

# Technologies, usages, droit « Informatique et libertés »: les enjeux quotidiens, locaux, régionaux et mondiaux

Journées Nationales de l'Informatique et des Libertés, Cotonou 4 et 5 août 2015

Marie GEORGES,  
Experte indépendante Informatique et Libertés

# Evolution des technologies/usages

## locaux- régionaux- mondiaux

- 1960-70 Ordinateur **pour la gestion** (facturation clients, fournisseurs, comptabilité, salaires - DRH, impôts, dossiers scolaires, fichier de police...)
  - > les Etats et grandes entreprises des pays riches, centralisation/Fichiers
  - IBM (tendance économique avec les Tics à l'oligopole voire au monopole)
  - Formulation des principes de base de la protection des données aux USA mais développés en Europe avec en + protection renforcées pour les données sensibles et CNIL (autorité indépendante administrative pour interprétation « IMPARTIALE »)

### Déjà des transferts internationaux=> instruments multilatéraux OCDE, Convention 108 du CdE

- 1980 + mini-informatique = **toute profession ds pays riches** (médecins, avocats ...)
  - MICROSOFT (idem)
- 1990 les prix baissent=> **Accès de tous les continents aux ordinateurs + 95 internet pays riches**= **relation entre individus et organisation** (e commerce, e administration...) PDP Toujours valable + **biométrie et ADN (le CORPS)**
- 2005 après la « bulle internet » émergence des **GAFAM mondiaux** (Google Gmail+ moteur recherche + Docs++ publicité/profil + réseaux, Apple,, Amazon, Facebook réseau social distribution mondialisée) **relations entre individus**
- **Smartphones**, « Cloud », « Big Data », (localisation, appli non sécurées), **objets connectés** (intimité),
- + **2013 Ed. Snowden - surveillance généralisée + accélération des transformations éco sociales/ruptures** (musique, éditions, + « plateformes i to i » achat/vente, locations équipements, voitures - chauffeurs, logements)+ i/collaboratif -->organisations, mais ½ emplois en - 2030

=>CUMUL des avantages mais aussi des difficultés. 2015 enfin l' ONU bouge et désigne un rapporteur spécial vie privée=> convention mondiale dans 10 ans? CdE assume/pays tiers

# Nature des données personnelles

- Elles sont l'expression de notre identité, de notre personnalité, de nos choix
  - Entre les mains d'un tiers dans le cadre de ses activités, sans leur respect  
Il en va de notre vie privée, de notre dignité, de nos libertés (fondement constitutionnel) En effet,  
Selon le contenu des données personnelles, diverses libertés et droits fondamentaux peuvent être en cause :
    - donnée sur la religion (parfois ce que vous achetez - viande halal -), opinion politique
    - géo localisation des mobiles pour leur faire parvenir leurs communications, ou GPS : liberté d'aller et venir,
    - nos recherches sur un moteur de recherche : liberté d'information..
  - Elles ne sont pas appropriables tout comme le corps. Envisager les données personnelles comme une propriété protégée de cette manière serait erronée (cf. serpent de mer aux USA, parfois en Europe)
- ⇒ **LE DROIT À LA PROTECTION DES DONNÉES RELÈVE DES DROITS DE LA PERSONNALITÉ. EN CONFLIT AVEC CEUX POUR QUI S'EST UNE PROPRIÉTÉ, D'OÙ LE RÔLE DE LA COOPÉRATION ENTRE APDP (CNIL) ET DE LA JUSTICE NATIONALE ET SUPRANATIONALE**

# Selon la nature, l'origine et la portée des innovations certains principes peuvent être mis à mal

- Centralisation des fichiers -> **augmentation du pouvoir des organisations sur les personnes** -> autorité indépendante interprète l'application des principes + risques attention interconnexion de fichiers et ID unique
- Cession de fichiers/publicité
  - Pays du nord par la poste et téléphone (gène/ vie privée=>droit d'opposition à la cession),
  - Généralisation mondiale, par e mail et sms = **+grande gêne dans la vie privée** que par la poste=> **plus de protection**=> consentement préalable UE)
- Formulaire d'embauche: peut - on demander la profession des parents? N'est ce pas **disproportionné + risque ≠ égalité ? Si bien sur**
- Fichier d'élèves: centraliser toutes les notes au plan national pour études statistiques sur le long terme: n'est ce pas **disproportionné?** Statistiques par école et centralisation seulement de ces résultats n'est il pas suffisant ? Si bien sur
- Biométrie identifiant une personne de manière unique: si les empreintes des 10 doigts= **présomption d'innocence et droit à la résistance** sont en jeu.
- Le moteur de recherche le plus connu
  - Il garde nos requêtes 13 mois. **La liberté d'information** devrait conduire à 0 mois, la sécurité à 3 mois (pour « étudier des services futurs » si oui ce devrait être avec mon accord...). Il a fini par donner **la possibilité de supprimer de sa mémoire les requêtes.**
  - **Désindexation** possible de documents sur vous si pas d'intérêt public, arrêt Google v. Espagne de la CJEU, mais que Europe=> nouvelle mise en demeure+ d'autres APDP horsEU

