CNIL
Commission Nationale de l'Informatique et des Libertés

Big data : quels enjeux pour la protection des données personnelles?

Sophie Vulliet-Tavernier, directrice des études, de l'innovation et de la prospective

Congrès big data

20 et 21 mars 2012

CNIL
Commission Nationale de l'Informatique et des Libertés

La protection des données personnelles: qu'est-ce que c'est ?

- Reconnaitre à toute personne **des droits sur ses données**
- **Des règles** pour encadrer les traitements de données personnelles
- Un régime de **sanctions** en cas de non respect des principes
- **Une autorité de contrôle indépendante**
- En Europe une **régulation par la loi**, dans le monde, une disparité de situations,

La protection des données dans le monde

- 50 Etats dotés de lois de protection des données

La protection des données personnelles en Europe : un droit fondamental

- **Convention n° 108 du Conseil de l'Europe** pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – 28 janvier 1981
- **Directive 95/46/CE du 24 octobre 1995** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (en cours de révision)
- **Charte des droits fondamentaux de l'UE (art 8)** – 18 décembre 2000
- **Traité de Lisbonne sur le fonctionnement de l'UE (art 16)-**1er novembre 2009

Commission Nationale de l'Informatique et des Libertés

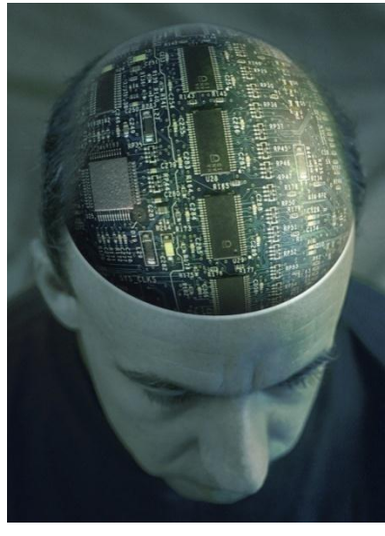
La protection des données personnelles en France

- **La loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, 2009, 2011…**
- **La CNIL, une autorité administrative indépendante**
  - **17 membres(+ le défenseur des droits)**
  - **Effectifs: 160 personnes**
  - **Budget 2012: 17 millions d'euros**
- **Une triple mission**
  - **Informer et conseiller**
  - **Contrôler les traitements: déclarations et contrôles sur place**
  - **Sanctionner en cas de non-respect de la loi**

- **Quelques chiffres**
  - 1,4 millions d'applications déclarées; 75 000 déclarations/an; 2000 demandes d'autorisation et d'avis/an
  - Correspondants informatique et libertés: 10 000 organismes
  - Plus de 4800 plaintes/an
  - 2000 demandes de droit d'accès indirect/an-plus de 4000 vérifications.
  - 400 contrôles en 2011
  - + de 570 mises en demeure; 42 sanctions pécuniaires (montant de près de 758 000 €)

Ce mode de régulation est-il adapté aux nouveaux défis?

- du tout numérique,
- de la globalisation,
- de l'opinion publique
- de la sécurité…
- ET DU BIG DATA ?



CNIL
Commission Nationale de l'Informatique et des Libertés

Le big data à l'épreuve de la protection des données…

- /Donnée personnelle, donnée sensible traitement de données personnelles
- /Finalités
- /pertinence des données
- /Sécurité
- /Transparence et droits

La donnée personnelle selon la loi et la CNIL

- **La loi**: « *constitue une* ***donnée à caractère personnel*** *toute information relative à une personne physique identifiée* ***ou qui peut être identifiée, directement ou indirectement****, par référence à un numéro d'identification* ***ou à un ou plusieurs éléments qui lui sont propres****.* ***Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne*** » (art.2)

- **La CNIL**: une interprétation large et une appréciation au cas par cas de cette notion:
  - / nature des données: ex. initiales des noms et prénoms, date et lieu de naissance, commune de résidence, lieu de travail, nature de l'emploi, des indications de dates (d'examens, d'hospitalisation, …); adresse IP…
  - / l'importance relative de l'échantillon de population concernée;
  - / le type de traitement effectué : ex. data mining.

La donnée sensible selon la loi et la CNIL

- La loi: « *il est interdit de collecter ou de traiter des données à caractère personnel* ***qui font apparaitre directement ou indirectement les origines raciales ou ethniques les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la santé ou à la vie sexuelle*** *de celles-ci* »(art. 8)
- Des dérogations possibles: consentement, données rendues publiques, dossiers médicaux, statistiques…

Big data: vers une nouvelle conception de la donnée personnelle et du traitement de données personnelles ?

- Stockage et analyse en continu de tout type de données
  - Données structurées comme non structurées, texte, photos, vidéos, audios, capteurs, données de geolocalisation, messages, commentaires, données comportementales, techniques, données géographiques, données publiques(open data), biometries….
- Des données toutes potentiellement personnelles et sensibles par recoupement?
- Des données prédictives des comportements= de nouvelles données sensibles

CNIL
Commission Nationale de l'Informatique et des Libertés

La grille d'analyse de la protection des données:
les 5 règles d'or

1. Finalité, proportionnalité
2. Pertinence des données traitées
3. Conservation limitée des données
4. Sécurité et confidentialité
5. Respect des droits des intéressés: loyauté et transparence (droit à l'information, consentement, droit d'opposition, droit d'accès et de rectification)

Le Big data à l'épreuve de la grille d'analyse

- /Finalités et utilisations possibles: prédiction des comportements et habitudes de vie, profilage et détection des comportements « anomaux » sur une logique statistique

- Des champs d'utilisation sensibles
  - Marketing ciblé, personnalisation du search…
  - Sécurité
  - Travail
  - Santé…
- Quid de la prise de décision automatique? Et discriminante?

