dans toute l'UE deux ans après publication
  - Considérant 46 de la directive 2012/0010 (COD) : nécessité de prendre des mesures « *tant au moment de la conception qu'à celui de la mise en œuvre du traitement* »

Préservation des droits fondamentaux (1)

- La révolution numérique ne doit pas permettre l'affaiblissement des droits fondamentaux existants sous prétexte que cela est possible
  - Surveillance généralisée des échanges numériques
- Elle doit au contraire inciter à en étendre la préservation
  - Transposition au monde numérique de droits garantis dans le monde physique

Préservation des droits fondamentaux (2)

- Les droits dans l'espace numérique sont les analogues de droits reconnus et préservés dans le monde physique :
  - La neutralité d'Internet est nécessaire à la liberté d'expression
  - Le droit à l'interopérabilité est l'analogue de la liberté d'association
  - Droit à l'oubli, droit à l'anonymat, etc.
- Ces droits doivent eux aussi être reconnus et protégés comme tels
  - Problèmes de périmètres législatifs

Bibliographie

- *IBM et l'holocauste*, Edwin Black, Robert Laffont, 2001
- *Le profilage des populations*, Armand Mattelard & André Vitalis, La Découverte, 2014
- La législation !
  - C'est facile à lire. Si, si... « *Law is Code* »
- « Recommandations de sécurité concernant l'analyse des flux HTTPS », note technique DAT-NT-19/ANSSI/SDE/NP