# Selon la nature, l'origine et la portée des innovations des problèmes d'autres natures peuvent émerger

- **Réseaux sociaux** -> liberté d'expression: la population, les jeunes en connaissent - ils les limites au regard de
  - la dignité des personnes (vidéo d'une arrestation ≠ présomption d'innocence),
  - la vie privée (pas de publication de photos ou vidéo sans l'accord des personnes)
  - la réputation et l'honneur (interdiction de porter atteinte à (ex. par fausse information
  - des discours de haine et du racisme (interdiction)?

De PLUS « **les limites à liberté d'expression** » sont de la compétence du juge non de la CNIL mais ayant le « nez sur toutes les innovations » une APDP a souvent pour **mission de fait** de renvoyer sur la bonne autorité le problème à résoudre, ici notamment par l' **Education et justice, MAIS => trop=> mise à contribution des services (ouverture d'une page de demande de retrait)**

- **ex Facebook a ouvert une procédure** pour demander de retirer de telles infos. La CNIL peut en donner le conseil.

- **usurpation identité/site de rencontres, la CNIL est compétente pour faire retirer l'information en cas de plainte**

- **Paiement par smartphone**: et si je me trompe de destinataire/numéros de téléphone j'envoie de l'argent à qlq d'autres ! Pas encore de procédure de « doublement du numéro » ni de reprise d'urgence (cf. carte de crédit)=question CNIL (erreur d'information) **mais aussi de protection du Consommateur.**  
**Coopération** entre les autorités

# “Smartphones”

## Enjeux techniques et juridiques

- **Qualité des Smartphones contre les collectes de données invisibles/abusives:**
  - Aucune procédure de certification actuellement de l'absence de back door dans le logiciel de base - mais des logiciels libres (parallèle avec les politiques étatiques dans de nombreux pays)
  - Pas de procédure systématique d'information, y compris pour la durée de conservation, et de consentement préalable pour l'accès d'une application Smartphone à toute donnée personnelle interne à l'équipement, exemple accès invisible à:
    - Géolocalisation/GPS (consentement préalable= garantie établie ds UE)
    - Répertoire des noms, n° tel, e mail... (atteinte à vie privée)
- Vers des symboles standards pour l'information due en vue d'une collecte/traitement loyale et légitime des données par les applications?
- Vers une certification « vie privée » des applications? (tout comme Apple et Google le font pour la cohérence de l'application avec leur logiciel de base) ?

# “Cloud” - Enjeux techniques et juridiques

- **Intérêt pratique**, changement radical d'approche économique pour l'utilisateur/entreprise : paiement de l'informatique “à l'usage” (simple dépense) et non investissement et personnels: pour mise au point de programme à distance, pour mise en œuvre d'application à distance...
- **Enjeux**, en plus de l'application effective de la PDP (« privacy by design », « by default »)
  - **Souveraineté** : cf. actuellement compétence des Etats sur les données localisées sur leur territoire, donc si pas sur « son territoire » risqué d'espionnage
  - **Disponibilité** (en + des politiques étatiques + coopération internationale pour promouvoir internet par plusieurs réseaux interconnectés)
  - **Sécurité** en transmission et en stockage (chiffrement fort, 2030 cryptage quantique)
  - **Reprise des données** possible pour changement de fournisseur

**PROBLEME : Contrat d'adhésion**, souvent peu explicite sur les « protections » : exemples, **isolement des données de deux entreprises, choix? localisation des données et leurs traces/jours, logs de tous les accès**, authentification des salariés, du Cloud, répertoire des suppressions des données en temps utile, disponibilité du services, audit possible...

