Enjeux démocratiques de la protection des données à caractère personnel

François Pellegrini

Inria

Enjeux démocratiques de la protection des données à caractère personnel

François Pellegrini

01

Statut des données à caractère personnel

Lois « Informatique & Libertés » (1)

- Créées en réaction au mésusage des données à caractère personnel par les États durant la première moitié du XXe siècle
  - > En France, loi « Informatique & Libertés » de 1978
- Participent au « droit à la sûreté », et non à un prétendu « droit à la sécurité »
- Organes de contrôle indépendants de l'exécutif et des administrations
  - > Modèle juridique original d'« Autorités administratives indépendantes »
  - > En France, la CNIL
    - 18 commissaires et 215 personnels

Lois « Informatique & Libertés » (2)

- Article 1er de la loi « Informatique & Libertés » :
  - « *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 »

Lois « Informatique & Libertés » (3)

- Concernent exclusivement les personnes physiques
  - > Cas « limite » des données d'entreprises unipersonnelles
- Encadrent l'usage de données relatives aux personnes
  - > Statut « personnaliste » (voire « inter-personnaliste » !) de la donnée à caractère personnel
  - > Pas de « propriété » sur les données à caractère personnel (ou en général, d'ailleurs !)
    - Donc pas de « vol »
    - On doit parler de « violation », d'« usage illicite », etc.

Le RGPD (1)

« *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)* »

- Évolution plutôt que révolution :
  - Cadre (plus) harmonisé à l'échelle européenne
  - Passage d'un régime d'autorisation préalable à un régime de contrôle a posteriori (sauf santé)
  - Application extra-territoriale
    - S'applique à tous les responsables de traitement qui traitent les données de résidents de l'Union européenne
  - Nouveaux droits et nouvelles obligations
    - Principe de protection des données par conception (« *privacy by design* »)

Le RGPD (2)

- Principe de responsabilisation en amont des responsables de traitements
  - > Conformité (« *compliance*) : respect du cadre légal et des obligations (renforcées) de moyens qui incombent au responsable de traitement et à ses sous-traitants
  - > Redevabilité (« *accountability* ») : le responsable de traitement doit justifier de ses actes
    - – Redevabilité renforcée en cas de risques significatifs : Analyse d'impact sur la protection des données (AIPD)

Donnée à caractère personnel

- Article 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 »
- Liberté générale de traitement dans le cadre de la loi :
  - > Base légale, respect du droit des personnes, etc.

Donnée sensible

- Article 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.* »
- Sauf liste limitative de cas

02

Biométrie et usages

Biométrie et usages (1)

- Quantification des caractéristiques physiques et psychologiques propres à chaque individu
  - > Taille, couleur des yeux, forme du visage, minuties digitales, réseau veineux, profil ADN, dynamique de frappe au clavier, style littéraire, etc.
- Deux usages principaux :
  - > Authentification : déterminer si une personne est celle qu'elle prétend être
    - Finalité administrative
  - > Identification : associer une personne ou une trace à une identité
    - Finalité de police
    - Usages ludiques (ou pas)
- Non révocable
  - > Risque majeur pour les personnes en cas de compromission et de mésusage

Biométrie et usages (2)

- Besoin de fournir des garde-fous juridiques mais aussi techniques pour empêcher le mésusage des données biométriques
  - > Les mesures de protection juridiques peuvent facilement être contournées
  - > Les mesures de protection techniques sont essentielles
    - – Mise en œuvre du principe de protection des données par conception

Considérations architecturales (1)

- Les bases de données centralisées permettent à la fois l'authentification et l'identification
  - > L'identification revient à tenter autant d'authentifications qu'il y a d'entrées dans le fichier
- Les systèmes de stockage individuels ne permettent que l'authentification
  - > Ne peuvent pas être détournés à large échelle

Considérations architecturales (2)

- Biométrie « à la main de l'usager »
  - > Les personnes doivent être seules en mesure de décider de l'usage de leur support biométrique
  - > Nécessité d'existence de moyens alternatifs
- Questions scientifiques et techniques
  - > Usage de la cryptographie asymétrique pour l'authentification des gabarits stockés à la main de l'usager ?
  - > Stockage des gabarits chiffrés en base centralisée à la main de l'usager ?
    - – Transmission sur le canal de communication d'une quantité d'information suffisante pour constituer un secret fiable (entropie et persistance)

03

Cahier des charges démocratique

- Renoncer au postulat démocratique
  - > Un système démocratique doit prendre toutes les mesures pour protéger les populations dans l'éventualité de sa disparition et en attente de sa renaissance
- L'État ne doit pas disposer de la biométrie de l'ensemble de ses citoyens
  - > Ni pouvoir reconstituer facilement un tel fichier
  - > La dé-duplication empêche de créer de faux papiers
    - – Un bon système d'identités doit être « faillible par conception »
- Les systèmes de surveillance ne doivent pas passer à l'échelle
  - > Refus des portes dérobées dans les systèmes cryptographiques
  - > Renoncement à la surveillance de masse
- Sortir du solutionnisme technologique
- Renforcer le droit à la sûreté