CNIL, MR01, MR03, hors-champ ? pourquoi, comment et questions

Jean-Marie Chrétien – DRCI CHU Angers – CIL adjoint recherche

7ème journée interrégionale du GIRCI Grand Ouest

Un peu d'histoire…

- Le Monde 21 mars 1974
  - Ministère de l'intérieur
  - 400 fichiers
  - 100 millions de fiches
  - Interconnexion !

• • • LE MONDE — 21 mars 1974 — Page 9

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une « division de l'informatique » au ministère de la justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur puissant destiné à rassembler la masse énorme des renseignements grapillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir chaque Français par un « identifiant », qui ne définisse que lui, maintenant terminé, est l'objet de convoitises ardentes; le ministère de l'intérieur y souhaite jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale.

Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique. Son importance exigerait qu'il en fût, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

« Safari » ou la chasse aux Français

Rue Jules-Breton, à Paris-13e, dans des locaux du ministre de l'intérieur, un ordinateur Iris-80 avec bi-processeur est en cours de mise en marche. A travers la France, les différents services de police détiennent, selon la confidence faite par un très haut magistrat, 100 millions de fiches, réparties dans 400 fichiers. Ainsi se trouve posées — et, à terme, théoriquement résolues — les données d'un problème comprenant, d'une part, l'énormité des renseigne-

l'origine, budgétairement, n'était pas du tout prévu pour la tâche qu'il a finalement assurée, mais pour « traiter » les données administratives du Fichier national des constructeurs (F.N.C.). Il s'agit donc apparemment d'un détournement manifeste de crédits d'études, ce qui n'était sans doute pas le vœu du Parlement qui les vota.

De vastes ambitions

Ce n'est pas, pourtant, que les avertissements aient manqué. Le Conseil d'Etat en 1970, puis le ministère de la justice en 1972 (qui avait rappelé le rôle dévolu à l'autorité judiciaire de « *gardien des libertés individuelles* » et donc réclamé voix au chapitre) ont insisté sur la nécessité d'une intervention législative qui préciserait les quelques éléments essentiels de l'emploi de l'informatique appliquée aux particuliers : réglementation de l'acces des tiers

outil, il n'apparaît pas — sauf erreurs négligeables, relativement — que l'accès des tiers ou le droit à contrôle des personnes visées — par demande d'un extrait — ait jamais provoqué des bavures préjudiciables à la légalité.

De même, le fichier national des conducteurs, dans sa partie judiciaire, est prévu par une loi, et il faut regretter que les textes d'application ait permis des illégalités injustifiables — mais connues

dite commission. D'autant qu'il est d'ores et déjà connu que M. Touffait a été rayé de la liste des « sachants ». Il semble d'ailleurs que les réactions vives qui sont enregistrées portent moins sur le renouvellement des structures, jugées inévitables, que sur la méthode « *à la hussarde* » employée par tel membre de l'entourage de M. Taittinger pour mener à bien ses projets de rénovation de la gestion dans le domaine judiciaire.

Est-ce à dire de plus que les

d'un *aggiornamento* technique, a illustré son discours par un large reportage sur les équipements du tribunal de Bobigny — plus réduits, donc plus rapides à réaliser, ainsi plus vite source d'orgueil pour leurs créateurs.

C'est donc un doute global qui pèse sur les intentions du gouvernement, en général, et du ministère de la justice, en particulier : ce dernier département, qui rappelle à tous sa mission de protection des libertés

Système **A**utomatisé pour les **F**ichiers **A**dministratifs et **R**épertoire des **I**ndividus

