La protection des données personnelles dans la recherche en informatique

Aspects juridiques et rôle de la CNIL

Cas particulier du monde de la recherche

SEMINAIRE CNIL- INRIA - 19-20 novembre 2014

La protection des données personnelles: les 4 piliers

- En Europe un droit fondamental et une **régulation par la loi**
  - **Des droits sur ses données**
  - **Des règles de bon usage**
  - **Une autorité de contrôle indépendante**
  - **Des sanctions** en cas de non respect des règles

- Dans le monde, une disparité de situations…

La protection des données personnelles en Europe et en France

- La directive européenne du 24 octobre 1995 : en cours de révision
- La loi informatique et libertés du 6 janvier 1978 modifiée en 2004:une éthique de l'informatique appliquée aux données personnelles
- La CNIL, une autorité administrative indépendante

La CNIL en bref

- Une autorité administrative indépendante
  - 17 membres + le défenseur des droits
  - Services: 180 personnes
  - Budget 2014: 17 millions d'euros
- Une triple mission
  - Information, conseil, concertation (partenariats), conformité (packs), éducation (www.educnum.fr), cnil lab
  - Contrôle : déclarations et contrôles sur place et en ligne
  - Sanction en cas de non-respect de la loi

2013

- *90 000 déclarations*
- *Correspondants informatique et libertés: 13 000 organismes*
- *200 interventions, 29 labels, guides pratiques, tutoriels vide http://www.cnil.fr/les-themes/securite/*
- *Plus de 5600 plaintes*
- *+ de 400 contrôles*
- *57 mises en demeure; 14 sanctions dont 7 financière*

1. RAPPEL DES NOTIONS CLES « INFORMATIQUE ET LIBERTES »
2. LES PRINCIPES DE PROTECTION DES DONNEES ET LEUR APPLICATION A LA RECHERCHE
3. FORMALITES ET CIL
4. QUELLES EVOLUTIONS POSSIBLES

1
Les notions clés « Informatique et Libertés »

1. Donnée à caractère personnel: définitions

Directive européenne de 1995

« ***toute information concernant une personne identifiée ou identifiable*** *; 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 ;* (…) *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* » (considérant 26 et article 2)

Loi « Informatique et Libertés »

« 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 » (article 2)

Donnée à caractère personnel: une notion large

Toute information relative à une **personne physique** identifiée ou identifiable, **directement ou indirectement** par référence à un numéro d'identification ou un ou plusieurs éléments spécifiques ou par recoupement

CNIL

La donnée à caractère personnel selon la CNIL

Une interprétation large et une appréciation au cas par cas :

/ nature des données:

- Données relatives à l'état civil: noms et prénoms
- Données se rapportant indirectement à l'etat civil :ex. initiales des noms et prénoms, date et lieu de naissance, n° de SS…
- Données de localisation spatiotemporelle: commune de résidence, lieu de travail, données de geolocalisation, indications de dates (d'examens, d'hospitalisation, …)
- Données spécifiques, cas isolés (pathologies rares, nature d'emploi…)
- Numéros de tel, de CB, numéros aléatoires renvoyant à une liste de correspondance avec identités
- Données biometriques, photos, voix…
- Données techniques : adresse ip, adresse mac,, données de connexion metadonnées, …
- **Données du web social**

/ l'importance relative de l'échantillon de population concernée;

/ le type de traitement effectué : ex. data mining, big data.

Exemples d' études « faussement » anonymes

- **collectes de données présentant un caractère indirectement identifiant**
  - cas des questionnaires en ligne avec enregistrement des données de connexion (identifiant/mot de passe, adresse IP), ou des entretiens de visu avec enregistrement visuel et/ou sonore
- **collecte de données pouvant être rattachées à des personnes déterminées, par recoupement/combinaison**
  - soit des réponses fournies entre elles
    - cas des questionnaires distribués aléatoirement dans la rue et sollicitant des données nombreuses et précises sur les répondants
  - soit de celles-ci avec une ou plusieurs caractéristiques prédéterminées des répondants
    - cas des questionnaires adressé à un groupe de personnes préidentifiées et susceptibles d'être individualisées

2. Le traitement: un champ très large

Toute opération ou tout ensemble d'opérations portant sur des données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, le verrouillage, l'effacement ou la destruction.