Le big data à l'épreuve de la grille d'analyse

- Recoupement, interconnexions et centralisation de toutes les données possibles…
- Une remise en question de la conception « traditionnelle » du traitement de données (fichier, SGBD…)
- Comment appliquer les principes de proportionnalité et de pertinence des données?
- Comment sécuriser les données (la question du cloud)?

Le big data à l'épreuve de la grille d'analyse

- **Des traitements et analyses à l'insu des personnes**
- **Comment informer et sur quoi?**
  - les conditions d'exploitation de ses données
  - Ses droits
- **Comment exercer ses droits**
  - Droit de s'opposer- consentir
  - Droit d'accès, de rectification, de suppression
  - Droit de connaitre et de contester la logique qui sous tend une décision prise sur le fondement d'un traitement

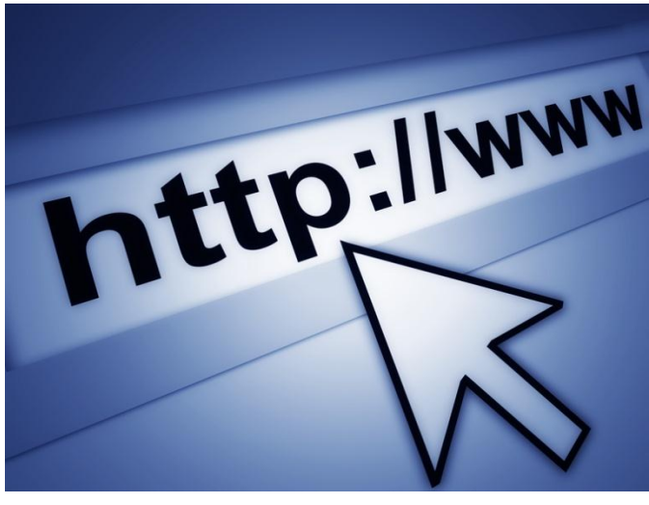
Quelle réponse possible?

- Vers une convention internationale de la protection des données?

- **En Europe: une réforme globale des règles de protection des données**

Le constat…

- Traçage accru et droit à l'oubli peu effectif
- Des droits peu exercés: comment assurer la maitrise de son patrimoine numérique?
- Des risques accrus: divulgation, failles de sécurité, utilisation détournée, usurpations d'identité…
- Des obligations mal respectées et des contraintes administratives trop lourdes et coûteuses
- La marchandisation des données
- Vie privée - vie publique: où est la frontière?



CNIL
Commission Nationale de l'Informatique et des Libertés

Le futur règlement européen: les 5 orientations de la commission européenne

- Garder les principes clés : donnée personnelle, donnée sensible, responsable de traitement, finalité, pertinence,…
- Renforcer les droits des personnes pour développer la confiance et contribuer à l'essor de l'économie numérique
- Assurer une plus grande harmonisation des règles de protection des données tout en renforçant la responsabilité des entreprises
- Etendre par une directive spécifique l'application des règles de protection des données au domaine de la coopération policière et judicaire
- Affirmer la dimension mondiale de la protection des données
- Renforcer le rôle des autorités de protection des données (APD) et du groupe européen des APD, le G29

CNIL
Commission Nationale de l'Informatique et des Libertés

Renforcer les droits des personnes

- Renforcement du consentement des personnes et du droit d'opposition
- Reconnaissance d'un «droit à l'oubli numérique»
- Reconnaissance d'un droit à la portabilité .
- Renforcement des obligations générales d'information: transparence

Responsabiliser les entreprises: l'accountability

- Documentation attestant de la conformité
- analyse d'impact pour les traitements à risques
- privacy by design ou by default
- délégué à la protection des données obligatoire pour le secteur public et pour les entreprises de + de 250 salariés ou lorsque les activités exigent un suivi régulier et systématique des traitements de données personnelles(big data?)
- Mesures de sécurité
- audits
- Obligation de notifier les failles de sécurité

CNIL
Commission Nationale de l'Informatique et des Libertés

La contrepartie: des formalités administratives allégées…

- **Disparition des déclarations**
- **Autorisation uniquement pour certains transferts Internationaux de données.**
- **Analyse d'impact et le cas échéant consultation préalable de l'autorité de contrôle uniquement pour certains traitements à risque**

CNIL
Commission Nationale de l'Informatique et des Libertés

Quelle gouvernance ?

- Sur la compétence des autorités nationales de protection des données
  - Entreprise au sein de l'UE : autorité compétente déterminée par le critère de l'établissement principal
  - Entreprise hors UE sans établissement en Europe : compétence déterminée par le ciblage des personnes concernées.
- Coopération renforcée entre autorités de protection des données
- Pouvoirs de sanctions financières renforcés pour les autorités de contrôle
- Une gouvernance européenne renforcée

La position de la CNIL

- Des avancées substantielles…
  - renforcement des droits, prise en compte de la protection des données dès la conception des produits et services, pouvoirs de sanctions renforcés…
- …Mais la défense de la vie privée ne s'éloigne t'elle pas du citoyen?
  - Une gouvernance trop complexe et bureaucratique
  - centralisation de la régulation de la vie privée au profit d'un nombre limité d'autorités et de la Commission dotée d'un pouvoir normatif important
  - Problème de prise en compte des législations nationales sectorielles par ex dans le domaine de la santé.

CNIL
Commission Nationale de l'Informatique et des Libertés

Big data et régulation

- La réforme européenne est-elle adaptée aux enjeux du big data?

- Quelle éthique, quels modes de régulation à l'horizon 2020?

CNIL
Commission Nationale de l'Informatique et des 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 » (Article 1er)

www.cnil.fr

8, rue Vivienne

CS 30223
75083 Paris Cedex 02