PROTECTION DES DONNEES PERSONNELLES ET RECHERCHE: QUELLES PERSPECTIVES?

Sophie Vulliet-Tavernier

Directeur des relations avec les publics et la recherche

CNIL

VIIème congrès international d'épidémiologie
ADELF-EPITER 7- 9 SEPTEMBRE 2016

Protection des données personnelles et recherche: quels enjeux aujourd'hui?

- Comment concilier les besoins spécifiques de la recherche et la protection des personnes?
- Des gisements de données personnelles de plus en plus massifs: l'accès aux données et leur réutilisation
- Prendre en compte les droits des personnes et l'aspiration à une plus grande maitrise de sa santé (et de ses données)
- La recherche française dans le contexte international trouver un cadre de régulation adapté

La CNIL en bref

- **Une autorité administrative indépendante**
  - 17 membres + le défenseur des droits
  - Services: 190 personnes
  - Budget 2016: 18 millions d'euros
- **Une triple mission**
  - **Contrôle** : déclarations et contrôles sur place et en ligne
  - **Sanction**
  - Information, **conseil**

- + de 90 000 déclarations/an;
- 800 autorisations recherche en 2015
- Correspondants informatique et libertés: +17000 organismes
- guides pratiques, tutoriels video
- 6000 plaintes/an
- + de 400 contrôles/an
- 62 mises en demeure; 18 sanctions dont 8 financières en 2014

La CNIL évolue…

- Mieux répondre aux besoins des usagers: **service besoin d'aide**, FAQ, refonte du site cnil.fr,
- Faire de **la pédagogie, sensibiliser, former**… (projet de mooc universités www.educnum.fr, vade mecum chercheurs…)
- Accompagner la **conformité**: labels (+ de 50), packs, et **PIA…Simplifier les procédures** (AU, MR)
- Avoir une **politique de contrôles et de sanctions + ciblée**
- **Accompagner l'innovation et la recherche** (conseils, partenariats, chaire de recherche, ANR, prix…)
- Développer en concertation, la **réflexion prospective et éthique**: open data, vie privée 2020, santé connectée, voiture connectée… **cahiers IP et labo de la CNIL http://linc.cnil.fr/**

RECHERCHE MEDICALE ET LOI I ET L: UN REGIME DEROGATOIRE

- L'exception recherche dans la loi: finalité compatible, possibilités de dérogation à l'obligation d'information, de traitement des données sensibles
- Une prise en compte des spécificités de la recherche en santé dès les années 90
- Des formalités particulières: avis CCTIRS+ autorisation CNIL
- Un nombre toujours croissant de dossiers et des délais à respecter…

RECHERCHE MEDICALE: SIMPLIFICATION DES PROCEDURES

- Depuis 2006 plus de 5000 autorisations en recherche dont près de 800 en 2015.
- 3 Méthodologies de référence:
  - MR 001 recherches biomedicales (art L 1121-1 du CSP)avec consentement: recherches interventionnelles, essais cliniques, recherches nécessitant l'examen des caractéristiques génétiques
    - Modifié en juillet 2016 pour tenir compte de l'évo des textes
    - + de 3300 engagements de conformité
    - https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033028257&dateTexte=&categorieLien=id
  - MR 002 études non interventionnelles de performances concernant des dispositifs médicaux de diagnostic in vitro
    - Une vingtaine d'engagements de conformité
    - http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031074605
  - MR 003 recherches sans consentement
    - https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033028290&dateTexte=&categorieLien=id

La méthodologie de référence MR 003

- **le champ d'application**:
  - recherches en soins courants, recherches non interventionnelles et essais cliniques de médicaments par grappes
  - Exclusion des dispositifs de vigilance, des collections d'échantillons biologiques, des recherches pour lesquelles une dérogation à l'obligation d'information est envisagée, des recherches comportant l'identification directe des personnes, ou nécessitant un appariement avec des données médico-adminsitratives, des recherches génétiques permettant d'identifier des personnes
- **Les données concernées**:
  - données indirectement identifiantes (n° ou code) à l'exclusion du nom ou du NIR pour les patients, données d'identification des PS
  - Données de santé, signalétiques, photos ou videos (sasn idnetification possible), origine ethnique, données génétiques, comportements, habitudes de vie, vie sexuelle, statut vital,
- **Information individuelle des personnes et droit d'opposition**
- **Sécurités: analyse de risques (cf grille)**
- **Formalités: engagement de conformité sur** https://www.cnil.fr/fr/declarer-un-fichier