✓Bases de données, dispositifs biométriques, réseaux sociaux, applications mobiles…

Comment repérer et délimiter un traitement ?

Comment raisonner?

- par finalité principale et/ou sous-finalités ?
- par opération spécifique ou fichier/logiciel utilisé ?

Pour les structures/laboratoires de recherche, 2 grandes catégories :

1. **Traitements liés à leur fonctionnement :** gestion RH (cf. la norme simplifiée n° 46) ; gestion administrative, financière et comptable ; sécurité des locaux (ex. : vidéosurveillance, contrôle d'accès par badge) ; etc.
2. **Traitements liés à leurs missions :** tous ceux effectués dans le cadre des travaux de recherche , de leur accompagnement et de leur valorisation

3. Responsable de traitement

« Sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités, et ses moyens »

↳ **sauf délégation de pouvoir, c'est en principe au représentant légal de l'organisme pour le compte duquel le traitement est mis en œuvre de veiller au respect des dispositions de la loi « I&L »** ➔président / directeur / de l'établissement d'enseignement supérieur, de l'organisme de recherche ou de la structure privée concerné.

↳**ATTENTION ! L'utilisation de fichiers préexistants (cf. collecte indirecte des données) ne décharge pas le réutilisateur de sa responsabilité « IL »** : le réutilisateur est responsable d'un nouveau traitement, dont il va définir la finalité et les moyens.

↳ De même, **en cas de recours à un « sous-traitant »** [art. 35 LIL] : **pas de transfert de responsabilité vers la personne qui traite les données pour le compte et sous l'autorité du RT** => tout « prestataire de service » doit agir sur instruction du RT et présenter des garanties suffisantes pour assurer sécurité et confidentialité des DCP.[cf. fiche pratique « sous-traitance » sur www.cnil.fr]

↳**Cas des « structures fédératives/associées », de type unités mixtes de recherche (UMR), des partenariats, consortiums: à discuter:**

Responsable de traitement: cas pratiques à discuter

- **Cas des traitements de recherche intervenant à l'issue d'un marché public ou d'un appel à projet** ➔ généralement, 2 hypothèses:

❑ 1ère hypothèse : le commanditaire = le RT (l'attributaire = le « sous-traitant »)

❑ 2nde hypothèse : l'organisme retenu = RT, compte tenu du faible niveau d'instruction et de contrôle dont va faire preuve le commanditaire

- **Cas des traitements de recherche intégrés dans un projet collaboratif, impliquant différents partenaires** ➔ 2 cas de figure :

❑ si le projet peut être fragmenté en différentes « briques » : chaque acteur = RT de la partie qu'il lui revient de mettre en œuvre

❑ si les briques sont interdépendantes : le RT pour l'ensemble du projet doit être désigné entre les partenaires

↳ Exemples: mobilitics - xdata…

Localisation du responsable de traitement

- **Application de la loi « IL » assujettie à un critère de localisation géographique** ➔ ne concerne que les traitements :

  ✓ dont le responsable est établi, de manière stable, sur le territoire français (filiale, succursale, voire bureau de représentation)

  ✓ **OU** dont le responsable est établi en dehors de l'UE mais recourt à des moyens de traitement situés sur le territoire français

- **En pratique, la loi IL française s'applique** :

  ✓ si le RT est un organisme américain ayant recours à un Data Center situé en France (si RT est allemand, application de la loi allemande)

  ✓ si le RT est un organisme français ayant recours à un « sous-traitant » situé en Chine

- **Cf. le** guide des transferts de données hors UE, sur le site de la CNIL

2
Les 5 règles d'or de la protection des données

Les règles de la protection des données

Finalité

Les données ne sont recueillies et traitées que pour un usage déterminé et légitime, préalablement défini

Tout détournement de finalité est passible de sanctions pénales

Proportionnalité et pertinence

Seules les informations pertinentes et nécessaires au regard des objectifs poursuivis doivent être traitées

