CONFERENCE DE PRINTEMPS
DES COMMISSAIRES A LA PROTECTION DES DONNEES

SEVILLE – 3 et 4 avril 2003

M. Michel Gentot, président de la Commission nationale de l'informatique et des libertés (CNIL), Paris

La CNIL et les fichiers de sécurité publique

Parmi les missions dont l'autorité française de protection des données est investie, il en est une aussi délicate qu'importante : le contrôle des fichiers de sécurité publique. Cette mission est en effet la « pierre de touche » de l'indépendance de l'autorité et la mesure de la soumission de l'Etat au droit commun.

Le contrôle des fichiers de police comporte deux aspects : le contrôle a priori et le contrôle a posteriori. Encadrer les conditions de fonctionnement des fichiers de police dans des conditions qui assurent un équilibre satisfaisant entre la liberté individuelle et l'efficacité des enquêtes. Surveiller la mise en œuvre des règles ainsi définies en donnant aux individus, autant que la sécurité publique le permet, un accès aux informations détenues sur eux. Tels sont les objectifs de la CNIL.

Atteindre ces objectifs est un combat permanent et encore inachevé. Deux exemples récents peuvent être cités : c'est en décembre dernier que la gendarmerie nationale s'est décidée à présenter à la CNIL un projet de création de son fichier d'enquêtes judiciaires (JUDEX), fichier dont la CNIL a de bonnes raisons de savoir qu'il fonctionnait depuis de nombreuses années. Autre exemple : un décret de juillet 2001 prévoit que les personnes figurant dans le fichier de police judiciaire de la police nationale (STIC) peuvent avoir connaissance, dans certains cas, du contenu de leur fiche. A l'heure qu'il est la CNIL attend toujours la mise en place du dispositif de consultation promis par le ministère de l'intérieur.

Le présent exposé a pour objet de décrire sommairement l'action de la CNIL, à la fois historique et quotidienne, dans ce double champ du contrôle a priori et du contrôle a posteriori des fichiers qu'on appelle souvent de « souveraineté ».

I. – LE CONTROLE A PRIORI DES FICHIERS DE SECURITE PUBLIQUE

La promulgation de la loi du 6 janvier 1978 a « fait sortir de l'ombre » les fichiers utilisés quotidiennement par la police dans l'exercice de ses missions et a conduit la CNIL, saisie de demandes d'autorisation au gré de la bonne volonté des gouvernements, à préciser sa doctrine en matière des garanties devant entourer la création et l'utilisation des fichiers de police.

1) Les fichiers de travail de la police judiciaire (STIC et JUDEX)

Créé après bien des vicissitudes par un décret du 5 juillet 2001, le **S**ystème de **T**raitements des **I**nfractions **C**onstatées (STIC) mis en œuvre par le ministère de l'Intérieur a une double finalité : faciliter la recherche des auteurs d'infractions et réaliser des statistiques.

Ce fichier recense les informations recueillies par les fonctionnaires de la police nationale dans le cadre des enquêtes concernant les crimes, délits et quelques contraventions. Il recense aussi bien des informations concernant les personnes mises en cause que les victimes et ne comporte pas, sauf exception, la suite judiciaire des procédures concernées.

À l'occasion de l'examen du STIC, la Commission a mis en exergue les garanties qui lui semblaient devoir nécessairement entourer l'utilisation de ce fichier :

- un encadrement strict de la finalité du STIC : seule la fiche STIC relative à l'affaire jugée doit apparaître dans le dossier et le STIC.
- une définition rigoureuse des personnes mises en cause, par référence aux dispositions du code de procédure pénale ;
- la reconnaissance, pour les victimes d'un droit d'opposition à voir des informations les concernant figurer dans le STIC une fois l'auteur des faits condamné de façon définitive ;
- un renforcement du contrôle du procureur de la République : une copie de la fiche STIC est systématiquement jointe au dossier de procédure ;
- un encadrement précis des cas de collectes de données sensibles : uniquement si elles résultent de la nature ou des circonstances de l'infraction ;
- une mise à jour plus rigoureuse : effacement en cas de relaxe, acquittement, non-lieu, amnistie ; mise à jour en cas de décision de classement suite pour insuffisance de charges ; les intéressés peuvent également demander la substitution de la qualification des faits lorsque celle-ci a évolué au cours de la procédure ;
- le choix de durées de conservation plus adaptées : cinq années de principe pour les mis en cause mineurs, vingt ans pour les mises en cause majeurs ; effacement en tout état de cause au 75^{e} anniversaire du mis en cause ;
- une procédure de droit d'accès indirect aménagée permettant, sous certaines conditions, la communication des informations à la personne concernée.

