COMMISSION
NATIONALE DE
L'INFORMATIQUE
ET DES LIBERTÉS

25e RAPPORT D'ACTIVITÉ 2004

prévu par l'article 11 de la loi du 6 janvier 1978,
modifiée par la loi du 6 août 2004

ISBN : 2-11-005792-0


J'ESPÈRE QU'IL N'EST PAS TROP TARD POUR LUI !
?
CNIL
URGENCES
C.N.I.L.
TRED

Sommaire

Avant-propos

Selon une étude récente, un peu moins d'un Français sur quatre a conscience d'être titulaire de droits à défendre en matière de protection des données personnelles. Et encore faut-il, lorsqu'il en a conscience, qu'il en connaisse la nature et la portée … Et si tel est le cas, sait-il que la mission fondamentale de la Commission nationale de l'informatique et des libertés est de l'assister dans la sauvegarde de ses droits ?

Ce constat sème une certaine angoisse au sein des équipes de notre commission, membres et collaborateurs, mais suscite également un formidable enthousiasme car le sens de la tâche à accomplir apparaît dès lors clairement : la « nouvelle CNIL », issue de la loi du 6 août 2004 modifiant la grande loi de 1978, doit déployer d'immenses efforts de communication, d'information, de pédagogie, à l'intention de l'ensemble des acteurs du monde informatique mais aussi, bien sûr, de l'ensemble des Français.

Et parmi les différentes actions mises en œuvre depuis un an dans ce domaine (telles que l'organisation des « Rencontres régionales », l'élaboration de guides spécialisés, la refonte du site internet, le développement des relations avec la presse, etc.), la rénovation du rapport annuel prévu par la loi est un axe fort.

C'est pourquoi nous avons travaillé d'arrache-pied afin que sa présentation puisse se tenir le plus tôt possible dans l'année de l'exercice considéré, tout en faisant en sorte qu'il soit très accessible et néanmoins d'une grande rigueur éthique et juridique.

Le pari sera gagné si de l'universitaire à l'agriculteur, de l'élève de première au chef d'entreprise, du ministre à l'artisan, du haut fonctionnaire au retraité, du journaliste à l'ouvrier, chacun trouve sinon du plaisir – n'exagérons rien – du moins un intérêt à la lecture de cette édition 2004.

Bien entendu les spécialistes – et les passionnés – pourront regretter de ne plus disposer du rapport, ancienne formule, considéré, à juste titre, en France et ailleurs, comme un monument, sur le plan de l'analyse juridique.

Mais je tiens à les rassurer. D'une part, l'ensemble des recommandations, avis et décisions de la CNIL feront l'objet d'une publication parallèle. D'autre part, si la présentation de ce rapport est allégée, et son volume réduit, son contenu reste, évidemment, rigoureux et diversifié.

Qu'on en juge :

Outre les éléments précis et chiffrés du bilan des activités multiples de la CNIL, outre un éclairage concret sur quelques aspects du traçage informatique auquel chacun de nous est soumis ou se soumet, le vingt-cinquième rapport donne un premier aperçu de l'application de la loi du 6 août 2004 qui a modifié profondément le texte fondateur de 1978.

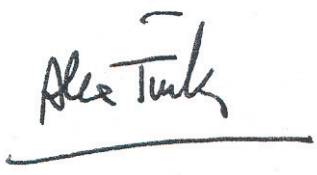
Il rappelle ensuite que 2004 aura été, pour la CNIL, l'année du passeport biométrique européen et du dossier médical personnel, deux sujets majeurs, entre autres, qui n'ont pas fini de la mobiliser. Par ailleurs il revient sur des questions déjà abordées l'an dernier, spam, vote électronique, télébilletique, etc. emblématiques des nouveaux usages technologiques auxquelles la protection des données personnelles est désormais confrontée. Sans prétendre à des conclusions définitives, le rapport fait état des réflexions que mène la CNIL sur l'évolution des usages de l'internet.

Un chapitre consacré au programme 2005 témoigne, s'il en était besoin, que les dossiers qui attendent la CNIL cette année ne sont pas minces : description des minorités, carte d'identité électronique, lutte contre la copie illicite de musique … autant de domaines où s'avère délicate la conciliation d'intérêts légitimes et la préservation de la vie privée ou de la liberté individuelle.

Pour autant, bien sûr, l'exercice a ses limites. Un rapport annuel ne peut jamais être exhaustif. Il exprime des préoccupations, des évolutions, des tendances, parfois des succès, mais il ne suffit pas à prendre la mesure de l'activité de l'organisme qui le produit.

Aussi, dois-je rappeler que notre Commission est toujours prête à répondre aux questions et à apporter les compléments d'information recherchés.

Cette mission d'information continue est inhérente à sa vocation d'institution protectrice des libertés individuelles.



Alex Türk
Président de la Commission nationale
de l'informatique et des libertés

LA CNIL

La CNIL en un CLIN d'œil

La Commission nationale de l'informatique et des libertés est chargée d'appliquer la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La mission générale de la CNIL est de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

LES MEMBRES DE LA CNIL

Le bureau

Président

Alex TÜRK, sénateur du Nord
Membre de la CNIL depuis 1992, président de l'autorité de contrôle Schengen de 1995 à 1997, de l'autorité de contrôle commune d'Europol (2000-2002), de l'autorité de contrôle d'Eurodac (2003) et vice-président de la CNIL de 2002 à 2004, Alex Türk est président de la CNIL depuis le 3 février 2004. Il préside la formation restreinte.

Vice-président délégué

Guy ROSIER, conseiller maître honoraire à la Cour des comptes
Secteur : Affaires économiques
Membre de la CNIL depuis janvier 1999, Guy Rosier a été élu vice-président le 26 février 2004, puis vice-président délégué le 5 octobre 2004. Membre de droit de la formation restreinte.

Vice-président

François GIQUEL, conseiller maître à la Cour des comptes
Secteur : Sécurité
Membre de la CNIL depuis février 1999, François Giquel a été élu vice-président le 5 octobre 2004. Membre de droit de la formation restreinte.

Les membres (commissaires)

François BERNARD, conseiller d'État honoraire
Secteur : Santé
François Bernard est membre de la CNIL depuis février 2004.

Hubert BOUCHET, membre du Conseil économique et social
Secteur : Travail
Hubert Bouchet est membre de la CNIL depuis novembre 1990, il a été vice-président délégué de février 1999 à août 2004. Il est membre élu de la formation restreinte chargée de prononcer les sanctions.

Jean-Marie COTTERET, professeur émérite des universités
Secteurs : Collectivités locales, audiovisuel
Jean-Marie Cotteret est membre de la CNIL depuis janvier 2004.

Anne DEBET, professeur des universités
Secteur : Affaires sociales
Anne Debet est membre de la CNIL depuis janvier 2004. Elle est membre élu de la formation restreinte chargée de prononcer les sanctions.

Emmanuel de GIVRY, conseiller à la Cour de cassation
Secteur : Gestion des risques et des droits
Emmanuel de Givry est membre de la CNIL depuis février 2004.

Georges de LA LOYÈRE, membre du Conseil économique et social
Secteur : Affaires internationales
Georges de La Loyère est membre de la CNIL depuis octobre 2004. Il est le représentant de la CNIL au sein du groupe de l'article 29 et des autorités de contrôle Europol et Schengen.

Francis DELATTRE, député du Val-d'Oise
Secteur : Affaires culturelles
Francis Delattre est membre de la CNIL depuis août 2002.

Patrick DELNATTE, député du Nord
Secteur : Justice
Patrick Delnatte est membre de CNIL depuis août 2002.

Jean-Pierre de LONGEVIALLE, conseiller d'État honoraire
Secteur : Finances publiques
Jean-Pierre de Longevialle est membre de la CNIL depuis décembre 2000.

Isabelle FALQUE-PIERROTIN, conseiller d'État, présidente du Conseil d'orientation et déléguée générale du Forum des droits sur l'internet
Secteur : Libertés publiques
Isabelle Falque-Pierrotin est membre de la CNIL depuis janvier 2004. Elle y préside le groupe de travail sur l'administration électronique.

Didier GASSE, conseiller maître à la Cour des comptes
Secteur : Télécommunications et réseaux
Didier Gasse est membre de la CNIL depuis janvier 1999. Il est le représentant de la France au sein de l'autorité de contrôle Eurojust.

Philippe LEMOINE, coprésident du directoire des Galeries Lafayette, président de Laser
Secteur : Technologie
Philippe Lemoine a été commissaire du gouvernement auprès de la CNIL de 1982 à 1984. Il est membre de la CNIL depuis janvier 1999.

Philippe NOGRIX, sénateur de l'Ille-et-Vilaine
Secteur : Monnaie et crédit
Philippe Nogrix est membre de la CNIL depuis octobre 2001.

Bernard PEYRAT, conseiller à la Cour de cassation
Secteur : Commerce
Bernard Peyrat est membre de la CNIL depuis février 2004. Il est membre élu de la formation restreinte chargée de prononcer les sanctions.

Commissaires du Gouvernement

Charlotte-Marie PITRAT
Catherine POZZO DI BORGO, adjointe

LES SERVICES AU 31 DÉCEMBRE 2004

Président

Alex TÜRK

Secrétaire général

Christophe PALLEZ

SECRÉTARIAT DE LA PRÉSIDENCE

Odile BOURRE, chef du secrétariat

Évelyne LE CAM, Ghislaine MERTES

SERVICE DE L'INFORMATION ET DE LA DOCUMENTATION

Chef de service

Edmée MOREAU

Information et documentation juridiques

Valérie BEL

Sites web et intranet

Anne-Sophie JACQUOT

Louis RAMIREZ

Bibliothèque et Informations générales

Solène BELEDIN

SERVICE DES AFFAIRES EUROPÉENNES ET INTERNATIONALES

Chef de service

Marie GEORGES

Clarisse GIROT

Assistance et secrétariat

Marie LEROUX

COMMUNICATION

Responsable

Elsa TROCHET-MACÉ

Brigitte BARBARANT, assistante communication

Revue de presse

Hervé GUDIN

DIRECTION DES AFFAIRES JURIDIQUES

Directeur: Sophie VULLIET-TAVERNIER

DIVISION DES AFFAIRES ÉCONOMIQUES

Chef de division

Sophie NERBONNE

Banque-crédit-assurances Organismes consulaires

Nathalie METALLINOS

Guillaume DESGENS-PASANAU

Communications électroniques – Services postaux – net-économie – transports

Leslie BASSE

Thomas DAUTIEU

Mathias MOULIN

Commerce-marketing – logement social – Immobilier – énergie

Odile JAMI

Xavier LEMARTELEUR

Françoise PARGOUD

Assistance juridique et secrétariat

Brigitte HUGER

Barbara BAVOIL

Halima GOUASMIA

DIVISION DES AFFAIRES PUBLIQUES ET SOCIALES

Chef de division

Jeanne BOSSI

Fiscalité-collectivités locales-administration électronique

Olivier COUTOR

Olivier LESOBRE

Justice-police – Droit d'accès indirect, libertés publiques

Bérengère MONEGIER DU SORBIER

Guillaume DELAFOSSE

Santé-assurance maladie Recherche médicale

Jeanne BOSSI

Daniéla PARROT

Travail-social

Norbert FORT

Laurent LIM

Statistiques-éducation

Fatima HAMDI

Assistance juridique et secrétariat

Audrey BACQUIÉ

Valérie GAUTIER

Catherine MANDINAUD

Eugénie MARQUES

Brigitte SALHI-SAGOT

Malika KHELLAF

SERVICE DES PLAINTES ET DES REQUÊTES GÉNÉRALES

Chef de service

Clémentine VOISARD

Associations – Partis – politiques – internet – Banque – fichiers centraux d'impayés