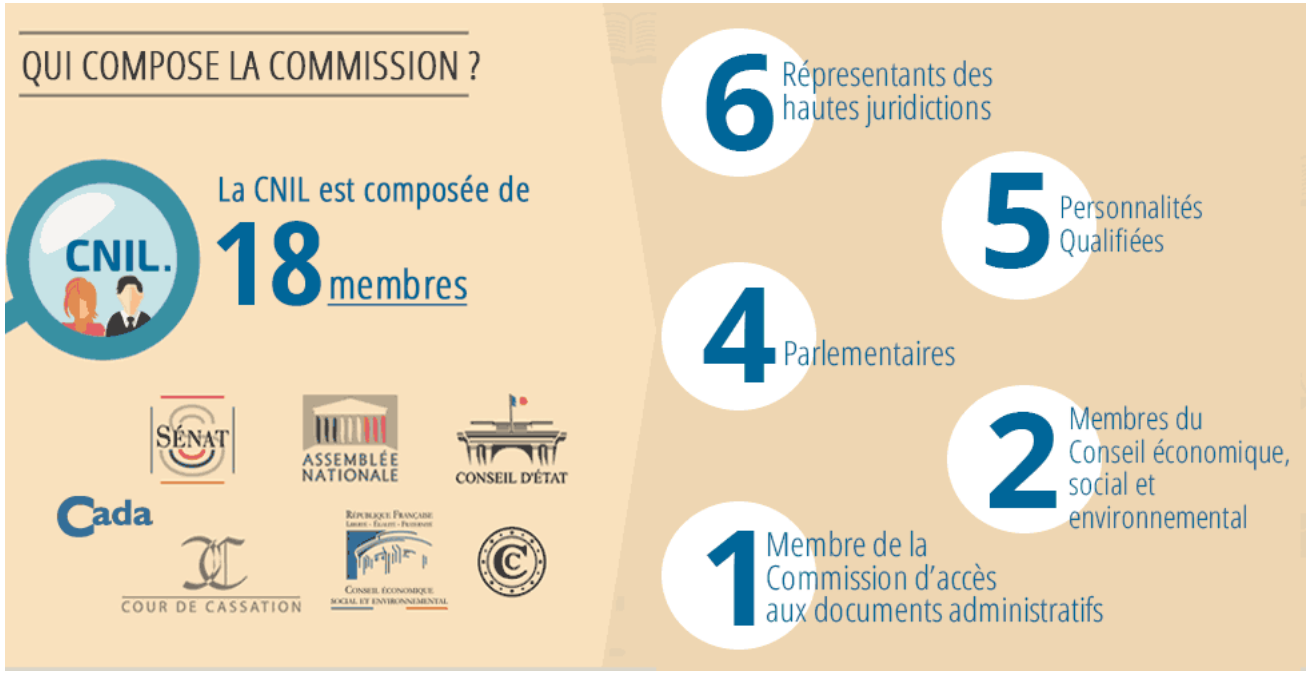
Scandale !

→ 1978 publication de la loi Informatique et Libertés et création de la CNIL

→ le projet SAFARI ne voit pas le jour

La CNIL : une autorité administrative **indépendante**

- Ne reçoit d'instruction d'aucune autorité
- Le président est élu par les membres
- 192 agents
- 5 directions
  - Direction de la conformité
    - **Secteur Santé**



Données personnelles et nominatives

- Personnelles

Les **données personnelles** correspondent à **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 (article 2 de la loi informatique et liberté)

  - Poids / Taille / Sexe
  - Age ou mois/année de naissance
  - Date d'opération
  - …

- Nominatives

Les données personnelles **permettant l'identification** sont des données **nominatives**

  - Nom, prénom
  - Adresse (physique ou électronique)
  - N° téléphone
  - Date et lieu de naissance
  - NIR
  - …

Un jeu de données sans données nominatives est-il anonyme ?

La réidentification : c'est loin d'être impossible ! Aux Etats-Unis, c'est un business.

- 87% de la population américaine est identifiable de façon unique à partir des éléments suivants
  - Code postal
  - Date de naissance
  - Sexe

Plus on dispose de données

→ plus le risque est important

For example, William Weld was governor of Massachusetts at that time and his medical records were in the GIC data. Governor Weld lived in Cambridge Massachusetts. According to the Cambridge Voter list, six people had his particular birth date; only three of them were men; and, he was the only one in his 5-digit ZIP code.

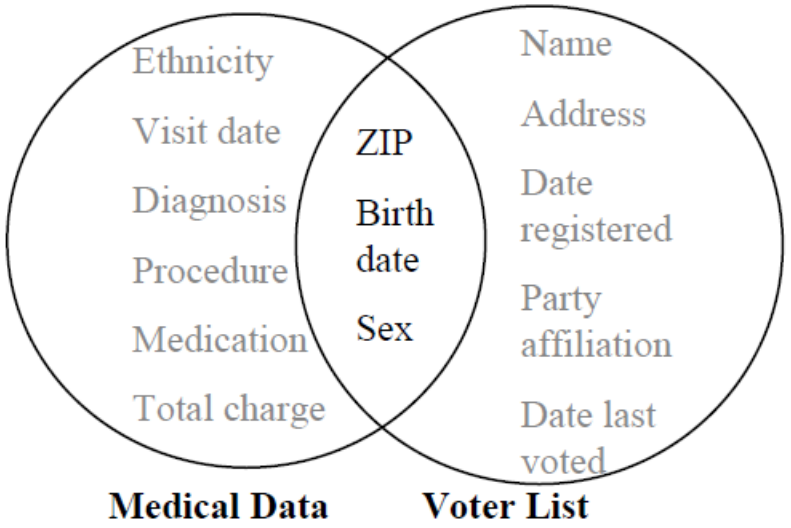


Figure 1 Linking to re-identify data

L. Sweeney. *k*-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,* 10 (5), 2002; 557-570

Les principes clés de la protection des données personnelles

- Finalité
  - Données recueillies pour un usage déterminé et légitime
- Proportionnalité et Pertinence
  - Des données nécessaires et pertinentes au regard de la finalité
- Conservation
  - Durée de conservation adaptée à la finalité (au-delà archivage, puis destruction)
- Respect des droits des personnes
  - Information, accès, opposition, oubli
- La sécurité des données
  - Logiciel, locaux, habilitations