Le fichier JUDEX lui, est le pendant du STIC pour la gendarmerie nationale. La Commission a émis, en janvier 2003, un avis favorable au décret portant création – en réalité régularisant ce fichier - en réaffirmant certains points de sa doctrine en matière de fichiers de police.

Comme la CNIL l'avait souhaitée elle-même, une loi est venue récemment consacrer l'existence des fichiers de police judiciaire (loi du 18 mars 2003) et par là même une partie des garanties que la CNIL avait définies, non sans un travail d'explication intense en direction du Gouvernement et des parlementaires. Nous n'avons cependant pas été entendus sur un point majeur : l'utilisation des ces fichiers dans des enquêtes administratives, telles que celles menées lors d'un recrutement dans certains emplois publics, de l'attribution d'un titre de séjour ou d'une décoration. Nous avons vu dans cette mesure, déjà introduite partiellement au lendemain du 11 septembre 2001 et largement étendue par cette loi, une réelle atteinte aux principes du secret de l'instruction et de la présomption d'innocence, sans compter un détournement de la finalité première de ces fichiers conçus pour faciliter les investigations criminelles et non servir de casier judiciaire, c'est à dire de mémoire des infractions pénales.

Pour être tout à fait honnête il faut préciser que le juge constitutionnel n'y a rien trouvé à redire.

2) Le fichier national automatisé des empreintes génétiques (FNAEG)

Le premier fichier national d'empreintes génétiques en matière criminelle et concernant uniquement les personnes condamnées pour des infractions à caractère sexuel, a été soumis à la Commission, en juillet 1999, qui a insisté notamment pour que les analyses destinées à l'identification ne portent sur des segments d'ADN « non codants », c'est-à-dire ne permettant pas de déterminer les caractéristiques des personnes concernées, à l'exception de leur sexe.

Cette première ébauche de fichier a été étendue en 2001 et dernièrement par la loi déjà citée du 18 mars 2003 sur la sécurité intérieure. La liste des infractions pénales pouvant donner lieu, pour les personnes condamnées définitivement, à enregistrement dans le fichier de l'ADN a ainsi été élargie à deux reprises mais surtout, avec la loi de mars 2003, est autorisé l'enregistrement des empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves ou concordants qu'elles aient commis l'une des infractions pouvant donner lieu à enregistrement. Ce d'autant que cet enregistrement est désormais possible sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction.

Nous avons considéré, dans notre avis sur le projet de loi sur la sécurité intérieure que cette extension modifiait profondément la nature même de ce fichier et impliquait en conséquence l'adoption de garanties nouvelles s'agissant tout particulièrement de ses modalités d'alimentation comme des règles de conservation et d'effacement des informations nominatives traitées.

3) Le fichier des véhicules volés (FVV) et le fichier des personnes recherchées (FPR)

Deux autres fichiers méritent d'être cités pour mémoire mais posent moins de problèmes.

Créé en 1996, le fichier des véhicules volés, mis en œuvre à la fois par le ministère de l'Intérieur et par celui de la Défense a pour finalité, comme le STIC et JUDEX, de faciliter les recherches de la police et de la gendarmerie pour la découverte et la restitution des véhicules volés, la surveillance des véhicules signalés dans le cadre de leurs missions répressives ou préventives et la recherche et la surveillance des personnes susceptibles d'utiliser un véhicule volé ou signalé.

Le fichier des personnes recherchées a pour objet de faciliter les recherches des autorités judiciaires, administratives ou militaires s'agissant, par exemple, des personnes recherchées dans le cadre d'une enquête judiciaire, des personnes condamnées n'ayant pas exécuté la décision rendue à leur encontre, les évadés, déserteurs et insoumis, les personnes frappées par une mesure d'interdiction de séjour ou une mesure d'expulsion comme les personnes disparues ou les malades mentaux devant faire l'objet d'un placement d'office.

4) Les fichiers de services des Renseignements Généraux

Dans le cadre de ses missions, la direction des renseignements généraux (DCRG) met en œuvre un fichier recensant des personnes physiques subdivisé en trois applications :

- le fichier « terrorisme » qui centralise les informations concernant les personnes susceptibles de porter atteinte à la sûreté de l'Etat ou à la sécurité publique par leurs agissements ou leur appartenance à un groupement dont l'activité est de nature à troubler l'ordre public ;
- le fichier « habilitation » qui centralise les informations concernant les personnes faisant l'objet d'une enquête dans le cadre des procédures d'habilitation secret défense ;
- le fichier « dossier départemental » qui centralise les informations concernant les personnes exerçant une influence sur les situations politiques, économiques ou sociales et dont la connaissance peut permettre au gouvernement d'apprécier ces situations, sous réserve que les informations collectées et conservées soient en rapport direct avec les responsabilités publiques de ces personnes.