Durée limitée de conservation

Les informations ne peuvent être conservées de façon indéfinie

Une durée de conservation précise doit être fixée en fonction de la finalité du traitement

Sécurité et confidentialité

Le responsable du traitement doit prendre les mesures nécessaires pour garantir la sécurité et la confidentialité des données

Les données peuvent néanmoins être communiquées à des « Tiers autorisés »

Respect des droits des personnes

Les personnes dont les données sont utilisées dans un traitement ont un droit d'information, d'accès, de rectification, de suppression et d'opposition/ consentement sur leurs données

CNIL

1. Finalité du traitement

- **PRINCIPE**

> Les données « sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités » (art 6)

- **Pierre angulaire de la législation I&L** :
  - fait le lien entre les données, les traitements et les missions de l'organisme qui les met en oeuvre
  - déclaration des traitements par finalité et non par logiciel/fichier utilisé
  - va permettre de déterminer les catégories de données susceptibles d'être traitées et leur durée de conservation

- **A retenir** :

« Un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données :

  - *s'il est réalisé dans le respect des principes et des procédures prévus* (par la loi)
  - *s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées »*

➔ **Quelles limites « éthiques » à la recherche ?**

2. Pertinence et proportionnalité des données

• **PRINCIPE**

Les données doivent être ***« adéquates, pertinentes et non excessives*** *au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs » (art 6 al.3)*

➔ **protection particulière accordée à certaines catégories de données**

✓Données dites « sensibles » :

- Origines raciales ou ethniques
- Opinions politiques, philosophiques ou religieuses, appartenances syndicales
- Données relatives à la santé ou à la vie sexuelle

✓Données relatives aux infractions, condamnations et mesures de sûreté

✓Numéro de sécurité sociale (NIR)

✓Données comportant des appréciations sur les difficultés sociales des personnes

✓Données biométriques

3. Conservation limitée des données

Principe 1

Les données « *sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* »

Principe 2

Les données « *ne peuvent être conservées au-delà de la cette durée qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-4 du Code du patrimoine* »

➢ **En pratique, effacement ou anonymisation des données à l'issue de cette durée, ou archivage**

4. Obligation de sécurité

PRINCIPE (art. 34) :

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »

2 volets : respect de l'intégrité et de la confidentialité des données

cf. les 3 guides de la CNIL sur la sécurité des données personnelles (méthodologie pour appréhender les risques « vie privée » et catalogue de mesures) :

- Réalisation d'une analyse des risques et adoption de mesures de sécurité physique et logique
- Gestion des habilitations et traçabilité des accès des utilisateurs
- Identification des destinataires des données
- Le cas des sous-traitants
- Le cas des tiers autorisés (police judiciaire, administration fiscale, …)

En matière de recherche statistique/scientifique, veiller à garantir l'anonymat des données diffusées

5. Respect des droits des personnes

- Droit à l'information
- Droit d'opposition/consentement
- Droit d'accès, rectification, suppression

5. Droit à l'information

Il faut une information sur :

1. l'identité du responsable du traitement
2. la finalité du traitement
3. le caractère obligatoire ou facultatif des réponses
4. les conséquences d'un défaut de réponse
5. les destinataires des données
6. les modalités d'exercice de leurs droits

• **Dérogations:**

- traitements nécessaires à la conservation des données à des fins historiques, statistiques ou scientifiques, ou à la réutilisation de ces données à des fins statistiques par l'INSEE et les SSM
- personnes concernées déjà informées
- information se révélant impossible ou exigeant des efforts disproportionnés par rapport à l'intérêt de la démarche

5. Droit d'opposition/consentement

• **Principe :**

Toute personne a le droit de s'opposer, pour des motifs légitimes, au traitement de ses données, sauf exceptions

➔ cas des « enquêtes obligatoires » agréées par le CNIS et ayant reçu le visa des ministres compétents

➔ pour les autres, nécessité d'informer les personnes du caractère facultatif des réponses