Le régime actuel pour la recherche en santé

- Engagement de conformité à une MR (unique)
  - Le promoteur ou le gestionnaire s'engage à respecter les termes de la MR
  - A vérifier pour chaque projet
- Autorisation explicite (hors MR)
- Déclaration normale (monocentriques) → registre CIL

MR01 et MR03 : un cadre commun pour un périmètre différent ?

MR01
Consentement exprès ou écrit

- Cat 1 et 2 (ex RBM + soins courants)

MR03
Information individuelle et non opposition

- Non interventionnelles
- Evaluation des « soins courants »
- Essais en grappe

→Traçabilité de l'information

Cadre commun

- Données des patients
- Données des investigateurs
- Durée de conservation des données (avant archivage ou destruction)
- Accès aux données des patients
- Accès aux données des professionnels
- Le contenu de l'information à destination des professionnels et des patients
- Sécurité et confidentialité
- Transmission des données

- Nécessité d'une analyse des risques

MR01 et MR03 : un cadre commun

MR01
Consentement exprès ou écrit

MR03
Information individuelle et non opposition

Une même liste de catégories de données autorisées (extrait):

- Initiales 2+1 => reco 1+1
- Age ou mois/année naissance (complète possible si <2 ans et justifié)
- lieu de naissance (si justifié)
- Date relatives à la conduite de la recherche
- Origine ethnique (si justifiée)
- Données génétiques (sauf pour réidentification)
- Statut vital (lorsqu'il est disponible dans dossier)
- Données socio-économiques
- Données comportementales

Transmission sous une forme ne permettant pas l'identification **directe ou indirecte**

Données identifiantes = liste de correspondance dans les centres

Minimisation des risques de réidentification

Liste de correspondance

N°	Nom	Prénom	Date naissance	Sexe
1	Dupont	Gérard	15/09/1987	M
2	Dupond	Albert	18/02/1954	M
3	Durant	Marcelle	24/02/1968	F

Base de données

N°	Initiales	Date de naissance	Sexe	Date d'admission	Date de chirurgie
1	DG	sept-87	M	15/03/2017	18/03/2017
2	DA	févr-54	M	18/04/2017	19/04/2017
3	DM	févr-68	F	19/04/2017	22/04/2017

Données transmises pour analyse

N°	age à la chirurgie	sexe	Délai admission Chirurgie
1	30	M	3
2	63	M	1
3	49	F	3

Exemples de projets hors cadre

- Collection Clinico-biologique en dehors d'une RIPH
- Suivi téléphonique centralisé à 6 mois
  - Collecte centralisée de données identifiantes
- Demande de dérogation à l'obligation d'information
  - Suivi d'une cohorte de patients cancéreux
- Appariement avec données type PMSI/SNIIRAM

Hors cadre → autorisation Recherche
Les délais de réponse n'ont pas raccourcis !

MR03 : un périmètre qui doit encore évoluer

- Etudes multicentriques sur données ?
  - Position CCTIRS → MR03
  - Position CNIL ?
  - Procédure CEREES ?
  - Pas de liste de correspondance ou liste conservée le temps de la collecte des données → déclaration ? normale ? qui ?

- Etudes d'évaluation des soins/pratiques ?
  - Retiré de la Cat 2 depuis mai/2017
  - Multicentrique sur données ?

MR03 : conservation des données et droit d'opposition (idem MR01)

Les données des patients peuvent être conservées jusqu'à la mise sur le marché du produit étudié ou jusqu'au rapport final de la recherche ou jusqu'à la publication des résultats de la recherche.

Les données des professionnels de santé intervenant dans la recherche peuvent être conservées pendant cinq ans après la fin de la dernière recherche à laquelle ils ont participé.

Elles font ensuite l'objet d'un archivage sur support papier ou informatique pour une durée conforme à la réglementation en vigueur.

→ Tous les types d'études n'ont pas une durée d'archivage définie

→ Comment gérer les demandes d'opposition et d'accès aux données enregistrées si les données n'existent plus ? A préciser dans information ?

Des questions ?