Émilie PASSEMARD

Travail-Social – Sécurité sociale-santé – Éducation nationale-Fiscal

Caroline PARROT

Marketing-sollicitations commerciales – Assurances – télécommunications

Xavier DELPORTE

Assistance juridique et secrétariat

Anna BENISTI

Véronique BREMOND

Véronique JENNEQUIN

Michèle SAISI

Siré BARRY

DIRECTION DES AFFAIRES ADMINISTRATIVES

Directeur: Thierry JARLET

Secrétariat de la direction

Brigitte BARBARANT, chef du secrétariat

Missions – Manifestations

Nathalie JACQUES

SERVICE DU PERSONNEL

Chef de service

Jean-Marc FERNANDES

Secrétariat

Anastasia TANFIN

SERVICE DE L'INFORMATIQUE INTERNE

Chef de service

Hervé BRASSART

Informatique

Gilbert BENICHOU, ingénieur

Thierry CARDONA, ingénieur

Philippe MIMIETTE, administrateur réseaux

Sébastien BÉNARD, technicien développeur

Giuseppe GIARMANA, technicien bureautique et téléphonie

Exploitation des formalités préalables

Mireille LACAN, responsable

Sonia CUSTOS

Christiane MARIE

SERVICE FINANCES ET LOGISTIQUE

Chef de service

Vincent PASCAL

Gestion budgétaire-Contrôle de gestion

Vincent PASCAL

Comptabilité

Liliane RAMBERT, comptable

Sébastien BOILEAU, gestionnaire

Logistique

Marie-Christiane BENJAMIN, standardiste

Jérôme BROSSARD, huissier

Noëlle CHAUMETTE, standardiste

Alain HOUDIN, conducteur

Joël LEPAGE, conducteur

Patrick MAHOUDEAU, conducteur

Mickaël MERI, huissier

Pierre RIHOUAY, huissier

Félisa RODRIGUEZ, agent technique

DIRECTION DE L'EXPERTISE ET DES CONTRÔLES

Directeur: Roger NGÔ

Secrétariat de la direction

Véronique FOUILLET

EXPERTISE

Yann LE HEGARAT, expert informaticien

Jean-Luc BERNARD, expert informaticien

SERVICE DES CONTRÔLES

Chef de service

Florence FOURETS

Jean-Paul MACKER, informaticien contrôleur

Michel GUEDRE, informaticien contrôleur

Bernard LAUNOIS, informaticien contrôleur

LES MOYENS

Le personnel

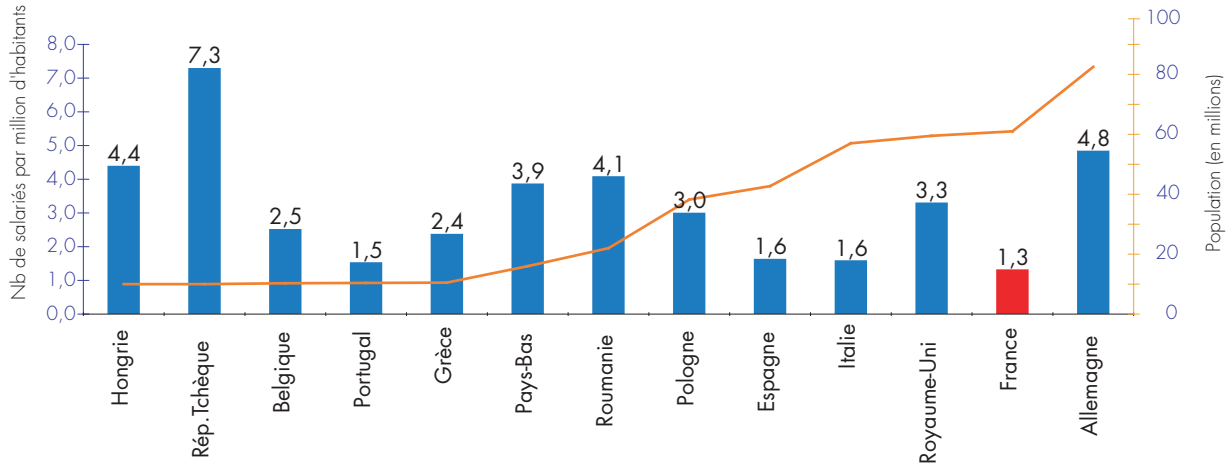
La CNIL dispose de 80 postes budgétaires en 2004. À cet effectif budgétaire doivent être ajoutés un poste d'informaticien de haute technicité (IHT) et, en 2004, des vacataires qui représentent deux équivalents temps plein (ETP).

Total des postes budgétaires

2003	2004	2005	% 2003-2004	% 2004-2005
76	80	83	+ 5,3 %	+ 3,8 %

L'effectif de la CNIL reste en deçà de celui dont disposent toutes les autres autorités de protection des données de l'Union européenne dont les missions sont pourtant identiques. En retenant un taux de trois employés par million (taux de la Pologne), l'effectif de la CNIL serait porté à 191 employés.

.



Le budget

En millions d'euros (M€)

	2003	2004	2005	% 2003-2004	% 2004-2005
Budget total voté (LFI)	**6,479**	**6,902**	**7,121**	**+ 6,53 %**	**+ 3,17 %**
Dépenses de personnel	**4,379**	**4,567**	**4,660**	**+ 4,31 %**	**+ 2,03 %**
Dépenses de fonctionnement	**2,100**	**2,335**	**2,461**	**+ 11,17 %**	**+ 5,40 %**
Hors informatique	1,613	1,684	1,880	+ 4,37 %	+ 11,65 %
Informatique	0,487	0,651	0,581	+ 33,68 %	– 10,77 %

Exécution du budget de fonctionnement

En millions d'euros (M€)

	2003	2004	2005 (prévision)	% 2003-2004	% 2004-2005
Immobilier	0,810	0,933	0,956	+ 15,1 %	+ 2,5 %
Informatique	0,410	0,548	0,571	+ 33,5 %	+ 4,1 %
Dépenses courantes	0,809	0,891	1,050	+ 10,2 %	+ 17,9 %
Total fonctionnement	**2,029**	**2,372**	**2,577**	**+ 16,9 %**	**+ 8,6 %**

La rénovation du système d'information de la CNIL s'est poursuivie en 2004. Les dépenses d'informatique ont augmenté de 32,8 % en 2003 et de 33,5 % en 2004. L'accroissement prévu des dépenses de communication pour mieux faire connaître la loi « Informatique et Libertés » au public explique l'accroissement de 17,9 % des « dépenses courantes ».

LES CHIFFRES CLÉS

Séances plénières

Les membres de la CNIL se réunissent en séance plénière deux fois par mois sur un ordre du jour établi à l'initiative de leur président.

Une partie importante de ces séances est consacrée à l'examen de projets de loi et de décrets soumis à la CNIL pour avis par le Gouvernement.

Lors de ces séances plénières, la CNIL adopte aussi des délibérations qui sont des avis ou des autorisations sur des traitements ou des fichiers. Avant la loi du 6 août 2004, étaient aussi examinées en séance plénière les suites à donner à certaines plaintes ou aux contrôles et il arrivait que la CNIL adresse des avertissements et dénonce des affaires à la justice. En ce qui concerne les avertissements, c'est désormais le rôle de la formation restreinte de la Commission, composée de six de ses membres.

MÉMO

Au total depuis 1978, la CNIL a décidé :
– 99 avis défavorables
– 61 avertissements
– 45 normes simplifiées
– 36 dénonciations au parquet

Enfin, nombre de rapports font le point sur les évolutions de l'informatique afin d'éclairer les membres de la CNIL dans la conduite de leurs missions.

Compte tenu de la grande variété des dossiers que la CNIL doit traiter, une répartition par secteur d'activité est établie entre les commissaires. Cette répartition a l'avantage d'instaurer une forme de spécialisation et de faciliter les contacts des commissaires avec les responsables de traitements. Néanmoins, les délibérations de la CNIL sont débattues selon les principes de la collégialité.

À l'occasion des 24 séances plénières qui se sont tenues en 2004, la CNIL a adopté 105 délibérations[1].

Parmi les décisions prises en 2004 par la CNIL, il convient de relever :
– 36 délibérations décidant d'une mission de contrôle, la Commission ayant procédé effectivement à 45 contrôles sur l'année (*cf.* p. 31) ;

– 7 avertissements, concernant le secteur bancaire ;
– 3 normes simplifiées visant à alléger les formalités de déclaration des collectivités locales ;
– 2 dispenses de déclaration concernant la gestion des rémunérations ;
– 2 dénonciations au parquet, l'une relative à la diffusion d'une « liste noire » de notaires sur internet, l'autre à des actions de prospection par fax sans le consentement des personnes ;
– 1 avis défavorable relatif à l'utilisation de la biométrie à des fins de gestion du temps de travail.

Saisines

Dans ses missions, la CNIL répond aux demandes de conseil qui lui sont adressées par des responsables de fichiers, instruit les plaintes dont elle est saisie par les citoyens, procède aux vérifications nécessaires dans le cadre du droit d'accès indirect aux fichiers intéressant la sécurité publique et la sûreté de l'État, et délivre à toute personne qui en fait la demande un extrait de la liste des traitements qui lui sont déclarés (« fichier des fichiers »).

Saisines	2003	2004	Variation 2003-2004
Demandes de droit d'accès indirect	1 163	1 970	+ 69,3 %
Plaintes	3 567	3 591	+ 0,6 %
Demandes de conseil	1 102	1 595	+ 44,7 %
Demandes d'extrait du fichier des fichiers	304	355	+ 16,7 %
Totaux	**6 136**	**7 511**	**+ 22,4 %**

1. Disponibles sur cédérom en annexe du rapport et sur le site Légifrance

En 2004, la CNIL a reçu 7 511 saisines soit une augmentation de 22,4 % d'une année sur l'autre, celles-ci se répartissent en :
– 3 591 plaintes (*cf.* p. 33) ;
– 1 970 demandes de droit d'accès indirect (*cf.* p. 44) ;
– 1 595 demandes de conseil ;
– 355 demandes d'extraits du « fichier des fichiers ».

Les secteurs d'activité qui, par ordre décroissant, ont suscité le nombre le plus important de demandes de conseil sont :
– le travail ;
– les collectivités locales ;
– la santé ;
– la fiscalité ;
– les télécommunications.

L'objet le plus fréquent des demandes de conseil est l'information sur les formalités préalables.

Les secteurs d'activité qui, par ordre décroissant, ont suscité le nombre le plus important de plaintes sont :
– la prospection commerciale ;
– la banque ;
– le travail ;
– les télécommunications.

L'objet le plus fréquent des plaintes est l'opposition à figurer dans un traitement.

M É M O

En 2004
+ 22% de saisines de la CNIL
+ 69% de demandes d'accès à des fichiers de police et de gendarmerie

Déclarations de fichiers

Pour la période du 1er janvier au 31 décembre 2004, la CNIL a enregistré 66 840 nouveaux traitements de données personnelles, soit une légère augmentation par rapport à 2003.

Avec les 3 454 déclarations de modification de traitements, déjà déclarés, reçues au cours de l'année 2004, 70 294 dossiers de formalités déclaratives ont été traités durant cette période par la CNIL.

M É M O

Plus d'1 million de fichiers déclarés à la CNIL depuis 1978

LA CNIL EN EUROPE ET DANS LE MONDE

La CNIL est confrontée à un double défi : celui de l'harmonisation et de l'application effective des règles communes de protection des données dans l'Union européenne qui s'est élargie en mai 2004 à dix nouveaux pays et celui de la reconnaissance de ce droit dans les pays qui, au Nord comme surtout au Sud, l'ignoraient.

Dans ce contexte les activités sont multiples, bilatérales et multilatérales.

