université de BORDEAUX

Données à caractère personnel

François Pellegrini
Professeur, Université de Bordeaux
francois.pellegrini@labri.fr

université de BORDEAUX

Identité (1)

- Chaque personne a, dans le monde physique, une ou plusieurs apparences :
  - Professionnelle
  - Amicale
  - Associative
  - etc.

université de BORDEAUX

Identité (2)

- L'identité est la manière dont une entité est reliée à ses apparences
- L'identité numérique est le lien créé, au moyen des technologies numériques, entre une personne et ses diverses apparences numériques

Identité (3)

- Perçue au travers de nombreuses facettes :
  - Ce que l'on déclare de soi
    - Informations fournies à l'inscription sur un site
  - Ce que l'on montre de soi
    - Ses actions
  - Ce que l'on peut connaître
    - Traces que l'on laisse

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 et numérotation des populations « sensibles »
    - Casier judiciaire (et autres « sommiers »)
    - Livret ouvrier
    - Carte d'identité pour les populations nomades et indigènes
  - Utilisation de la mécanographie pour la mise en œuvre de tris a posteriori
    - Cas des Pays-Bas dans les années 1940

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

Données personnelles et contrôle (4)

- 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
  - « CLOUD Act », « Bullrun / Edgehill », « Muscular », « ExpressLane », etc.

université de BORDEAUX

Lois « Informatique & Libertés » (1)

- Création de lois spécifiques
  - En France, loi « Informatique et Libertés » de 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, la CNIL
    - 18 commissaires et ~220 personnels

Lois « Informatique & Libertés » (2)

- Art. 1 LIL :

  « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

  Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

- Principe d'« autodétermination informationnelle »

université de BORDEAUX

Lois « Informatique & Libertés » (3)

- Convention n° 108 du Conseil de l'Europe du 28 janvier 1981
  - 47 États membres
- Directive 95/46/CE
- Règlement 2016/679 (RGPD) en vigueur au 25/5/2018
  - Application immédiate et uniforme au niveau européen
  - Mais encore quelques interprétations laissées aux États membres...
    - Âge de la « majorité numérique », etc.

Missions de la CNIL

- Autorisation
  - Étude de projets de traitements soumis à autorisation
  - Élaboration de doctrines relatives aux différents types de traitements
- Contrôle
  - Contrôles en ligne depuis 2014
- Sanction
  - Tribunal administratif spécialisé en matière de données personnelles
- Conseil

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

- Concerne uniquement les personnes physiques
- S'appliquait aux « informations nominatives »
  - Directement associées au nom de l'individu
- Extension de son périmètre aux informations « indirectement » nominatives
  - Numéros d'immatriculation, de téléphone, etc.

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

- Extension aux « données à caractère personnel »
  - Tout ce qui est rattachable aux personnes physiques
    - Biométrie, traces comportementales, méta-données, etc.
  - Par exemple :
    - Courbe de charge électrique d'un foyer
      - Question du pas d'échantillonnage
    - Style des textes
    - Biométrie
      - Non révocable !
  - Données à caractère « inter-personnel » !

Champ d'application de la loi « I&L » (3)

- Donnée à caractère personnel (art. 4 RGPD)
  - « Toute information se rapportant à une personne physique identifiée ou identifiable [...] ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »

Champ d'application de la loi « I&L » (4)

- Donnée sensible (art. 9 RGPD)
  - « Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. […] »

Critères de licéité

- Licéité appréciée selon les critères suivants :
  - Finalité : déterminée, explicite et légitime
  - Base légale
  - Responsable du traitement
  - Destinataires des données traitées
  - Durée de conservation
  - Mesures de sécurité de conservation
  - Exercice des droits des personnes : information, droit d'accès, de rectification, d'opposition, etc.
- Contrôles de proportionnalité

université de BORDEAUX

Base légale

- Tout traitement doit avoir une base légale (art. 6 RGPD) :
  - Consentement
  - Nécessité pour l'exécution d'un contrat
  - Respect d'une obligation légale
  - Sauvegarde des intérêts vitaux de la personne
  - Mission d'intérêt public ou relevant de l'autorité publique dont est investi le responsable
  - Intérêts légitimes poursuivis par le responsable de traitement ou par un tiers
    - À moins que ne prévale l'intérêt légitime des personnes