• **Dans certains cas, il est nécessaire de recueillir un consentement explicite (case à cocher « j'accepte »)**

➔ en particulier pour traiter des données sensibles (sauf autres exceptions prévues à l'art. 8 de la loi « I&L »)

5. Droits d'accès et de rectification

- **Principe :**

Toute personne peut, directement auprès du responsable des traitements, avoir accès à l'ensemble des informations la concernant, en obtenir la copie et exiger qu'elles soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées

- **Dérogation possible:**

Ce droit peut être exclu lorsque les données sont conservées *« sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherches scientifiques ou historiques »*

3
Formalités préalables applicables et CIL

Déclarations, exonérations et dispenses

Les traitements hors du champ de la loi/exonérés de déclaration par la loi

fichiers de personnes morales, traitements dans le cadre d'activités exclusivement personnelles (ex. agendas)
fichiers des membres des partis politiques, syndicats et églises

Les fichiers dispensés de déclaration par la CNIL

paie , fichiers de fournisseurs, information et communication externes, …

Les traitements courants soumis à déclaration, sauf CIL

gestion RH, fichiers clients, **recherches hors données sensibles**…

Les traitements à risque soumis à autorisation ou avis de la CNIL

traitements de données sensibles (y compris à des fins de recherche), dispositifs biometriques, fichiers de police, téléservices, interconnexions sous certaines conditions

- Les packs de conformité

Le correspondant Informatique et Libertés

- Une désignation **facultative**, notifiée à la CNIL
- **dispense des déclarations courantes** (normales et simplifiées) mais tenue par le CIL d'un registre des traitements
- Assure une meilleure application de la loi (culture informatique et libertés), contacts privilégiés avec la CNIL (ateliers de formation, service dédié,…)
- CIL INRIA: Didier.Benza@inria.fr

En résumé les spécificités « recherche »…

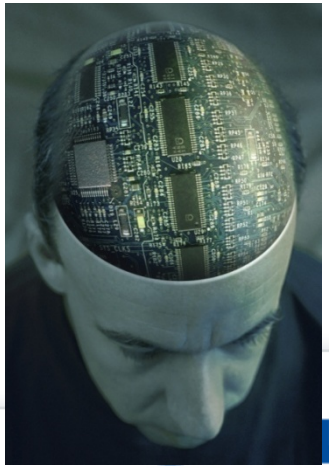
- Finalités: les exceptions recherche et statistiques
- Des dérogations possibles pour les données sensibles
- Conservation à des fins historiques, statistiques ou scientifiques
- Droits des personnes: des dérogations et aménagements possibles en cas de réutilisation des données à des fins statistiques
- Sécurité et anonymat - cloud

Recherche et statistiques: elements de réflexion - vers un encadrement spécifique?

- La question de la définition du champ?
- Données pseudonymisées = cadre allégé?
- La question du big data
- Données du web social et loyauté de la collecte
- Quels contrôles sur les traitements de recherche et par qui?
- Quelles dérogations et quelles contreparties?

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

- du tout numérique,
- des modèles économiques du numérique
- et de la globalisation,
- de l'évolution des usages et des comportements
- de la sécurité…



Quels impacts…

- 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 lourdes et coûteuses
- La marchandisation des données
- Vie privée - vie publique: où est la frontière?

Le futur règlement européen: les orientations

- 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
- 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

Renforcer les droits des personnes

- Renforcement du consentement des personnes et du droit d'opposition
  - consentement explicite (déclaration ou acte positif univoque) et non présumé. .
- Reconnaissance d'un «droit à l'oubli numérique»
  - droit à l'oubli consacré : suppression des données si aucun motif légitime ne justifie leur conservation. Cf arrêt CJUE 13 mai 2014
  - réaffirmation notamment des obligations en matière de limitation de conservation des données et du droit d'effacement des données.
- Reconnaissance d'un droit à la portabilité
  - droit d'obtenir communication des données d'un système de traitement à un autre;
  - sans que le responsable de traitement puisse s'y opposer et ce dans un format standard.
- Renforcement des obligations générales d'information: transparence
  - Outre les mentions existantes, information sur la durée de conservation, le droit d'effacement, et le cas échant , sur la perte de données personnelles…
  - Possibilité d'engager des actions collectives