Activités bilatérales

En 2004, les activités bilatérales n'ont fait qu'augmenter, sous des formes diverses :
– accueil de délégations étrangères (22 en 2005, en provenance de tous les continents, notamment Albanie, Croatie, États-Unis, Canada, Brésil, Japon, Hong Kong, Indonésie, Algérie, Cameroun …) et participation à des conférences en et hors d'Europe (Thaïlande notamment) ;
– échange d'informations et de bonnes pratiques avec les autres autorités nationales. La CNIL a pris en particulier l'initiative de lancer un réseau européen des experts en matière de technologies de l'information ;
– participation à des programmes de coopération auprès de ses homologues nouveaux membres de l'Union européenne, avec l'implication notamment de trois experts de la CNIL dans le programme Phare, établi par la Commission européenne pour la Lituanie.

Qu'est-ce que c'est ?

Le groupe de l'article 29

L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité de protection des données nationale. Ce groupe, dit « de l'article 29 », a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays tiers et de conseiller la Commission sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles.

Activités multilatérales

Sur le plan européen

La CNIL participe à la mise en œuvre des instruments européens sur la protection des données établis dans le domaine communautaire et dans celui de la coopération policière.

Dans le domaine communautaire, il s'agit de sa participation aux travaux du **groupe dit « de l'article 29 »** des autorités indépendantes en charge de la protection des données, institué par la directive générale 95/46/CE.

Dans le cadre de sa participation à l'élaboration de la législation européenne encadrant de nouveaux traitements de données, le groupe a émis des avis largement repris par le Parlement européen notamment sur les modèles de visa, titre de séjour et passeport européen incluant des éléments biométriques, avis dont le représentant de la CNIL a été le rapporteur (*cf.* « L'identification biométrique des voyageurs »), ainsi qu'en matière de transfert de données relatives aux passagers contenues dans les systèmes d'information sur les réservations vers les autorités américaines, canadienne et australienne (cf. « Les données des passagers aériens (PNR) : des transferts légalisés mais non sécurisés »).

Le groupe a établi des recommandations[2] dans les domaines où une interprétation commune européenne est stratégique (données génétiques, dispositions « antispam » de la directive sur les communications électroniques 2002/58/CE, application de la protection des données à l'usage des puces RFID …).

Le groupe a également travaillé sur la mise en œuvre de la directive de 1995 par l'adoption de mesures communes en matière d'information des personnes concernées sur le traitement de leurs données, et la réflexion sur la simplification et l'harmonisation des procédures de formalités préalables à la création des traitements. Il a arrêté le principe de contrôles coordonnés dans certains secteurs cible qui seront choisis en 2005.

2. Ces textes sont accessibles sur le site europa, à l'adresse : http://europa.eu.int/comm/internal_market/privacy/workingroup_fr.htm.

Dans le domaine de la coopération policière, la CNIL siège au sein des autorités de contrôle communes (ACC), Europol, Schengen et système d'information douanier :

L'ACC Europol s'est réunie quatre fois durant l'année 2004. Désormais présidée par **Emilio Aced Felez**, membre de la délégation espagnole, l'Autorité s'est prononcée sur deux créations de fichiers dits « d'analyse », sur une demande expresse visant à autoriser Europol à prolonger la durée de conservation de données enregistrées dans un fichier d'analyse spécifique, ainsi que sur le niveau de protection des données offert par la Croatie, État tiers avec lequel Europol envisage de signer un accord permettant d'échanger des données. En outre, l'ACC a mené une nouvelle inspection à Europol en mars 2004. Ces actions figurent dans le deuxième rapport d'activité de l'autorité (octobre 2002 – octobre 2004).

L'ACC Schengen, quant à elle, présidée par **Ulco Van de Pol**, membre de la délégation néerlandaise, s'est réunie cinq fois. Elle a poursuivi ses travaux portant sur le SIS II, et a rendu un avis sur ce projet européen en mai 2004. Le SIS doit en effet connaître de profondes modifications dans les prochaines années en raison de l'intégration de nouveaux États membres mais aussi de la volonté des gouvernements de le faire évoluer vers un instrument d'enquête. Les exigences de la sécurité publique rendraient indispensables un accroissement de ses fonctionnalités, l'enregistrement de nouvelles catégories d'information, le prolongement des durées de conservation et la consultation des données par un plus grand nombre de services.

Qu'est-ce que c'est ?

Schengen

Le système d'information Schengen (SIS) centralise au niveau européen, sur le fondement d'une convention du 19 juin 1990, des signalements concernant soit des personnes recherchées ou placées sous surveillance, soit des véhicules ou des objets recherchés. L'autorité de contrôle commune Schengen exerce un contrôle technique du fichier central (C-SIS) installé à Strasbourg et vérifie le respect par les États participant au système des droits accordés aux personnes.

Europol

Europol, office européen de police installé à La Haye, a pour mission d'améliorer la prévention et la lutte contre le terrorisme, le trafic illicite de stupéfiants et autres formes graves de criminalité internationale. Cet office gère un important système informatisé de données. L'autorité de contrôle commune Europol a pour tâche de surveiller l'activité d'Europol.

Système d'information douanier

C'est une base de données européenne visant à prévenir, rechercher et poursuivre les infractions aux réglementations douanière et agricole. L'autorité de contrôle commune du système d'information douanier surveille le fonctionnement du système d'information des douanes, en concertation avec les autorités de contrôle nationales et le contrôleur européen à la protection des données.

Questions à …

Georges de LA LOYÈRE

Membre du Conseil économique et social
Commissaire en charge du secteur « International »

Quelle feuille de route la CNIL se donne-t-elle en 2005 ?

En 2005 la CNIL entend se concentrer sur deux objectifs :
– contribuer à assurer en Europe, dans le cadre de la nouvelle constitution qui consacre la protection des données comme droit fondamental (article 8), une plus grande cohérence et une meilleure visibilité des instruments de protection, aujourd'hui disparates, selon qu'il s'agit de traitements de données relevant du droit communautaire ou de la sécurité de l'Union ;
– définir et mettre en œuvre un plan d'action donnant suite à l'appel lancé à Ouagadougou en novembre 2004 par les chefs d'États et de Gouvernement de la francophonie en faveur de la création ou du développement des règles sur la protection des données. En effet, si tous les pays du Nord de la francophonie assurent cette protection, il n'en est pas de même dans les pays du sud.

L'ACC du Système d'information des douanes (SID), présidée par **Francis Aldhouse**, s'est réunie à trois reprises en 2004, rencontrant à plusieurs occasions des représentants de l'Office européen de la lutte antifraude (OLAF) qui assure la gestion technique de la base de données unique du SID pour le compte de la Commission européenne. Elle s'est interrogée sur les raisons de l'actuelle sous-utilisation du système par les administrations douanières nationales, qui semblent être d'ordre technique et juridique (multiplicité des fichiers aux finalités connexes, absence de liens entre eux). Des propositions de modification des textes régissant le SID sont en cours d'adoption.

Une des principales préoccupations de la conférence européenne des commissaires à la protection des données qui s'est réunie en avril 2004 à **Rotterdam** a été de déterminer comment autorités nationales et autorités de contrôle communes pouvaient se coordonner pour évaluer les initiatives de plus en plus fortes des gouvernements européens dans le domaine de la coopération policière.

Un membre de la CNIL, **Didier Gasse**, est aussi le représentant de la France au sein de l'organe de contrôle commun **Eurojust**. Créée en 2002, Eurojust a pour objectif d'améliorer la coordination et la coopération entre les enquêteurs et procureurs travaillant sur des dossiers de criminalité internationale grave et de leur prêter son concours en vue de renforcer leur efficacité. Chacun des pays de l'Union européenne y est représenté par un membre au sein d'un collège. Un organe de contrôle commun indépendant, mis en place en 2004, contrôle de manière collégiale les activités d'Eurojust en ce qui concerne le traitement des données à caractère personnel. Chaque État membre y désigne un représentant.

Sur le plan mondial

La conférence internationale des commissaires à la protection des données qui se tient annuellement a été organisée cette année par l'autorité polonaise à **Wroclaw**. La CNIL a apporté sa contribution sur les thèmes centraux de l'enjeu de sécurité au plan mondial et des flux transfrontières ainsi que sur la protection de la vie privée des salariés.

Par ailleurs la CNIL a pris l'initiative de suggérer au Gouvernement français de faire prendre en compte la préoccupation de développement de la protection des données au sein des pays francophones notamment lors du **sommet de la francophonie à Ouagadougou**.

L'IMAGE DE LA CNIL

En juin 2004, une étude portant sur la perception et l'image de la CNIL a été menée par TNS SOFRES sur un échantillon de 1 000 personnes représentatives de la population française. Voici les principaux constats.

La notoriété

Le profil type de la personne qui connaît la CNIL : homme entre 25 et 49 ans/cadre ou profession intellectuelle vivant en agglomération parisienne, utilisateur d'internet. La connaissance diminue sur les populations jeunes et sur les plus anciens.

Question : Connaissez-vous ne serait-ce que de nom la CNIL ?	
Oui	32
Non	68
	100 %

Question : Connaissez-vous ne serait-ce que de nom la Commission nationale de l'informatique et des libertés ?	
Oui	45
Non	55
	100 %

Le rôle de la CNIL

Un rôle assez défini : les thèmes de protection des libertés individuelles et de régulation notamment sur internet sont dominants.

Question : Selon vous, à quoi sert la CNIL — Question ouverte - Réponses spontanées	Ensemble de l'échantillon	Connaissent la CNIL
Citations autour de l'idée de protection	**22**	**41**
La protection des libertés individuelles	10	18
Pour le respect de la vie privée	9	18
Idées de protection en général / sans précision	3	6
Citations autour de l'idée d'internet	**9**	**14**
C'est la police informatique, pour éviter les dérapages sur internet	4	7
Pour la sécurisation des données sur internet	3	5
Pour le contrôle de ce qui se passe sur internet	1	2
Contre le piratage informatique	1	1
Citations générales sur l'organisme	**5**	**8**
Un organisme utile / nécessaire	1	2
Un organisme inutile / complexe / flou	1	1
Citations autour de de surveillance / de contrôles	**1**	**2**
Recensement / fichage des individus	1	2
Autres citations	4	6
Sans réponse	63	35
	% (1)	% (1)

(1) Le total des pourcentages est supérieur à 100, les personnes interrogées ayant pu donner plusieurs réponses.

L'identification

Une perception assez floue : seulement 24 % des personnes interrogées (38 % parmi ceux qui connaissent la CNIL) savent que c'est un organisme indépendant. Il est important que, lors de ses communications, la Commission mette plus l'accent sur son statut d'indépendance.

Question :
Selon vous la CNIL c'est...

	Ensemble de l'échantillon	Connaissent la CNIL
Un organisme indépendant	24	38
Une association de défense des citoyens	18	17
Le service d'un ministère	16	26
Sans opinion	42	19
	100%	100%

L'opinion

La notoriété a un impact positif sur l'image : ceux qui connaissent la CNIL en ont plutôt une bonne opinion. La CNIL a donc intérêt à faire connaître ses missions auprès des citoyens.

Question :
D'une manière générale, avez-vous plutôt une bonne opinion ou plutôt mauvaise de la CNIL ?

	Ensemble de l'échantillon	Connaissent la CNIL
Une très bonne opinion	3	6
Plutôt une bonne opinion	29	51
Sous-total bonne opinion	**32**	**57**
Plutôt une mauvaise opinion	3	6
Une très mauvaise opinion	1	1
Sous-total mauvaise opinion	**4**	**7**
Sans opinion	64	36
	100%	100%

Les droits

Une grande méconnaissance des droits en matière de protection de données personnelles : moins d'un quart des personnes interrogées ont le sentiment d'être suffisamment informées sur leurs droits.

Question :
Vous-même, avez-vous le sentiment d'être suffisamment informé à propos de vos droits en matière de protection des informations personnelles vous concernant

	Ensemble de l'échantillon	Connaissent la CNIL
Oui, tout à fait	3	4
Oui, plutôt	18	21
Sous-total oui	**21**	**25**
Non, plutôt pas	39	44
Non, pas du tout	39	30
Sous-total non	**78**	**74**
Sans opinion	1	1
	100%	100%

À l'issue de cette enquête, on constate une grande disparité entre Paris et la province ainsi qu'un manque d'information évident sur le thème de la protection des données personnelles et ce, particulièrement auprès des jeunes qui sont de gros consommateurs des nouvelles technologies et de l'internet.