=> **Les APDP élaborent des listes de questions pour choix du Cloud et management** du projet (traitements stratégiques/pas sur le « cloud », sensibles, autres, progressivité...) et des clauses contractuelles de sauvegardes

+ **Les Etats élaborent des politiques de « Cloud » nationaux**

# “Big Data” ou “Données massives”

## Enjeux techniques et de connaissance

**QUID ? Volume des données, Variété des données, Vitesse de transmission (Gartner)**

=>Gérer des évènements 3V (ex. moteur de recherche, )=> analyse du problème, le découper=>traitements en //, faire remonter les réponses, les synthétiser, ou

=>Découvrir des relations (corrélations) entre les données, leur sens/nouvelles connaissances: **physique des particules, astronomie, climatologie, génomique,**

=>Même objectif **entre des données relatives à des personnes différentes** (non pas la causalité; mais celle ci peut être après recherche), **faire des prédictions individuelles**

**Grandes attentes en écologie, santé/épidémiologie et en marketing économique (et politique)**

# “Big Data” ou “Données Massives”

## Enjeux techniques, sociaux et juridiques

- **Si besoin d’une durée de conservation des données au delà du nécessaire au regard de la réalisation de la finalité d’origine** ... comment: **loi ou consentement**, des personnes concernées, cf.
  - **rendre anonyme des données n’est quasi plus possible** (trop de données détaillées identifient la personne vis à vis de son entourage..)
  - Jusqu’à ce que l’on sache faire ces calculs sur des données chiffrées (recherche en cours au MIT)
- **Croisement de données** issues de plusieurs sources même problème que précédemment (**loi ou consentement**)
- **Finalité : Décision automatique à l’égard d’une personne ?** Contraire au droit à l’autonomie (liberté), et selon la nature des données prises en compte peut être contraire à un autre droit fondamental: **mission de l’ADP d’examiner les données prises en compte +**
  - **possibilité pour la personne d’apporter ses arguments, décision humaine.**
  - **Interdiction d’usage en matière de décision de la justice**

# “Big Data” ou Données Massives

## Enjeux techniques, sociaux et juridiques

- **Finalité : décision des prix** dans un magasin en fonction de la population locale
  - Risque de discrimination indirecte : **l'ADP doit veiller aux critères**
- **Finalité: prédiction santé**
  - **Consentement pour faire partie de l'étude/prédiction**
  - + **Droit de ne pas connaître la prédiction** (déjà présent dans la convention du CdE sur la génétique)
- **Finalité : études avec résultats statistiques.**
  - Loi ou accord des personnes pour l'usage des données y compris pour connaître ou non les résultats, mais
  - **si large population concernée, ne faudrait il pas avoir une garantie que les études sont faites dans un intérêt public?**
    - => **définir une taille de population/données** au delà desquelles seules des **études d'intérêt public** pourraient être faite selon **un mécanisme** également défini par la loi?

# Internet des objets

- Les objets appartiennent à quelqu'un, et/ ou ils peuvent collecter des données sur une personne, sur son comportement etc.
- Flux permanent de données personnelles de la personne à l'objet, de l'objet à un autre objet...
- Exemples:
  - Voiture : capteurs sur les dispositifs pour mesurer l'usure ou la simuler, l'enregistrer, la vitesse, lieux... > prédiction sur le moment de l'entretien nécessaire
  - Montre au poignet avec capteurs pour nombre de battements de cœur, nombre d'epas dans la journée, vitesse de marche...
  - Machine à respirer la nuit, enregistrant le nombre de jours où elle est utilisée, et le nombre d'heures par nuit, nbre d'évènements liés à non respiration....

## Enjeux : vers du Big Data +

- Qui conçoit la machine le logiciel d'analyse? Indépendance des parties prenantes?  
**Si dans domaine de la santé, autorisation de mise sur le marché, comme les médicaments et équipements médicaux ?**
- **Où est réalisée l'analyse des données** : dans l'objet/chez la personne seulement, et/ou chez le constructeurs, et/ou le vendeur, et/ou le médecin prescripteur ?
- **Élaboration de nouvelles normes sur base des résultats, obligatoires ou non?** (cf par exemple les assurances) **Il a fallu une décision du Conseil d'Etat (il y a un mois) sur plainte d'associations de patients pour dire que ce n'est pas à la sécurité sociale de fixer un traitement médical** dans le cas de la machine à respirer la nuit (La SS avait décidé: pas de remboursement si - de 20 jrs/mois, – de 4h par nuit)

# Conclusions

Les CNILs doivent

- suivre les nouvelles technologies et les nouveaux usages;
- les analyser au regard des DH et des transformations sociales en jeu;
- formuler des recommandations après échanges avec les parties prenantes et avec leurs homologues.

Si les recommandations sont formulées très tôt alors leurs recommandations seront le plus souvent bien suivies.

Si besoin de disposition (s) législative(s) ou judiciaire: ne pas hésiter à les promouvoir.

Si besoin de mettre à jour l'instrument régional ou de portée mondiale, ne pas hésiter à en prendre l'initiative avec les homologues