L’anonymisation en matière de recherche biomédicale

Nathalie Bosmans
CPP Tours Ouest I
Janvier - février 2010
nathalie.bosmans-2@etu.univ-tours.fr

Plan

- I- Définitions :
  - 1-Les avantages
  - 2- Les problématiques
  - 3- La solution intermédiaire

- II- La législation :
  - 1- La législation française
  - 2- La législation communautaire

Définitions

- Anonyme : perdre l'identité civile.
- Anonymisation réversible : processus de rendre anonyme avec la possibilité de retrouver l'identification de la personne. C'est ce qu'on appelle communément le codage ou le cryptage.
- Anonymisation irréversible : processus de rendre anonyme sans pouvoir identifier la personne.
- Données à caractère personnel : selon la directive européenne, toute information concernant une personne physique identifiée ou identifiable (personne concernée)
- Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

1 - Les avantages

- Utiliser un échantillon d'une recherche irréversiblement anonymisé empêche l'obligation du recueil du consentement de la personne et permet ainsi un gain de temps
- Permet d'utiliser un échantillon biologique, par exemple, sans rechercher la personne pour obtenir son consentement

2 - Les problématiques

- S’assurer du consentement de la personne pour l’anonymisation de ses échantillons (article 56 de la loi de 1978)
- Retrouver une personne lorsqu’un investigateur découvre une pathologie avec de graves conséquences
- Quel contrôle ?
- Les dangers de l’exportation des CEBH à l’étranger

3 - Solution intermédiaire

- Le but est de trouver un intermédiaire entre l'anonymisation irréversible et l'identification des données.
- Solution de l'anonymisation réversible : la codification. Les données sont chiffrées pour protéger la personne. Pourtant, si besoin, la personne peut être retrouvée.
- Nouvelle problématique: le code possède une clef. Qui contrôle le détenteur de cette clef ?

II - La législation

- La seule référence qui existe en droit français est la loi n°78-17 du 6 janvier 1978 dans le chapitre consacré aux données personnelles collectées à la suite d'une recherche biomédicale
- Au niveau communautaire, c'est la directive européenne du 24 octobre 1995 n° 95/46 CE 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 qui fixe les règles
- Au niveau international, technique de la conclusion de conventions entre l'Union européenne et les pays tiers

1 - La législation française

- Question : Quels moyens permettent d'imposer l'anonymisation des données ?
- Rôle de l'investigateur est essentiel
- Rôles du CPP, de la CNIL, les possibles sanctions pénales

Le rôle de l'investigateur

- C'est à lui de diriger et de surveiller la recherche (article L.1121-1 CSP et article 34 de la loi de 1978 par rapport au « responsable du traitement »)
- Par ses responsabilités, doit s'assurer de la confidentialité des données, et, surtout, de leur protection

Pouvoirs/Missions CPP ?

- Question : le CPP peut-il imposer l'anonymisation des données personnelles conduites à l'étranger ?
- Article L.1123-7 Code de la Santé Publique : mission de protéger les personnes
- Aucun pouvoir de police donc il ne peut pas l'imposer
- Mais possède un moyen de pression : l'avis sous réserve (qui peut s'ensuivre d'un avis défavorable fondé sur la protection des personnes et des données qui les concernent ➔ leur vie privée ?)

La CNIL

- Quelle réelle action dans le domaine de la recherche biomédicale? Peut-elle interdire l'exportation de données personnelles ?
- Ses pouvoirs de police:

  - investigation

  - sanction (avertissement, mise en demeure, amendes, injonction de cesser le traitement des données)
- Par le biais de ses pouvoirs de police, la CNIL peut interdire l'exportation de données personnelles (accord conclu avec certains Etats)
- Contrôle préalable à toute recherche sur le respect des dispositions réglementaires ou législatives
- Double contrôle avec le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé (CCTIRS) puis de la CNIL

En pratique

- Le CPP ne peut pas imposer une anonymisation des données. La CNIL peut-elle le faire ?
- Le promoteur de la recherche doit respecter la méthodologie MR001*(=référentiel qui définit les modalités de gestion des données dans ce cadre particulier de la recherche)*. Cette méthodologie consiste à protéger les données issues d'une recherche. Dans ce cadre, les données doivent être anonymisées
- Si ce n'est pas une recherche biomédicale, le promoteur doit demander l'autorisation de la CNIL
- La demande d'autorisation doit expliquer comment ces données sont rendues anonymes
- Si ces données ne sont pas rendues anonymes, l'autorisation sera refusée
- Si les données sont quand même utilisées malgré le refus d'autorisation de la CNIL, alors il y aura des sanctions

Les dispositions pénales

= le moyen coercitif

- Si le promoteur ne respecte pas son obligation de déclarer le traitement des données à caractère personnel, il risque 5 ans d'emprisonnement et 300 000€ d'amende (article 226-16 Code pénal)
- Toute une section du Code pénal est consacrée à la protection contre les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques

2 – La législation communautaire

- Question : Quelle législation sur l'exportation des données à caractère personnel ?
- Dans le champ de l'Union européenne
- Notion d'adéquation
- En-dehors du champ européen. Exemples:
  - Suisse
  - Canada
  - Etats-Unis