Évolutions du fait du RGPD (1)

- Principales dispositions du RGPD :
  - Passage d'un régime d'autorisation à un régime répressif (contrôles à posteriori)
    - Sauf domaines tels que la santé, où l'autorisation demeure
  - Cadre harmonisé au niveau de l'Union européenne
    - Application extra-territoriale
  - Renforcement du consentement
  - Droit à la portabilité des données personnelles
    - Relève tant du droit des personnes que du droit de la concurrence
    - Intérêt à s’appliquer aux données non personnelles

Évolutions du fait du RGPD (2)

- Minimisation des données
- Protection intégrée des données
  - En anglais : « Privacy by design »
    - Mais « protection des données » et « vie privée » sont des concepts distincts
      - Des données personnelles peuvent être publiques
        - Listes électorales
      - Des informations de vie privée peuvent ne pas exister sous la forme de données à caractère personnel
- Obligation de notification en cas de violation
  - À l'autorité de protection des données
  - Aux personnes concernées
- Délégué à la protection des données
  - Doit disposer des moyens d'assurer son rôle

université de BORDEAUX

Évolutions du fait du RGPD (3)

- Obligations du responsable de traitement
  - Registre des traitements
  - Éventuelle analyse d'impact sur la protection des données
  - Encadrement des transferts hors UE
  - Information des personnes
  - Matérialisation du consentement
  - Procédures pour l'exercice des droits
  - Contrats avec les sous-traitants
  - Procédures en cas de violations de données
    - Internes et externes

université de BORDEAUX

AIPD

- Lorsqu'un responsable souhaite mettre en œuvre un traitement, il doit en vérifier les risques pour les personnes
- Si susceptible d'engendrer des risques élevés pour les droits et libertés des personnes, mise en œuvre d'une Analyse d'impact sur la protection des données (AIPD)
  - Logiciel libre « PIA » de la CNIL
- Si risque résiduel important, consultation de l'autorité de protection des données

Anonymisation et réidentification (1)

- L'anonymisation des données est un sujet critique à l'ère du numérique
  - Alimentation des algorithmes de « mégadonnées »
  - « *Open data* »
  - Respect de la vie privée des citoyens
    - Nécessité de ne pas pouvoir réidentifier

université de BORDEAUX

Protection intégrée des DCP

- Prendre en compte la protection des données à caractère personnel dès la conception des dispositifs (« *data protection by design* » / « *privacy by design* »)
  - Assurance supplémentaire pour les responsables de traitements quant à leur conformité aux lois « I&L »
- Configuration de base la plus protectrice (« *data protection by default* » / « *privacy by default* »)

Statut des DCP

- En Europe, les données personnelles sont attachées à la personne et leur contrôle est inaliénable
  - Vision « personnaliste » de la donnée
    - Attachée à la personne dont elle émane
    - Au contraire de la vision « propriétariste »
  - Vision sociale de la donnée, plutôt qu'individuelle
    - Cas des données médicales
  - Données à caractère « inter-personnel »
    - Évident avec les données génétiques, les patro/matro-nymes, etc.

Gestion de la biométrie

- Les données biométriques sont extrêmement sensibles
  - Non révocables car intimement associées aux personnes
- Deux principaux usages :
  - L'authentification : pouvoir assurer qu'une personne est bien la bonne
  - L'identification : retrouver une personne dans une base de données à partir de ses traces
    - Ne doit pas être possible hors fichiers de police
      - Mésusage du FNAEG avec la « recherche en parentèle »
    - Conservation de la biométrie dans TES

université de BORDEAUX

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* »
- Le site de la CNIL

  https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
- Travaux de Y.-A. de Montjoye et autres sur la réidentification