Lors de procédure tumultueuse d'examen des textes réglementant ces fichiers en 1991, la CNIL a obtenu un certain nombre d'améliorations dans l'alimentation et l'accès à ces fichiers :

- les antécédents judiciaires des personnes ayant bénéficié d'une décision de non-lieu, de relaxe ou d'acquittement ne figureront plus dans le fichier central du terrorisme ;
- la DCRG s'est engagée à publier annuellement un état de ses fichiers et une mise à jour des fichiers sera effectuée « selon une procédure contrôlée par la CNIL » ;
- la possibilité d'obtenir communication des informations figurant dans ces fichiers par l'intermédiaire du droit d'accès, comme cela sera expliqué ultérieurement.

5) Le système d'information Schengen (SIS)

Il n'est cité ici que pour mémoire. Chacun en connaît bien les caractéristiques de ce système qui comprend une partie nationale.

On pourrait enfin citer les fichiers des services dits « secrets » que sont la direction de la surveillance du territoire, la direction de la protection de la sécurité de la défense et la direction générale de la sécurité extérieure. La CNIL les connaît et les contrôle.

II. – LE CONTROLE A POSTERIORI : LE DROIT D'ACCÈS INDIRECT

La CNIL a le droit et le devoir d'effectuer des contrôles d'ensemble des fichiers de sécurité. C'est ainsi qu'elle a procédé au cours des années 1998-99 à un contrôle général des fichiers des services des Renseignements généraux, comme elle a l'obligation de le faire tous les cinq ans. Toutefois il apparaît que c'est en répondant aux demandes individuelles, de plus en plus nombreuses, d'accès aux fichiers que la CNIL opère un contrôle à la fois permanent et qu'on pourrait qualifier de très efficace s'il n'était terni par la longueur des délais dans lesquels il est mené (plusieurs mois entre la demande d'accès et la vérification).

En application des articles 39 et 45 de la loi du 6 janvier 1978, toute personne a le droit de demander que la CNIL vérifie les renseignements la concernant pouvant figurer dans des traitements automatisés et des fichiers intéressant la sûreté de l'État, la défense et la sécurité publique. Ces investigations sont effectuées par les membres de la Commission appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes.

Depuis sa création, la CNIL a reçu 7 523 demandes de droit d'accès indirect qui ont donné lieu à plus de 12 500 investigations et le nombre de ces requêtes augmente régulièrement d'une année sur l'autre. On peut même parler – ce sera un des thèmes du rapport d'activité 2002 – d'une véritable « explosion » du nombre des demandes. Pour la seule année 2002, la Commission a ainsi été saisie de 1 264 demandes (le double de l'année précédente), qui vont donner lieu à plus de 2 500 vérifications dans les mois à venir, une même requête pouvant concerner plusieurs traitements (d'ordinaire, le fichier des renseignements généraux, le N-SIS Schengen et les deux fichiers centralisés de police judiciaire – le STIC et JUDEX).

Au cours de la même année 2002, les commissaires en charge de la procédure du droit d'accès indirect ont procédé à 2 315 vérifications.

Fichiers concernés par les investigations effectuées au cours de l'année 2002

1) MINISTÈRE DE L'INTÉRIEUR	**2184**
- renseignements généraux	1012
- police judiciaire	304
- police urbaine	141
- direction de la surveillance du territoire	66
- système d'information Schengen	661
2) MINISTÈRE DE LA DÉFENSE	**129**
- gendarmerie nationale	73
- direction de la protection de la sécurité de la défense	32
- direction générale de la sécurité extérieure	24
3) MINISTÈRE DES FINANCES	**2**
- fichier national informatisé de documentation de la direction générale des douanes et droits indirects	2
TOTAL	**2315**

1) Les fichiers de police judiciaire

S'agissant des fichiers de police judiciaire et en particulier du STIC, les investigations menées ont conduit la CNIL à faire procéder dans 64 cas (sur les 175 saisines de personnes réellement fichées, soit 37 %) à des mises à jour, voire à la suppression de signalements erronés ou manifestement non justifiés.