Ces résultats incitent donc la CNIL à orienter sa politique de communication vers une approche beaucoup plus grand public. La CNIL doit adopter une démarche de vulgarisation et de proximité pour que les citoyens sachent qu'ils ont des droits en matière de données personnelles et que la CNIL est chargée de faire valoir ces droits et les défendre. Si jusqu'à maintenant, la CNIL s'est davantage adressée aux responsables de traitement en termes d'obligations, il lui apparaît, aujourd'hui, essentiel de porter ses efforts vers l'information du public car pour défendre ses droits encore faut-il les connaître !

LA NOUVELLE LOI « INFORMATIQUE ET LIBERTÉS »

Dernier État à transposer la **directive européenne du 24 octobre 1995** sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, la France a fait le choix, symbolique, de maintenir la **loi «Informatique et Libertés» du 6 janvier 1978** tout en la remaniant profondément. Certes, les grands principes de fond de la protection des données sont réaffirmés. Mais, tant dans sa structure que dans sa philosophie d'ensemble, la loi du 6 janvier 1978 telle qu'elle a été modifiée par la **loi du 6 août 2004** a subi d'importants changements et a été considérablement enrichie qu'il s'agisse de son champ d'application, de l'institution du correspondant à la protection des données, innovation majeure, ou encore des nouveaux pouvoirs accordés à la CNIL tout particulièrement en matière de contrôle sur place et de sanctions.

La nouvelle loi «Informatique et Libertés» c'est tout d'abord un allégement substantiel des obligations déclaratives, le contrôle *a priori* de la CNIL sur les fichiers devant désormais s'exercer essentiellement sur les traitements présentant des risques particuliers d'atteinte aux droits et libertés. La déclaration devient ainsi le régime de droit commun pour la plupart des traitements et de larges possibilités d'exemption et de simplification des formalités sont par ailleurs prévues.

C'est ensuite un accroissement important des pouvoirs d'intervention de la CNIL, tant en ce qui concerne les investigations sur place que les sanctions. Alors qu'auparavant, la CNIL, constatant un manquement à la loi, ne pouvait que délivrer des avertissements aux organismes en cause ou les dénoncer au parquet, la nouvelle loi la dote de pouvoirs de sanctions administratives, notamment pécuniaires, importants.

L'éventail des mesures coercitives et des sanctions est large : hormis l'avertissement, la Commission pourra désormais prononcer une sanction pécuniaire – sauf à l'encontre de l'État -, une injonction de cesser le traitement ou encore retirer son autorisation.

Enfin, la nouvelle loi renforce les droits des personnes sur leurs données. En effet elle oblige les responsables de fichiers à faire œuvre de plus de transparence vis-à-vis des personnes fichées ou susceptibles de l'être, celles-ci devant désormais être informées plus précisément sur les conditions d'utilisation des données et sur leurs droits. Un droit d'opposition inconditionnel en matière de prospection commerciale est enfin consacré dans la loi et les conditions d'exercice du droit d'accès et de rectification sont précisées.

La réforme de la loi de 1978 induit donc un changement profond des méthodes d'intervention de la CNIL. Celle-ci s'est engagée, sans attendre, dans cette voie en adoptant en 2004 plusieurs mesures de simplification et d'exonération des formalités déclaratives notamment dans certains secteur-clés comme celui des collectivités locales. Pour pouvoir poursuivre la politique de contrôles sur place décidée au printemps et être à même d'utiliser ses nouveaux pouvoirs de sanctions, la Commission a d'ores et déjà modifié son règlement intérieur.

Questions à …

Francis DELATTRE

Député du Val-d'Oise
Commissaire en charge du secteur «Affaires culturelles»

En tant que rapporteur de la commission des lois de l'Assemblée nationale, quels messages avez-vous souhaité faire passer concernant la nouvelle loi «Informatique et Libertés» ?

J'ai souligné lors du débat parlementaire que la nouvelle loi «Informatique et Libertés» était une loi de simplification pour les entreprises.
À l'arrivée, si quelques catégories de traitements particulièrement «sensibles» sont désormais soumises à autorisation de la CNIL, l'immense majorité des applications informatiques du secteur privé relève de la déclaration et même de la déclaration simplifiée.
La CNIL peut d'ailleurs aller plus loin et exonérer de toute déclaration des catégories entières de traitements. Enfin l'entreprise qui aura désigné un correspondant à la protection des données sera dispensée de toute déclaration puisque le correspondant tiendra la liste des traitements et veillera, sous le regard de la CNIL, à ce que ces traitements soient conformes aux principes de la loi. Ces dispenses ne concernent pas les autorisations.

Pourquoi une telle volonté de simplifier ?

Il s'agit de faciliter la vie des entreprises mais surtout de renforcer l'application de la loi. Dégagée de tâches purement bureaucratiques, la CNIL sera plus sur le terrain pour expliquer, conseiller et aussi contrôler. À cet égard j'ai obtenu de l'Assemblée nationale que la publicité des sanctions prononcées par la CNIL soit exemplaire.

RECENTRAGE SUR LES TRAITEMENTS À RISQUE

Désormais, le régime de formalités ne dépend plus seulement d'un critère organique, c'est-à-dire l'appartenance du responsable de traitement au secteur public ou au secteur privé, mais d'un critère matériel, à savoir le caractère sensible du traitement, du fait de la finalité poursuivie ou de la nature des informations traitées. Les traitements relevant du contrôle préalable de la CNIL (avis ou autorisation) sont ainsi limitativement énumérés. Depuis l'entrée en vigueur de la nouvelle loi, la Commission s'est déjà prononcée sur plusieurs dossiers relevant de l'article 25 qui définit huit catégories de traitements à risques soumis à autorisation préalable de la CNIL.

1) Les traitements de données sensibles devant faire l'objet à bref délai d'un procédé d'anonymisation, ou justifiés par l'intérêt public (ex. fichiers de gestion des prestations des organismes d'assurance maladie obligatoire), ou encore réalisés par l'INSEE ou un service statistique ministériel à des fins statistiques. Les données sensibles sont les données qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

2) Les traitements automatisés portant sur des données génétiques, à l'exception de ceux mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements.

3) Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté mis en œuvre par les sociétés de droits d'auteur dans le cadre des actions de lutte contre le téléchargement illicite des fichiers (musique, vidéos …) sur internet.

4) Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire.

Il s'agit de traitements qui sont « susceptibles » d'exclure une personne et non pas seulement de ceux qui excluent avec certitude et sans discussion possible une personne. Le caractère systématique de l'exclusion n'est donc pas une condition nécessaire de l'application de ce critère. Ainsi, parce qu'une personne peut se voir refuser la possibilité de contracter du fait de son inscription dans une liste de mauvais payeurs qui fait l'objet d'un traitement, ledit fichier est susceptible d'exclure une personne d'un contrat et est, à ce titre, soumis à autorisation de la CNIL. Il s'agit donc d'encadrer les fichiers dits « listes noires » : fichiers mutualisés d'impayés que ce soit dans le domaine de la téléphonie, du crédit, des banques, de l'assurance, des loueurs de véhicules mais aussi les traitements de crédit *scoring*.

La CNIL a fait application de ce critère d'autorisation, à l'occasion de l'examen, le 21 septembre 2004, de la modification du fichier d'impayés téléphoniques mis en œuvre par le GIE preventel, modification jugée substantielle puisqu'il s'agissait du seuil d'inscription des personnes au fichie. Le 2 décembre 2004, saisie de l'expérimentation que souhaite mener la Banque de France sur le phénomène des « chèques flambants », c'est-à-dire des chèques qui sont émis massivement et en quelques jours, à partir d'un même compte, la CNIL a considéré que, s'agissant d'un traitement dont la finalité est de permettre au commerçant d'apprécier l'opportunité d'accepter ou de refuser le chèque qui lui est présenté en paiement, il convenait de faire application du régime de l'autorisation. Dans les deux cas l'autorisation a été accordée.

5) Les traitements automatisés ayant pour objet l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ou l'interconnexion de fichiers de personnes relevant du secteur privé et dont les finalités principales sont différentes. La Commission a examiné deux cas d'interconnexions relevant de cette procédure d'autorisation : le premier concernait la mise en œuvre de façon conjointe par EDF-GDF et par la Caisse nationale d'assurance maladie des travailleurs salariés de transmissions de données dans le cadre du dispositif de tarification sociale de l'électricité. La CNIL n'a accordé qu'une autorisation limitée à six mois, le dispositif proposé ne lui paraissant

pas satisfaisant (*cf.* p. 56). Le deuxième cas portait sur une interconnexion d'un fichier de gestion des contrats de location de véhicules avec le système de contrôle automatisé des infractions routières.

6) Les traitements de personnes privées portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR) et ceux qui requièrent une consultation de ce répertoire sans inclure le NIR.

Sont notamment concernés par cette catégorie les traitements de la paie du personnel et des organismes d'assurance maladie. Toutefois, ces organismes ont déjà été autorisés à utiliser le numéro d'inscription des personnes, c'est-à-dire le NIR, par des décrets intervenus en application de l'article 18 de la loi du 6 janvier 1978 avant modification. Ces autorisations sont acquises et ne seront pas remises en cause. Il n'y aura dès lors pas lieu de soumettre les traitements concernés à une nouvelle autorisation au seul motif qu'ils comporteraient le numéro de Sécurité sociale ou NIR.

7) Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes

Sont ici principalement visés les fichiers de gestion de l'action sociale.

8) Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Le contrôle préalable de ces traitements devrait permettre à la CNIL d'encadrer plus rigoureusement dans le secteur privé les conditions d'utilisation des techniques biométriques sensibles qui, telles les empreintes digitales, comportent des risques particuliers d'atteinte à la vie privée.

SIMPLIFICATION

Dans le cas de l'ancienne comme de la nouvelle loi « Informatique et Libertés », la CNIL peut établir des normes destinées à simplifier l'obligation de déclaration des fichiers les plus courants et qui ne sont pas susceptibles, dans le cadre de leur utilisation régulière, de porter atteinte à la vie privée ou aux libertés des personnes. Une fois vérifié le respect des conditions posées par ces normes, il suffit au responsable du fichier de réaliser une déclaration en ligne de conformité à cette norme sur le site de la CNIL (www.cnil.fr).

Deux axes forts de simplification des formalités déclaratives ont ainsi été définis par la CNIL en 2004.

Le premier concerne les applications utilisées quotidiennement par les collectivités locales.

Ainsi, ont été adoptées plusieurs normes simplifiées concernant des fichiers très courants. La norme simplifiée n° 43, portant sur les utilisations habituelles de l'état civil, prend en compte également des évolutions technologiques récentes (numérisation des actes, signature électronique …) et fixe des règles sur la publication des événements dans la presse locale. La norme simplifiée n° 44 relative à la gestion du cadastre permet de déclarer notamment les traitements des cédéroms VISDGI remis par l'administration fiscale aux communes. Elle a aussi défini les conditions de délivrance des informations cadastrales au public ce qu'aucun texte législatif ou réglementaire n'avait encore fait clairement. La norme simplifiée n° 45 sur l'utilisation des rôles des impôts locaux permet de déclarer plus facilement les traitements des cédéroms VISDGI d'impôts locaux mais aussi la plupart des logiciels d'analyse de la fiscalité locale (à l'exclusion du recensement des bases d'imposition).