Dans le champ de l'Union européenne

- Directive européenne n°95/46/CE du 24 octobre 1995
- Respect obligation d'information et de consentement de la personne concernée
- Article 17 directive : au responsable du traitement de protéger les données
- Article 18 directive : obligation de notification à l'autorité de contrôle

La notion d’adéquation

- Selon le paragraphe 56 de l’introduction de la directive n°95/46/CE « le caractère adéquat du niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts »
- Interdiction partage des données si cette protection adéquate n’est pas assurée

Exceptions à la notion d'adéquation

- Consentement de la personne concernée
- Nécessité dans contexte contractuel ou d'une action en justice
- Sauvegarde d'un intérêt public important l'exige (par exemple en cas d'échanges internationaux de données entre les administrations fiscales ou douanières ou entre les services compétents en matière de sécurité sociale)
- Transfert effectué à partir d'un registre légal qui peut être consulté par le public ou par des personnes ayant un intérêt légitime et qui répondent à la demande des personnes concernées. Ici, le transfert ne portera pas sur la totalité des données ni sur des catégories de données contenues dans ce registre.

Exemple de la Suisse

- Directives médico-éthiques et recommandations « biobanques : Prélèvement, conservation et utilisation de matériel biologique humain» du 23 mai 2006 de l'Académie Suisse des Sciences Médicales
- Commissions d'éthique cantonales de la recherche approuvent l'usage , en accord avec le donneur, d'échantillons et de données anonymisés de manière irréversible

Exemple du Canada

- Adéquation de la directive 95/46/CE avec la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

- Décision Commission de l'Union européenne du 20 décembre 2001 n°2002/2/CE

Le Safe Harbour
ou la sphère de sécurité

- Principe : protéger les données personnelles même en dehors des frontières étatiques
- Relations Union européenne / Etats-Unis
- Quelles garanties ?
- Quelle réelle efficacité ?

Relations Union européenne / Etats-Unis

- groupes de travail pour concilier la législation européenne et la législation américaine.
- Safe Harbour = minimum requis pour protéger les renseignements personnels issus de l'UE.
- Ce sont les entreprises et les organisations américaines qui s'engagent à respecter cet accord.
- Comme il constitue un minimum, elles sont libres d'ajouter des conditions de protections supplémentaires mais ne peuvent pas en enlever.

Garanties (1/3)

- **Notification** : Obligation du responsable du traitement d'informer préalablement la personne concernée des raisons de la collecte et de l'utilisation des renseignements , des tiers qui y auront accès et des droits qui lui seront reconnus (→transparence et accès suffisant)

- **Choix** : choix de l'opt-out dans le Safe Harbour. Autrement dit, possibilité pour la personne concernée de demander que cesse le traitement de ses renseignements pour les fins mentionnées lors de la collecte

- **Intégrité des données** : pertinence des données collectées par rapport à l'objet du traitement

Garanties (2/3)

- **Transfert ultérieur** : le tiers destinataire doit souscrire aux principes du Safe Harbour ou à la directive (ou autre mécanisme attestant le niveau adéquat de la protection) ou a conclu un accord dans lequel il s'engage à assurer au moins ce niveau (remarque : c'est au responsable du traitement de le certifier et non pas au tiers)

- **Sécurité** : le responsable du traitement doit prendre les mesures nécessaires pour éviter la perte, l'utilisation abusive, les consultations illicites, la divulgation, les modifications et la destruction des données

- **Accès** : droit d'accès à leurs données, pouvoir les corriger, les modifier ou les supprimer si elles sont inexactes sauf si leur demande est disproportionnée

Garanties (3/3)

- **Droit de recours et sanctions** du responsable du traitement qui n'a pas appliqué ces principes

- **Volontariat** : déclaration publique et contrôle par la Federal Trade Commission

- **Pouvoirs de la Federal Trade Commission** :

- ordonnance de cessation
- prescriptions administratives si non respect persiste
- astreintes

Efficacité ?

- Application limitée :

  -source d'hétérogénéité au sein même des Etats-Unis (entreprises qui l'adoptent et d'autres pas)

  -dérogations possibles qui peuvent être dangereuses pour la protection des données

  -recours aux clauses contractuelles

- Une certaine influence : sensibilisation des entreprises et organisations américaines sur le sujet de protection des données personnelles

Bibliographie sur le Safe Harbor

- Cynthia Chassigneux « Aterritorialité des atteintes face aux logiques territoriales de protection juridique et problème de l'absence d'homogénéité des législations protectrices » Lex electronica, vol.9, n°2, Numéro spécial, hiver 2004 http://www.lex-electronica.org/articles/v9-2/chassigneux.htm

- Joëlle Béderère « L'accord Safe Harbor relatif aux flux transfrontières de données de l'Union européenne vers les États-Unis » Mémoire de DEA informatique et droit, disponible sur www.droit-ntic.com

- Julien Le Clainche « La protection des données nominatives personnelles nominatives dans le cadre de la recherche dans le domaine de la santé » Mémoire de DEA informatique et droit, disponible sur www.droit-ntic.com