Quelques exemples de signalements erronés ou non justifiés

Ainsi, un requérant s'est vu refuser un stage dans une juridiction parce qu'il était signalé dans le STIC comme « mis en cause » dans une affaire de vol de cyclomoteur alors même que, aux termes des durées de conservation fixées par le décret du 5 juillet 2001 portant création de ce fichier, ces informations n'auraient plus dû figurer dans le traitement. Les commissaires de la CNIL en charge du droit d'accès indirect ont en conséquence demandé aux services de police judiciaire de supprimer la fiche correspondante ; ces derniers en ont avisé le procureur de la République de la juridiction concernée afin que la candidature du requérant soit réexaminée.

De même, un requérant était signalé dans le STIC à la suite de sa garde à vue, en tant que témoin, dans une enquête concernant une affaire de trafic de fausse monnaie datant de 1984. À la demande des magistrats de la CNIL, les services de police judiciaire ont procédé à la suppression de la fiche de l'intéressé.

Un autre requérant, qui avait déposé une plainte contre une banque, était signalé dans le STIC comme auteur d'une dénonciation calomnieuse à la suite de « l'interprétation » par un enquêteur de sa démarche. Sa fiche a donc été supprimée à l'occasion de l'exercice du droit d'accès indirect.

2) Les fichiers des renseignements généraux

Le décret du 14 octobre 1991 a fixé, de manière exemplaire, les modalités particulières d'exercice du droit d'accès aux fichiers des renseignements généraux. Il prévoit notamment que les membres de la CNIL chargés du droit d'accès indirect peuvent, en accord avec le ministre de l'Intérieur, constater que certaines informations figurant dans les fichiers ne mettent pas en cause la sûreté de l'État, la défense ou la sécurité publique et peuvent donc être communiquées au requérant.

En pratique, trois situations peuvent se présenter :

- si les renseignements généraux ne détiennent aucune information concernant un requérant, la CNIL en informe alors ce dernier, avec l'accord du ministre de l'Intérieur ;
- si les renseignements généraux disposent d'informations sur un requérant ne mettant pas en cause la sûreté de l'État, la défense ou la sécurité publique, elles lui sont communiquées, avec l'accord avec le ministre de l'Intérieur ;
- si la communication de ces informations à l'intéressé est de nature à nuire à la sûreté de l'État, la défense ou la sécurité publique, un membre de la CNIL procède à l'examen du dossier et, s'il y a lieu, exerce le droit de rectification ou d'effacement des données inexactes ou des données dont la collecte est interdite par la loi. Le président de la CNIL adresse ensuite au requérant une lettre lui indiquant, conformément aux termes de l'article 39 de la loi du 6 janvier 1978, qu'il a été procédé aux vérifications et les voies de recours contentieux qui lui sont ouverts.

La Commission a procédé, en 2002, a plus de mille investigations auprès des services des renseignements généraux. Seules 236 personnes étaient réellement fichées. On trouvera ci-dessous le résultat des investigations concernant ces personnes.

Résultats des investigations	Requérants fichés	En pourcentage
- dossiers jugés non communicables	36	15 %
- communication refusée par le ministre de l'Intérieur	0	
- communication acceptée par le ministre de l'Intérieur	200	85 %
= communication totale = communication partielle	199 1	
Total	236	100 %

À la suite de ces communications, quinze requérants ont rédigé une note d'observation qui a été insérée dans le dossier des renseignements généraux les concernant et il a été procédé à la suppression partielle de cinq dossiers et à la suppression totale de huit dossiers.

3) Le système d'information Schengen

Depuis l'entrée en vigueur du décret n° 95-577 du 6 mai 1995 relatif au système informatique national du système d'information Schengen dénommé N-SIS, la CNIL a reçu 1 855 demandes de droit d'accès indirect, dont 661 pour la seule année 2002.

650 requérants, sur ces 1855 demandes, étaient réellement fichés, dont 312 (48 %) par l'Allemagne, 230 (35 %) par la France et 68 (10,5 %) par la France, ces trois pays ayant procédé à 93,5 % des signalements.

À la suite aux démarches entreprises par la CNIL, 273 signalements ont été supprimés du N-SIS (42 %), dont 215 par l'Allemagne, 40 par la France, 10 par l'Italie, 4 par l'Espagne, 3 par les Pays-Bas, 1 par la Belgique.

Tels sont les éléments que la CNIL souhaitait présenter pour partager, avec modestie, une expérience qui n'est pas faite que de succès et dont les résultats peuvent être remis en question à tout moment. Il s'agit ainsi de susciter un échange sur les pratiques de nos autorités de contrôle dans une Europe où la sécurité est une préoccupation assez largement commune pour ne pas dire une obsession envahissante.