Par ailleurs, la CNIL a accepté que le projet de décret visant à organiser l'assistance aux personnes fragiles en cas d'événements climatiques exceptionnels, dispense de déclaration les communes et les préfectures mettant en œuvre leur « fichier canicule », dans le cadre strict ainsi défini par le texte réglementaire. Elle a également dispensé de déclaration les traitements informatiques mis en œuvre dans le cadre des procédures de dématérialisation des marchés publics et les fichiers de fournisseurs.

Il faut toutefois rappeler que ces dispenses de déclaration ne sont effectives qu'à la condition que les traitements respectent les prescriptions définies dans les décisions de dispense de déclaration.

La loi aménage une possibilité de simplification pour les traitements relevant de la procédure d'autorisation. En effet, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation. La Commission a fait pour la première fois application de cette disposition en adoptant le 14 décembre 2004 une autorisation unique pour les systèmes d'information géographique (SIG), qui sont fréquemment mis en œuvre par les collectivités locales ou leurs groupements, en matière d'urbanisme et du cadastre pour permettre l'instruction des demandes de permis de construire et autres formalités, la délivrance des relevés de propriétés …

La CNIL a adopté une procédure identique pour les fichiers mis en œuvre par plus d'une centaine de distributeurs d'électricité et destinés à gérer le tarif social au bénéfice des personnes les plus démunies.

Le second axe de simplification concerne les applications mises en œuvre par l'ensemble des employeurs publics et privés.

La loi du 6 août 2004 modifiant la loi du 6 janvier 1978 permet désormais de dispenser de déclaration les traitements les plus courants et non susceptibles de porter atteinte à la vie privée ou aux libertés des personnes. Ainsi la CNIL a-elle décidé, en 2004, de procéder à cette dispense de déclaration des fichiers de paie, de gestion des déclarations sociales obligatoires et de tenue des registres obligatoires (registre unique du personnel notamment).

Elle a également mené, au cours de cette année 2004, une série de consultations auprès des partenaires sociaux et des ministères concernés qui lui a permis d'aboutir, en janvier 2005, à l'adoption d'une norme simplifiée pour la gestion des ressources humaines. Cette norme n° 46 vient compléter les mesures de simplification déjà prises par la CNIL dans ce domaine (norme simplifiée n° 40 concernant la mise en place d'autocommutateurs et d'annuaires téléphoniques internes, norme simplifiée n° 42 concernant le contrôle des accès aux locaux professionnels, la gestion des horaires et des congés, et la restauration d'entreprise).

Dans un domaine très différent, mais toujours dans le souci de poursuivre un objectif de simplification des formalités préalables, une norme simplifiée relative à la gestion des cabinets médicaux est actuellement à l'étude.

DIFFUSION DE LA CULTURE « INFORMATIQUE ET LIBERTÉS »

Le correspondant « informatique et libertés » (CIL)

La vision de la CNIL

La nouvelle loi « Informatique et Libertés » prévoit que tout organisme, privé comme public, bénéficiera d'un allègement de ses obligations déclaratives dès lors qu'il aura désigné un **correspondant à la protection des données** qui pourrait être dénommé **« correspondant informatique et libertés »**. Le statut et les missions du correspondant seront précisés dans un décret d'application. La CNIL a apporté sa propre contribution aux réflexions en cours sur la définition de ce correspondant.

L'exemple allemand

Une délégation de la CNIL a effectué, en octobre 2004, une mission d'étude auprès de ses homologues allemands, le détaché fédéral à la protection des données et le détaché du *Land* de Rhénanie du Nord – Westphalie. C'est la même dénomination de « détaché à la protection des données » qui est appliquée aux correspondants désignés par les entreprises et les administrations. Cette fonction existe de longue date et sa désignation est en principe

Questions à …

Jean-Marie COTTERET

Professeur émérite des universités
Commissaire en charge des secteurs « Collectivités locales » et « Audiovisuel »

Quelles seront les missions du correspondant ?
Au-delà de la tenue de la liste des traitements (à l'instar du « fichier des fichiers » tenu par la CNIL), le correspondant aura un rôle essentiel dans la diffusion de la culture « informatique et libertés » au sein de l'organisme l'ayant désigné et sera l'interlocuteur privilégié non seulement de la CNIL mais également des personnes concernées par les traitements soumis à la loi du 6 janvier 1978. Conseil en amont, pédagogie, audit et médiation devront ainsi accompagner un rôle d'alerte du responsable de traitement sur les irrégularités constatées.

Le responsable de traitement peut-il désigner un correspondant extérieur à l'organisme ?
La CNIL considère que la loi permet de désigner un correspondant qui n'appartient pas au personnel de l'organisme. Elle estime cependant qu'une désignation extérieure ne devrait être possible qu'en deçà d'un seuil à définir et devrait répondre au souci d'une « mutualisation » des fonctions de correspondant permettant à plusieurs responsables de traitement de se regrouper afin de désigner le même correspondant.

Quelles sont les qualifications requises pour être correspondant ?
Il n'est pas possible de déterminer a priori la nature et le niveau des qualifications requises qui dépendent de la taille et de l'activité du responsable de traitement. Il est évident que le CIL devra avoir une connaissance de la loi « Informatique et Libertés » et des technologies informatiques qu'elles soient standards ou spécifiques à l'activité de l'organisme l'ayant désigné.

Comment assurer l'indépendance du correspondant ?
Le législateur a mis le correspondant à l'abri des sanctions de l'employeur du fait de l'accomplissement de ses missions et l'a doté de la faculté de saisir la CNIL des difficultés rencontrées. Il apparaît à celle-ci qu'au-delà de ces dispositions, c'est la position hiérarchique du CIL, caractérisée par la possibilité de communiquer directement avec la direction de l'organisme, l'interdiction pour le responsable de traitement d'interférer dans l'accomplissement des missions du CIL et l'absence de conflit d'intérêts avec les fonctions exercées en même temps qui sont de nature à apporter les garanties de l'indépendance. Ainsi, par exemple le chef d'entreprise qui est le responsable du traitement, ne devrait pas pouvoir être désigné comme correspondant.

obligatoire. Prévue dès l'origine dans la loi fédérale relative à la protection des données personnelles de 1977, l'obligation de désigner un détaché à la protection des données a été étendue en 2001 au secteur public.

Une désignation obligatoire moyennant des conditions de seuil

Tout organisme privé doit désigner un détaché à la protection des données dès lors que plus de 4 personnes sont employées régulièrement au traitement automatisé de données à caractère personnel, ou plus de 20 personnes sont employées régulièrement au traitement manuel de telles données, ou encore pour des traitements soumis à un contrôle préalable en raison des risques qu'ils présentent. En pratique, compte tenu notamment du développement de l'usage de l'informatique, très peu d'organismes échappent à cette obligation.

Dans le secteur public fédéral, cette désignation est obligatoire, sans considération du nombre de personnes employées lorsque le traitement est automatisé et à partir de 20 personnes lorsqu'il est manuel. Il est cependant possible aux autorités fédérales de nommer un seul détaché pour plusieurs départements ou organismes publics. La plupart des lois des *Länder* ont repris cette obligation.

Les missions du détaché allemand à la protection des données

Les missions du détaché à la protection des données sont définies très largement. S'il est d'une manière générale chargé de veiller à l'application de la législation relative à la protection des données à caractère personnel, la loi fédérale confie au détaché une mission générale de surveillance de la conformité de l'utilisation des traitements mis en œuvre et il doit pour ce faire être informé en temps utile des projets de traitements. Il a un rôle pédagogique essentiel et doit familiariser, «grâce à des mesures appropriées», les personnes affectées au traitement de données à caractère personnel à la législation applicable en matière de protection des données personnelles, ainsi qu'avec les exigences particulières de la protection des données. Le détaché doit également effectuer le contrôle préalable prévu par la loi fédérale à charge pour lui d'en déférer à l'autorité compétente en cas de doute. Enfin, il a une mission d'information de toute personne qui a fait la demande sur les traitements mis en œuvre par le responsable de traitement. Ses fonctions de surveillance le conduisent à être l'interlocuteur privilégié non seulement de l'autorité de contrôle compétente mais également des personnes concernées par le traitement. Tenu au secret professionnel en application de la loi fédérale, il ne peut révéler ni l'identité des personnes concernées, ni les circonstances l'ayant conduit à tirer des conclusions sur la personne en cause.

La CNIL retient

Le détaché à la protection des données doit être à l'abri des conflits d'intérêt, d'où une incompatibilité avec des fonctions de direction, de même que l'exercice de fonctions dans les domaines ayant trait à la gestion des ressources humaines, à l'administration des systèmes d'information, aux technologies de l'information, ainsi que tout département mettant en œuvre des traitements de données sensibles ou de grande envergure (par exemple : le marketing). L'absence de conflit d'intérêts est appréciée au cas par cas et, en Allemagne, les autorités de contrôle compétentes, saisies le plus souvent par des salariés, interviennent régulièrement pour obtenir, amiablement ou sous la contrainte, la décharge du détaché ne présentant pas cette qualité.

Les capacités et qualités nécessaires à l'exercice des fonctions de détaché

Bien que la loi fédérale ne définisse pas les qualifications nécessaires à l'accomplissement des devoirs incombant au détaché à la protection des données, les acteurs de la protection des données conviennent qu'à une bonne connaissance de la réglementation relative à la protection des données personnelles doit être associée la connaissance des standards technologiques, des principes de gestion de l'entreprise, de l'organisation de l'entreprise et des traitements de données opérés. Il est entendu que lorsque le détaché ne possède pas lors de sa désignation l'ensemble de ces connaissances, il doit les acquérir et que le responsable de traitement doit lui donner la possibilité de se former.

La communication

Les colloques et formations

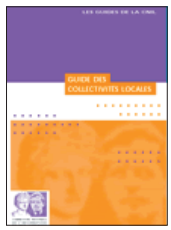
La CNIL est très souvent sollicitée pour intervenir à l'occasion de colloques ou conférences pour conduire des actions de sensibilisation à la loi « Informatique et Libertés ». L'entrée en vigueur de la nouvelle loi, dont la clarté n'est pas la principale vertu, a déjà commencé à générer un nombre croissant de demandes. La CNIL intervient dans des cadres très divers tels que des associations ou organismes professionnels, des universités, des salons. Pour l'année 2004, la CNIL a assuré 210 interventions à des conférences/colloques/séminaires ou animation de formations qui ont mobilisé 388 membres ou agents. À titre d'information, la CNIL a reçu, en 2004, 298 sollicitations d'interventions.

La CNIL a participé également au Salon des maires et des collectivités locales en qualité d'exposant.

Accueil sur le stand de la CNIL, au salon des Maires et des Collectivités locales du président du Sénat, Christian Poncelet, par le président de la CNIL.

Les guides et rapports de la CNIL

À l'occasion du Salon des maires et des collectivités locales, la CNIL a publié un ***Guide des collectivités locales*** dans la collection des **« Guides de la CNIL »**. Ce guide pratique de cinquante-cinq pages fait le point sur la protection des données personnelles relatives aux administrés et au personnel municipal et sur les règles essentielles à respecter. Il recense l'ensemble des fichiers de données personnelles gérées par les collectivités locales ainsi que les modalités de déclaration.



Le guide pratique *Halte aux publicités*; paru en janvier 2005; informe les personnes sur la prospection commerciale non sollicitée et leur donne des conseils pour faire valoir leurs droits et éviter de recevoir de nouvelles sollicitations.

En 2004, la CNIL a édité le rapport ***Cybersurveillance sur les lieux de travail*** qui s'attache aux technologies de l'information et de la communication sur les lieux de travail et au nécessaire équilibre à trouver entre les intérêts des employeurs et le respect des droits et libertés des employés (La Documentation française, mars 2004).

Ces guides et rapports sont disponibles en téléchargement sur le site de la CNIL.

Le tour de France des régions

Pour faire connaître la nouvelle loi « Informatique et Libertés » et en expliquer les règles, la CNIL a entamé en janvier 2005 une démarche inédite de communication de proximité qui s'étendra à l'ensemble des régions françaises. Cette initiative a aussi pour objectif de pallier l'absence, pour le moment, de représentations régionales de la CNIL et de réduire le déficit de notoriété constaté par le sondage de la SOFRES.