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

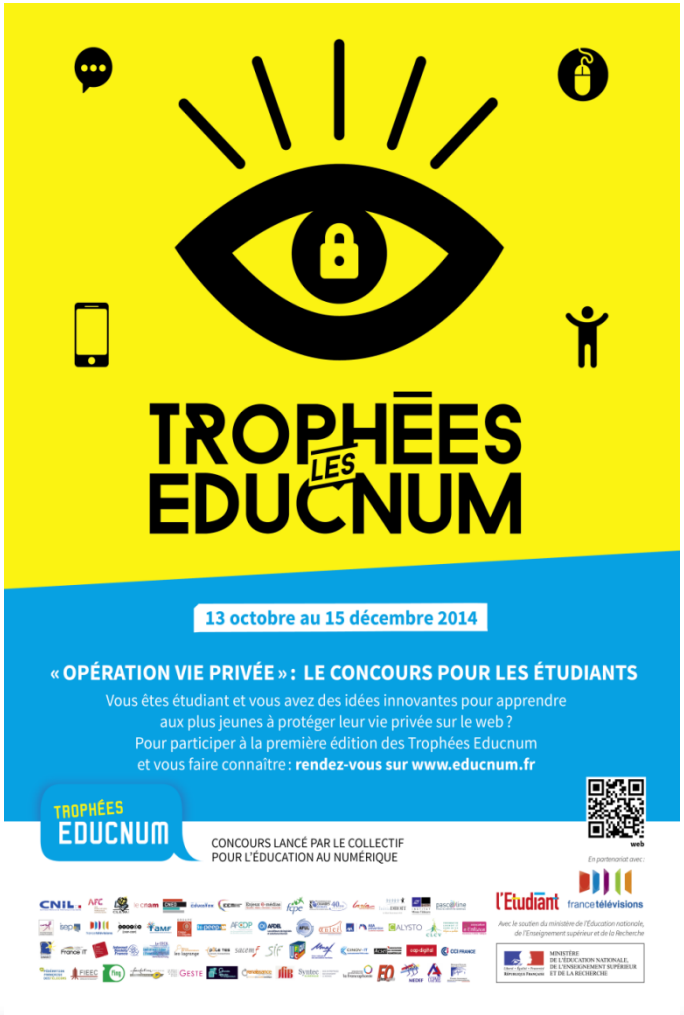
La contrepartie: des formalités administratives allégées…

- **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**
  - l'évaluation systématique et à grande échelle des aspects personnels propres à une personne physique ou visant à analyser ou à prévoir, en particulier, la situation économique de ladite personne physique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement, qui est fondée sur un traitement automatisé et sur la base de laquelle sont prises des mesures produisant des effets juridiques concernant ou affectant de manière significative ladite personne
  - le traitement d'informations relatives à la vie sexuelle, à la santé, à l'origine raciale et ethnique ou destinées à la fourniture de soins de santé, à des recherches épidémiologiques ou à des études relatives à des maladies mentales ou infectieuses, lorsque les données sont traitées aux fins de l'adoption de mesures ou de décisions à grande échelle visant des personnes précises
  - la surveillance de zones accessibles au public, notamment par vidéosurveillance;
  - fichiers informatisés de grande ampleur concernant des enfants, ou traitement de données génétiques ou biométriques;
  - autres traitements inscrits sur liste établie par la CNIL .

La CNIL évolue…

- Développer la concertation (open data, vie privée 2020, droit à l'oubli…
- Accompagner l'innovation (partenariats recherche, projets big data…
- Mieux répondre aux besoins des usagers (FAQ, tutoriels, refonte du site…)
- promouvoir une démarche de conformité (labels, packs…)
- Avoir une politique de contrôles et de sanctions plus ciblée
- Contribuer à l'éducation au numérique (culture numérique)

Les trophées Educnum



Commission Nationale de l'Informatique et des Libertés

www.cnil.fr

Suivez la CNIL sur...