LES EVOLUTIONS EN COURS

- **La loi de modernisation de notre système de santé (art 193):de nouvelles modalités pour l'accès et la réutilisation des données de santé à des fins de recherche et d'évaluation:**
  - Modification de la loi I et L pour les traitements de données à des fins de recherche, étude et d'évaluation en santé: **réorganisation du circuit des demandes d'autorisation CNIL:**
  - INDS: guichet unique + avis sur intérêt public de la recherche+ recommandations:
  - Avis, selon les types de recherche, des CPP ou du CEREES
  - Possibilité de procédures simplifiées et déclaration pour les traitements de données de santé en cas d'alerte sanitaire
  - Création du SNDS et définition des modalités d'accès

LES EVOLUTIONS EN COURS

- **Le projet de loi pour une République numérique:**
  - Utilisation du NIR chiffré à des fins de recherche et de statistiques et simplification des procédures (declaration)
  - Droits des mineurs: en matière de recherche médicale, sous certaines conditions, l'information d'un des parents peut suffire; possibilité pour les mineurs de plus de 15 ans de s'opposer à l'information des parents; droit à l'oubli des mineurs
  - CNIL: certification des méthodes d'anonymisation et promotion du chiffrement
  - CNIL: un pouvoir de sanction renforcé : de 150 000 à 3 millions d'euros
  - Création du SNDS et définition des modalités d'accès

Le règlement européen: les objectifs (entrée en vigueur mai 2018)

- 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

- Renforcer le rôle des autorités de protection des données (APD) et du groupe européen des APD, le G29

Des principes précisés

Les grands principes

- collecte loyale et transparente
- principe de finalité (légitime, explicite et spécifique) et possible réutilisation des données pour des traitements ultérieurs sous certaines conditions
- principe de proportionnalité des données (adéquates, pertinentes et non excessives)
- durée de conservation limitée
- Garantie d'une sécurité appropriée des données

Les bases légales

- distinction entre les données à caractère personnel et les données sensibles pour lesquelles le principe d'interdiction est maintenu. La définition des données sensibles est étendue (prise en compte des données génétiques)
- bases légales renforcées (consentement)

De nouvelles définitions

- **données génétiques, données de santé, données biométriques, pseudonymisation…**

Renforcement global des droits existants

Le renforcement des droits existants

- obligation générale de faciliter l'exercice des droits (fourniture d'une information claire, intelligible et aisément accessible)
- information renforcée (ex. transferts hors de l'UE)
- droit d'accès précisé (ex. : possibilité d'introduire une réclamation devant une « CNIL »)
- droit de rectification maintenu
- droit à l'effacement et à l'oubli numérique confirmé
- clarification de l'expression du consentement

Les nouveaux droits

- la portabilité des données
- la limitation du traitement
- conditions particulières pour le traitement des données des mineurs

Moins de formalités, plus de responsabilisation

Les responsables de traitements (et sous traitants) ont une obligation générale de mettre en place des mesures appropriées et de démontrer cette conformité à tout moment : **c'est l' *accountability***.

- l'application des principes de ***privacy by design*** et ***privacy by default***
- la conduite **d'analyses d'impact**, ou « DPIA »
- la tenue d'un **registre** des traitements mis en œuvre
- la **notification de failles** de sécurité (aux autorités et personnes concernées)
- la **consultation de la CNIL** pour certains traitements présentant des risques élevés
- la **certification** de traitements et l'adhésion à des **codes de conduite**

Prise en compte des spécificités de la recherche et des statistiques

- La recherche : une définition du champ et des dispositions particulières (ex art 89)
- Reutilisation des données à des fins de recherche: finalité licite et compatible, …
- Possibilité de traiter des données sensibles moyennant des garanties légales
- Possibilités de **dérogations** en matière d'information, d'exercice des droits des personnes, de durée de conservation…
- Garanties / droits et libertés des personnes: ex: minimisation, pseudonymisation

En conclusion: quelques éléments de réflexion

- Harmonisation nécessaire entre droit national et droit européen
- Au-delà des formalités, la nécessaire prise en compte de la démarche « ethique » I et L
- L'importance des travaux de recherche sur le chiffrement, les méthodes d'anonymat et pseudonymat; le développement des dispositifs d'accès sécurisé aux données type casd…vers une recherche plus interdisciplinaire?
- Transparence, participation citoyenne et retours vers les personnes
- Les enjeux majeurs: big data, cloud, objets connectés, IA, homme augmenté, modèles économiques du numérique, GAFA, …

Commission Nationale de l'Informatique et des Libertés

www.cnil.fr

Suivez la CNIL sur...