Pendant trois jours, le président, ainsi que des membres ou des agents de la CNIL, vont à la rencontre des acteurs locaux publics et privés concernés par la protection des données personnelles : élus, entreprises, professionnels de la santé, associations d'usagers, professionnels de l'éducation et du secteur social, magistrats, avocats, presse, etc.

Le programme des rencontres régionales de la CNIL constitue un projet majeur en 2005 puisqu'il prévoit l'organisation de 8 rencontres dans l'année. Ces événements mobilisent en moyenne 20 personnes de la commission pendant trois jours, soit un quart des effectifs...

Le site internet et l'information au public

Après six ans d'existence (ouverture en janvier 1998) et une refonte totale, un nouveau site a été mis en ligne le 10 mars 2004 pour mettre en relief l'actualité, offrir des contenus plus proches des citoyens et se doter de nouveaux outils pour répondre à une audience toujours en hausse.

Le **nouveau site web de la CNIL** fournit une information en lien direct avec l'actualité (tribune, agenda, échos des séances ...) et propose en particulier des contenus pour faciliter les démarches des personnes (rubrique « AGIR », modèles de lettres, modèles de mentions d'information ...).

M E M O

Volume du site (www.cnil.fr) au 31 décembre 2004

– 1 310 pages html
– 150 fichiers PDF en téléchargement

Audience 2004

Avec plus de 7 millions de pages vues sur l'année 2004, le site de la CNIL est visité en moyenne par 3 000 personnes par jour, soit un gain de 1 000 visiteurs quotidiens par rapport à 2003.

En 2004 deux sondages en ligne ont été effectués :
– janvier 2004 : sondage en ligne sur la géolocalisation des enfants : 1 600 contributions ;
– juillet 2004 : sondage sur les services de banque à distance : 1 859 contributions.

Lancée en septembre 2003, la lettre mensuelle d'information baptisée ***Lettre InfoCNIL*** compte 8 642 abonnés au 31 décembre 2004.

Enfin, en 2004, ont été reçues près de 1 000 demandes d'information du public adressées au **service « Information Documentation »** (renseignements, documentation, recherches), soit cinq fois plus qu'en 2003. Cette explosion des demandes externes peut s'expliquer par la publication sur le site de la CNIL, à partir de 2004, des coordonnées d'un « contact Documentation » (nom, prénom, ligne directe) et sans doute par l'intérêt suscité par la nouvelle loi.

Préfecture du Nord, Lille, janvier 2005.

Conseil général du Pas-de-Calais, Arras, janvier 2005.

LES CONTRÔLES

Le bilan 2004 des contrôles

En 2004, 45 missions de contrôle sur place ont été opérées, en application de 31 décisions adoptées par la Commission[3]. La différence entre ces deux chiffres s'explique par le fait que certaines décisions de contrôles, concernant en particulier de grandes sociétés, ont nécessité plusieurs déplacements, notamment auprès de prestataires de services à qui une partie de l'activité commerciale est confiée (ex. : les sociétés agissant pour le compte d'agences de voyages en ligne). Comparativement à l'année 2003 (trente et un contrôles effectués), **le nombre de contrôles progresse mais reste nettement insuffisant**. Il faut toutefois noter que l'activité du service des contrôles a été suspendue pendant cinq mois en raison de l'adoption de la nouvelle loi du 6 août 2004.

Les principales missions de contrôle ont porté sur les secteurs suivants :

a) les applications clientèles mises en œuvre par les banques : vérification des modalités de traitement des informations détenues à partir de la gestion des comptes et des moyens de paiement et des opérations de classement de la clientèle auxquelles les banques procèdent : crédit *scoring*, segmentation comportementale, lutte contre la fraude ;

b) les sociétés de voyage en ligne : examen des systèmes informatiques de gestion de la clientèle, des modalités d'utilisation du courrier électronique comme moyen de communication avec les clients, des mesures de sécurité mises en œuvre et des modalités de traitement spécifiques des données relatives à la carte bancaire ;

c) les salles de sport : vérification des modalités de gestion des fichiers clientèle, en particulier l'enregistrement éventuel d'informations dans des zones « bloc-notes » ou la tenue d'un fichier des « personnes interdites » ;

d) les modalités d'information de la clientèle des contrôles opérés lors d'un paiement par chèque : vérification dans quatre magasins FNAC à Paris des modalités d'information de la clientèle, au moment de son passage en caisse, de la mise en œuvre de systèmes de contrôle des paiements par chèque dont la finalité est de se prémunir contre des impayés irrécouvrables.

En outre, plus spécifiquement, **au vu de plaintes reçues par la Commission :**

– un contrôle a été diligenté auprès d'un des principaux fournisseurs d'accès à internet, Wanadoo, afin de vérifier les modalités de gestion du fichier clients ;
– un contrôle a été opéré auprès d'un office HLM, afin de vérifier l'information portée à la connaissance de la Commission selon laquelle cet organisme enregistrait l'origine ethnique des locataires du parc immobilier qu'il gère.

D'autres missions de contrôle, engagées en 2004 auprès de grandes enseignes commerciales et portant sur les dispositifs de fidélisation de la clientèle, doivent être poursuivies en 2005.

Objectifs et méthodes

Sous l'empire de la loi du 6 janvier 1978, la Commission pouvait déjà charger un ou plusieurs de ses membres ou de ses agents de procéder au contrôle sur place d'un traitement. Toutefois, les chiffres en témoignent, le contrôle *a posteriori* a joué depuis vingt-cinq ans un rôle mineur au sein de l'activité de la CNIL, puisque depuis 1978, elle n'a effectué qu'un peu plus de trois cents missions de vérification.

L'entrée en vigueur de la loi du 6 août conduit à modifier cet état de fait : l'allégement des formalités préalables devant être remplies par tout responsable de traitement de données à caractère personnel, la limitation du régime d'autorisation aux seuls traitements générateurs de risques pour les libertés et l'accroissement des pouvoirs corrélatifs de sanction devraient conduire la CNIL à multiplier les contrôles sur place, appelés désormais à jouer un rôle essentiel dans le cadre de l'une de ses principales missions, *« veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions »* de la loi. À défaut, la réduction des interventions *a priori* de la Commission provoquerait un abaissement du niveau général de protection instauré par le législateur de 1978.

La définition par la CNIL, dès mars 2004, **d'une nouvelle politique des contrôles**, marquée par la volonté d'augmenter significativement les vérifications sur place afin d'aller au plus près des traitements, a anticipé cette modification législative. Il s'agit pour la Commission de déterminer les secteurs d'activité devant faire l'objet de missions de contrôle sur place, que ce soit pour s'assurer du suivi des délibérations ou recommandations de la CNIL, pour répondre à une inquiétude naissante de l'opinion publique, ou encore, plus spécifiquement, pour s'assurer des mesures de sécurité mises en œuvre pour

3. Compte tenu de l'entrée en vigueur de la loi du 6 août 2004, il s'agit tant de délibérations de la CNIL réunie en séance plénière que de décisions du président.

assurer la confidentialité des informations traitées. Bien évidemment, la CNIL continuera à faire des contrôles pour instruire des plaintes ou des réclamations qui lui auront été adressées par des particuliers.

Sans attendre la publication du décret d'application, la CNIL a modifié en novembre 2004 son règlement intérieur pour fixer les procédures de contrôle dans le cadre de la nouvelle loi, en particulier l'établissement du procès-verbal et l'information du procureur de la République territorialement compétent prévus par l'article 44 de la loi. En outre, conformément à l'article 19 de la loi modifiée, certains des agents de la Commission ont été habilités à procéder à des vérifications.

Cette intensification des contrôles sur place est susceptible de se heurter à l'attitude de certains responsables de traitement qui pourraient invoquer le secret professionnel pour ne pas satisfaire les demandes de la délégation de la Commission. Il appartient à la CNIL de rappeler que selon le Conseil constitutionnel, *« l'invocation injustifiée du secret professionnel pourrait constituer une entrave passible des peines prévues par l'article 51 nouveau de la loi du 6 janvier 1978 »* (*cf.* décision du 29 juillet 2004).

LES SANCTIONS

Jusqu'à l'entrée en vigueur de la nouvelle loi «Informatique et Libertés», la CNIL, constatant un manquement à la loi, ne pouvait que délivrer des avertissements à l'organisme en cause ou dénoncer les faits au parquet. La loi du 6 août 2004 l'a dotée de pouvoirs de sanctions administratives et pécuniaires importants.

Le bilan 2004 des sanctions

Les avertissements

Dans le prolongement des six avertissements prononcés en 2003, la CNIL a, au cours de l'année 2004, décidé d'adresser trois nouveaux avertissements à des établissements financiers qui n'avaient pas respecté la réglementation relative au Fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France. Dans le premier cas, la banque avait inscrit à tort l'une de ses clientes au FICP. Dans le second cas, l'établissement avait maintenu l'inscription de sa cliente au FICP alors que l'incident de paiement qui se trouvait à l'origine de l'inscription avait été régularisé depuis plusieurs mois. Dans le troisième cas, la banque avait inscrit l'un de ses clients au FICP le 30 avril 2003 pour un incident de paiement caractérisé datant du 20 avril 1993, soit dix ans auparavant.

Seule l'intervention de la CNIL a permis le «défichage» des personnes concernées qui avaient vainement tenté de l'obtenir auprès de ces établissements. Ces derniers avertissements portent à neuf le nombre total d'avertissements délivrés par la CNIL après constatation du non-respect, par les professionnels de la banque et du crédit, des règles d'alimentation et de fonctionnement du FICP.

La CNIL a également prononcé deux avertissements, le 25 mars 2004 et le 3 juin 2004 à l'encontre de banques qui n'avaient pas pris de précaution suffisante pour assurer la confidentialité des informations concernant leurs clients. Le premier avertissement concernait un établissement financier qui avait adressé des relevés de compte à d'autres personnes que leur titulaire. Dans le second cas, un des clients a pu accéder, *via* internet, en tapant son mot de passe et son code d'accès personnel, au compte d'un autre client.

Les dénonciations au parquet

La CNIL a dénoncé au parquet, le 27 avril 2004, une association qui diffusait sur son site internet une «liste noire» de notaires : les coordonnées de plus de 2 500 notaires français, présentés comme ayant commis des irrégularités ou des malversations, étaient ainsi accessibles sur internet.

Plusieurs notaires avaient demandé à cette association, sur les conseils de la CNIL et sur le fondement de la loi du 6 janvier 1978 qui reconnaît à toute personne le droit de s'opposer, pour des raisons légitimes, à ce que des informations la concernant fassent l'objet d'un traitement automatisé, de retirer leur nom du site. La responsable de l'association en cause n'avait répondu ni à leurs demandes, ni aux courriers de la CNIL et n'avait donc retiré aucun nom de son site.

La CNIL a en conséquence décidé de saisir le parquet de ces faits, sur le fondement de l'article 226-18 du Code pénal qui punit de cinq ans d'emprisonnement et de 300 000 € d'amende le fait de procéder à un traitement d'informations nominatives malgré l'opposition de la personne concernée. Elle a en effet estimé que la diffusion de telles informations pouvait avoir des conséquences graves sur la vie professionnelle des notaires cités et que ceux-ci avaient donc des motifs légitimes à voir leurs noms retirés du site.

Le 15 novembre 2004, le président de la CNIL a également dénoncé au parquet une société qui avait adressé des publicités non sollicitées par voie de télécopies, fait susceptible de constituer l'infraction punie par l'article R. 10-1 du Code des postes et des communications électroniques. L'article L. 34-5 du Code des postes et des communications électroniques interdit en effet l'envoi par télécopie de messages publicitaires, sauf à l'égard des personnes qui auraient spécialement exprimé leur consentement à être ainsi démarchées. L'article R. 10-1 punit de l'amende prévue pour les contraventions de quatrième classe (750 €) tout message de prospection adressé en infraction à ces dispositions. L'article L. 34-5 du Code des postes et des communications électroniques dispose par ailleurs que la CNIL veille au respect des dispositions de cet article. La CNIL avait été saisie de huit réclamations concernant cette société.

Objectifs et méthodes

La CNIL a considéré que les dispositions de la nouvelle loi relatives aux sanctions étaient immédiatement applicables et, sans attendre la parution du décret d'application, a par une délibération du 9 décembre 2004, complété son règlement intérieur par un chapitre spécifique consacré aux procédures de sanction. La Commission

entend en effet pouvoir utiliser rapidement l'ensemble des moyens de contrôle et de coercition mis à sa disposition pour s'assurer de l'application effective de la loi.

Un éventail de sanctions graduées

L'éventail des mesures coercitives et des sanctions tel qu'il est défini au chapitre VII de la loi du 6 janvier 1978 (articles 45 à 49) est large : hormis l'avertissement, la CNIL peut désormais, après une mise en demeure infructueuse et à l'issue d'une procédure contradictoire, prononcer une sanction pécuniaire – à l'exception des traitements mis en œuvre par l'État -, une injonction de cesser le traitement (pour les traitements relevant du régime déclaratif), ou encore retirer son autorisation (pour les traitements soumis à une telle procédure).

En outre, en cas d'urgence et de violation des droits et libertés résultant de la mise en œuvre d'un traitement, la Commission peut décider l'interruption temporaire de celui-ci ou le verrouillage de données (pendant trois mois) à l'exception de certains traitements de l'État et en particulier des traitements dits de souveraineté intéressant la sûreté de l'État, la défense ou la sécurité publique et ceux ayant pour objet la recherche d'infractions pénales ou l'exécution des condamnations, pour lesquels la CNIL a cependant la possibilité d'informer le Premier ministre *« pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée »*.

En cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander en référé au juge d'ordonner toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés. Le montant des sanctions pécuniaires susceptibles d'être infligées peut atteindre 150 000 € lors du premier manquement constaté et 300 000 € ou 5 % du chiffre d'affaire hors taxes du dernier exercice s'il s'agit d'une entreprise dans la limite de 300 000 € (article 47 alinéa 2). Le montant de ces sanctions doit en outre être *« proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement »*.

Enfin, l'éventail des sanctions pénales prévues aux articles 226-16 à 226-24 du Code pénal ne doit pas être oublié, la CNIL conservant bien entendu la possibilité de dénoncer au parquet les infractions à la loi dont elle a connaissance.

Les règles de procédure

Nouveauté introduite par la loi du 6 août, la plupart des mesures coercitives, parmi lesquelles les sanctions pécuniaires, doivent être prononcées, non par la formation plénière de la commission (dont ne relèvent que les décisions de verrouillage des données et d'information du Premier ministre) mais par une formation restreinte composée de six membres (le président, les deux vices-présidents et trois membres élus par la commission en son sein pour la durée de leur mandat).

L'article 46 de la loi modifiée dispose que les sanctions qui relèvent de la compétence de la **formation restreinte** *« sont prononcées sur la base d'un rapport établi par l'un des membres de la CNIL, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte* […] ».

Ce même article précise les dispositions devant être prises pour assurer le respect du principe du contradictoire qui doit sous-tendre la procédure de sanction quelle que soit la formation de la commission qui la prononce. Il est ainsi prévu que le rapport proposant la sanction, soit notifié pour observations au responsable du traitement qui peut se faire représenter ou assister.

Enfin, la loi de 1978 modifiée en 2004 prévoit que la commission peut rendre publics les avertissements qu'elle prononce et en cas de mauvaise foi du responsable du traitement, les autres sanctions notamment en ordonnant leur insertion dans des journaux ou autres supports. Le législateur a ainsi entendu laisser à la CNIL une marge d'appréciation dans la publicité qui doit entourer les sanctions qu'elle prononce.

Les nouvelles dispositions introduites dans le règlement intérieur ont précisé les règles procédurales applicables préalablement au prononcé des mesures et sanctions, qu'il s'agisse de la mise en demeure, décidée en formation restreinte, du respect du contradictoire tant en ce qui concerne l'avertissement que les autres sanctions ou encore des règles de quorum permettant à la commission, réunie en formation restreinte ou en formation plénière, de délibérer valablement.

L'HOMO INFORMATICUS EN 2004

DANS QUELS FICHIERS ?

Ce bref panorama non exhaustif des nouveaux fichiers créés en 2004 permet d'entrevoir la diversité des traitements mis en œuvre en France. Pour certains, ces fichiers concernent un nombre très important de citoyens. D'autres fichiers apparus en 2004 font l'objet d'un développement spécifique dans ce rapport.

Banque/finances

Le fichier des personnes habilitées à procéder au démarchage bancaire ou financier

La CNIL a émis un avis favorable en mars 2004 à un projet de décret relatif à la mise en œuvre d'un fichier des personnes habilitées à procéder au démarchage bancaire ou financier. Ce projet constitue l'un des textes d'application de la loi de sécurité financière qui a profondément réformé le cadre juridique du démarchage bancaire et financier : il stipule que les démarcheurs doivent être enregistrés par leurs mandants ou leurs employeurs auprès des autorités d'agrément. Ce fichier vise à permettre à chacun de vérifier qu'il a affaire à un démarcheur habilité, en particulier à l'occasion de transactions à distance.

Le fichier des conseillers en investissements financiers

Un projet d'établissement de listes de personnes habilitées à exercer la profession de conseiller en investissements financiers (CIF) a également été étudié par la CNIL le 1er juillet 2004 qui a rendu un avis favorable. Les nouvelles dispositions du Code monétaire et financier créent le statut de conseiller en investissements financiers : celui-ci doit adhérer à une association professionnelle agréée par l'Autorité des marchés financiers (AMF). Ces associations centralisent des listes qui sont librement consultables par le public auprès de l'AMF.

Social

La gestion individualisée des bénéficiaires de l'assurance maladie

La CNIL a émis un avis favorable le 1er juillet 2004 au projet soumis par la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) portant sur la refonte du système d'information et notamment de son répertoire des bénéficiaires (assurés et ayants droit). La CNAMTS envisage en effet de mettre en place une base nationale dénommée « référentiel individus national » permettant d'identifier chaque bénéficiaire de l'assurance maladie relevant du régime général ou des régimes partenaires[4] et d'assurer ainsi une gestion individualisée des ouvrants droit et des ayants droit, et non plus une gestion par famille comme c'est actuellement le cas.

Ce traitement tend à éviter les enregistrements multiples de bénéficiaires, de mieux connaître les prestations qui lui sont servies et d'améliorer les échanges de données entre les caisses primaires d'assurance maladie, en particulier lors des changements de caisses de rattachement. Il simplifierait les procédures de délivrance et de mise à jour des cartes Vitale et faciliterait la gestion de l'accueil et des demandes de renseignements quel que soit le mode de contact choisi.

Concernant ce traitement, la CNIL a émis un avis favorable sous réserve que le projet d'acte réglementaire soit modifié de façon à préciser que :
– la duplication de la base de données nationale dans chaque centre informatique régional est limitée aux bénéficiaires de la région concernée ; toutefois les deux centres informatiques de la région Île-de-France pourront détenir les données concernant l'ensemble des bénéficiaires de l'assurance maladie de l'Île-de-France ; la part de la base nationale correspondant à des CPAM qui participent

4. Les régimes partenaires (ou hébergés) sont des régimes qui ont signé une convention avec la CNAMTS pour le règlement des prestations de leurs bénéficiaires : CNMSS (militaire), CAVIMAC (culte), CRPCEN (clercs et employés de notaires).

à une même plate-forme de services interrégionale, pourra être dupliquée dans les bases régionales concernées et dans l'hypothèse où une CPAM aide une autre caisse à résorber son retard en matière de liquidation des feuilles de soins, la caisse qui aide pourra accéder à la part du fichier RFI correspondant à la caisse aidée ;

– l'adresse n'est pas intégrée dans la base de données « RFI nationale ». La CNIL considère qu'eu égard à la finalité poursuivie par le RFI national, la conservation à l'échelon national de l'adresse n'est pas justifiée ; toutefois en cas de changement d'adresse, la CNAMTS est autorisée à enregistrer l'adresse dans la base de données « RFI national », le temps strictement nécessaire à la gestion du changement d'adresse par les caisses concernées et à la transmission du dossier du bénéficiaire à la nouvelle caisse de rattachement.

Le fichier « canicule »

À la suite des terribles conséquences de la canicule de l'été 2003, **le plan « Vermeil »**, prévu par la loi du 30 juin 2004 relative à la solidarité des personnes âgées et handicapées, oblige les maires à procéder au recueil des coordonnées des personnes concernées qui souhaitent bénéficier de ce dispositif de veille et d'alerte. Lors de son déclenchement en cas de risques exceptionnels, ce plan prévoit d'organiser un contact périodique avec les personnes enregistrées afin de leur apporter les conseils et l'assistance dont elles ont besoin.

Dans ce but, un registre communal est créé comportant les nom, prénoms, date de naissance, adresse et numéro de téléphone de la personne inscrite. De plus sont enregistrées les coordonnées du service intervenant à domicile, de la personne à prévenir en cas d'urgence et les nom et qualité de la tierce personne ayant le cas échéant effectué la demande.

Ce registre est constitué par le maire à partir des informations recueillies auprès des organismes de Sécurité sociale (caisses primaires d'assurance maladie, mutualité sociale agricole, caisses d'assurance maladie régionales des professions indépendantes) ou par extraction des fichiers sociaux communaux retenant les personnes âgées de plus de 65 ans. Les informations transmises se limitent aux nom, prénoms, civilité et adresse de ces personnes, ce qui permet de les contacter pour leur demander si elles veulent figurer dans le registre.

Les personnes contactées sont expressément informées par la collectivité des modalités d'obtention de leurs coordonnées. L'inscription des données figurant dans le registre est alors réalisée à l'initiative soit de la personne concernée, soit d'un tiers (famille, voisins, proches, professionnels médicaux ou paramédicaux, etc.).

Les destinataires des informations, qui en assurent la sécurité et la confidentialité, sont tenus au secret professionnel.

Afin de préserver la tranquillité des personnes âgées et handicapées, la CNIL a appelé l'attention du ministère sur la nécessité de limiter les transmissions des données du registre aux seuls agents disposant d'une compétence particulière dans le domaine social ou sanitaire et de ne pas en multiplier les destinataires départementaux ou locaux seuls désignés par le préfet.

Les garanties demandées par la CNIL ont été intégrées au décret du 1er septembre 2004.

Santé

Une base de données génétiques anonymisées accessible sur internet

Le 4 mars 2004, la CNIL a émis un avis favorable à la mise en place, par le laboratoire de génétique de l'université Joseph-Fourier de Grenoble, d'une base de données commune sur les maladies génétiques, accessible sur internet, en vue d'améliorer la connaissance de ces maladies.

À l'occasion du diagnostic d'une maladie génétique, les médecins ont la possibilité de créer des dossiers de personnes et de transmettre sous un identifiant individuel anonymisé et avec l'accord exprès du patient, des informations centralisées dans une base de données accessible uniquement aux médecins et chercheurs leur permettant ainsi d'offrir une aide au diagnostic et au conseil génétique.

Les informations médicales relatives aux autres membres de la famille du patient concerné ne sont enregistrées dans la base que dans la mesure où elles auront été obtenues directement auprès de ces personnes et le patient lui-même ne peut accéder qu'aux seules données le concernant auprès d'un médecin généticien habilité, à l'exclusion de celles qui concernent d'autres membres de la famille.

QUELLES TRACES ?

Téléphone, internet, billétique, monétique font partie de notre vie courante. L'utilisation de ces outils facilite souvent notre quotidien, mais il faut savoir qu'à chaque fois que nous avons recours à ces systèmes, nous laissons une trace.

Pour étudier les traces de l'*Homo Informaticus*, nous vous proposons d'en suivre un spécimen, du lever au coucher, et d'identifier les traces qu'il laisse, consciemment ou inconsciemment, tels de petits cailloux sur son passage.

Paul se réveille à 6 heures 30. Après un petit-déjeuner en famille, il accède au sous-sol de son immeuble à l'aide de son **badge** pour aller chercher sa voiture au parking et il allume **son téléphone portable** qui ne le quittera pas de la journée. Il dépose sa femme Valérie à la gare qui, pour se rendre sur son lieu de travail, utilise les transports en commun : sa **carte de transport** est au fond de son sac à main et à l'approche du portillon, il lui suffit de passer son sac sur le lecteur.

Pour éviter les embouteillages, Paul emprunte un tronçon d'autoroute payant. Il est abonné à l'année et possède **un pass** qui enregistre ses passages à chaque péage. Il arrive au pied de la tour qui abrite les bureaux de son entreprise dans un quartier d'affaires de l'ouest parisien. Il lui faut utiliser son **badge d'entreprise** pour accéder au parking. Comme dans les autres tours, des **caméras** sont installées un peu partout et reliées au PC Sécurité. Paul doit garder son badge à portée de main puisqu'il devra encore s'en servir pour **« badger »** dans l'ascenseur. Le badge est un sésame sans lequel rien n'est possible. Il sert aussi à régler son repas au restaurant d'entreprise.

Une fois dans son bureau, Paul se connecte à sa **messagerie électronique** et se rend sur **internet** pour consulter les titres de la presse économique. Il se rend ce matin à un salon professionnel qui se tient dans le quartier d'affaires. Il s'enregistre auprès d'une borne qui lui donne en retour **un badge d'accès au salon**. Paul sait déjà qu'il ne tardera pas à recevoir des sollicitations de la part des exposants ou d'autres entreprises ayant fait l'acquisition du fichier des participants. À chaque stand visité, on lui demande **sa carte de visite**. Certains lui proposent même de transférer son contact directement depuis **son assistant personnel**. Paul a ensuite rendez-vous avec un client qu'il invite à déjeuner. Il paie avec **sa carte de crédit**.

Retour au bureau. Sa messagerie est encombrée de **« spams »** depuis que son nom figure parmi la **liste des contacts du site internet de son entreprise.** Les « spams » commencent même à envahir **son téléphone portable.** Paul s'accorde 5 minutes pour **réserver en ligne** des billets de train. À l'issue de sa commande, on lui demande s'il est d'accord pour recevoir la *newsletter* et les offres promotionnelles en avant-première. Il doit répondre à des questions relatives à ses loisirs, la composition de son foyer, ses habitudes de consommation. Paul se demande si tout cela est bien nécessaire mais il répond néanmoins à ces questions qui ne sont pas obligatoires.

Paul rentre à la maison vers 19 heures. Le téléphone sonne. On propose à Paul de profiter d'une offre exceptionnelle pour changer les fenêtres de sa maison. Hier, son opérateur de téléphonie mobile lui suggérait de changer sa formule d'abonnement. Même si Paul s'y connaît en **prospection commerciale** – c'est son métier – il préfère être tranquille le soir à la maison. Il regarde sur la table du salon le courrier du jour : **ses relevés bancaires, une attestation de remboursement de soins médicaux, la taxe d'habitation**, et enfin **un relevé d'achats par correspondance** effectués par Valérie avec sa carte « Éléphant ».

Paul s'endort ce soir après avoir regardé un film sur sa télévision équipée **d'un boîtier numérique**, sans se douter du nombre de traces semées ici ou là pendant toute cette journée, laissées volontairement ou non, susceptibles d'être utilisées pour alimenter de nombreux fichiers.

Bien entendu, il a laissé tout au long de ce périple quotidien quelques milliers d'empreintes de ses dix doigts. Mais, comme il s'en fait la remarque avant de sombrer dans le sommeil : il n'a rien à se reprocher… lui non…

À propos des fichiers

FNCI

Le Fichier national des chèques irréguliers (FNCI) recense les coordonnées des comptes clos, des comptes dont le titulaire est frappé par une interdiction d'émettre des chèques ainsi que les oppositions pour perte ou vol de chèques.

« Je vais payer en caisse d'un magasin : quels contrôles ? »

Lorsqu'un client paye en espèces à la caisse d'un magasin, il ne laisse aucune trace sur son identité ou sur la nature de sa transaction. Le paiement par chèque ou par carte bancaire se caractérise au contraire par l'enregistrement de données nominatives parfois insoupçonnées.

Par exemple, le paiement par chèque à la caisse d'un magasin fait l'objet de contrôles dont la plupart des consommateurs ignorent l'existence et dont la finalité est d'apprécier l'opportunité d'accepter ou de refuser le chèque afin de permettre au commerçant d'éviter des impayés. Bien sûr, ces contrôles ne sont pas systématiques et chaque commerçant décide d'y procéder ou non.

Ainsi, le remplissage automatique du chèque par une imprimante permet certes de faciliter la vie du client mais aussi et surtout de procéder à de nombreuses vérifications. L'imprimante est en effet dotée d'un lecteur optique chargé d'analyser l'information contenue dans la piste CMC7 du chèque, suite numérique située en bas de celui-ci donnant de nombreuses informations sur le porteur.

Une fois déchiffrées, les informations contenues dans la piste CMC7 permettent au système informatique du commerçant de procéder à plusieurs contrôles, soit sur son propre système informatique, soit en sollicitant des informations auprès de tiers.

Les vérifications effectuées auprès du FNCI

Le législateur a confié à la Banque de France la gestion du Fichier national des chèques irréguliers (FNCI). Tout commerçant peut accéder à ce fichier[5]. La réponse obtenue du Fichier national des chèques irréguliers, à partir de la transmission des données figurant sur la ligne codée en bas du chèque (piste CMC7), prend la forme d'un code couleur :

vert : aucune information recensée dans le fichier concernant le chèque ;

rouge : chèque irrégulier (compte dont le titulaire est frappé d'une interdiction bancaire ou judiciaire ; formule de chèque recensée au titre d'une opposition pour perte ou vol ; compte clôturé ; faux chèque) ;

orange : compte déclaré au titre d'une opposition pour perte ou vol auprès du Centre national d'appel des chèques perdus ou volés, ou du banquier (les numéros des chèques concernés n'ont pas encore été précisés dans le FNCI) ;

blanc : réponse impossible (lecture de la piste CMC7 impossible ; établissement teneur de compte inexistant ; coordonnées transmises inexistantes).

Les vérifications effectuées dans le système informatique du commerçant

Le client a-t-il un impayé dans le magasin ?

En analysant le numéro de compte figurant sur la piste CMC7, le système informatique identifie les personnes dont la remise d'un précédent chèque tiré sur le même compte fait l'objet d'un impayé non régularisé.

Le chèque est-il susceptible d'être « flambant » ?

Il s'agit d'une nouvelle fraude sur le chèque, réalisée principalement avant l'alimentation du FNCI et détectée

5. Un fichier identique est utilisé pour les paiements par carte bancaire (fichier « centralisation des retraits de cartes bancaires »).

N° de compte : sur douze positions.

Code Banque : 4 caractères à partir de la sixième position ici 7806.

N° du chèque : sur sept positions.

par la constatation d'une utilisation massive d'un chéquier sur un laps de temps très court et parfois sur tout le territoire national. Afin de s'en prémunir, les commerçants vérifient le nombre de paiements effectués par chèques dans leur magasin (ou dans une chaîne de magasins), sur la base du même numéro de compte, durant la période récente. Si le nombre de chèque émis est excessif, il peut s'agir d'un « flambant ». La Banque de France mène actuellement une expérimentation sur ce sujet afin d'apprécier l'opportunité de modifier le FNCI.

Les vérifications effectuées auprès d'une société de garantie

Certaines sociétés privées proposent également aux commerçants un autre contrôle qui prend la forme d'un calcul du risque statistique de chaque opération réglée par chèque. Ce calcul de risque s'appuie à la fois sur une analyse de l'historique des transactions ayant fait l'objet d'une demande de garantie par un commerçant et sur l'utilisation d'une grille de score appliquée à différents éléments objectifs concernant la transaction et le client (banque du client, heure et montant de l'achat, type de commerce concerné, type de pièce d'identité présentée et région de l'achat, etc.). Chaque élément se voit appliquer une pondération spécifique et la société de garantie de chèques calcule pour chaque opération un score. Selon le score obtenu, elle accepte ou non de garantir le paiement si le commerçant accepte le chèque. Au cas où le chèque garanti par cette méthode serait ultérieurement rejeté par la banque du client, le commerçant est dédommagé.

B O N À S A V O I R

Suite à l'adoption de la loi portant mesures urgentes de réformes à caractère économique et financier (MURCEF), les principaux établissements financiers se sont engagés, dans une charte signée le 9 janvier 2003 à proposer à leurs clients une convention de compte précisant le fonctionnement de leur compte de dépôt et les modalités d'utilisation de leurs données personnelles. Le client doit donc lire attentivement, avant de signer, la convention de compte qui précise, au minimum, les finalités des traitements mis en œuvre par la banque, les destinataires des données personnelles qui le concernent et qui sont protégées par le secret bancaire, le droit de ce client de s'opposer à un traitement de données à des fins de prospection commerciale ainsi que les modalités d'exercice du droit d'accès aux données qui le concernent.

« Que sait mon banquier sur moi ? »

Les informations détenues par mon banquier

Monsieur K. souhaite ouvrir un compte bancaire. Il se rend dans une agence et rencontre un conseiller de clientèle. Afin de pouvoir ouvrir le compte, M. K. va être invité à communiquer un certain nombre d'informations le concernant afin que celles-ci soient enregistrées dans le système informatique de la banque. Ces informations sont souvent nombreuses et de natures différentes :
– informations d'identification : nom, prénom, adresse postale, date et lieu de naissance, etc. ;
– informations financières : revenus, logement, patrimoine, informations fiscales, avoirs détenus à la concurrence, etc. ;
– informations professionnelles : formation, diplômes, métier, nom de l'employeur, etc. ;
– informations familiales : situation de famille, nombre d'enfants, etc.

La CNIL surveille

La CNIL surveille la mise en œuvre de l'ensemble de ces systèmes de contrôle des paiements et s'assure que ceux-ci respectent la réglementation « Informatique et Libertés », s'agissant en particulier de l'information des clients aux caisses des magasins.

La CNIL rappelle

Le client d'une banque n'est pas obligé de répondre à l'ensemble des questions qui lui sont posées : il dispose d'un droit d'opposition et doit par ailleurs être informé du caractère facultatif ou obligatoire des questions posées. La CNIL vérifie également que les informations enregistrées par le banquier dans une fiche client ne sont pas interdites par la loi « Informatique et Libertés ». Par exemple, il est interdit, sauf exception, de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciale ou éthnique, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, qui sont relatives à la santé ou la vie sexuelle de celles-ci.

Qu'est-ce que c'est ?

La segmentation comportementale

La segmentation comportementale permet, à partir d'informations sur les comportements observés, d'établir le profil socio-économique, voire psychologique, d'une personne, laquelle sera ensuite classée dans un « segment ». Le segment dans lequel est classé le client correspond généralement à une note ou un verbe d'action tel que : « À privilégier », « À découvrir ». La CNIL vérifie systématiquement que les systèmes de segmentation comportementale ne portent pas atteinte à la vie privée du client (par exemple le banquier n'est pas autorisé à analyser le détail des opérations financières de son client chez des commerçants lorsqu'il règle par carte bancaire) et que les segments utilisés ne sont pas péjoratifs.

La « zone bloc-notes »

La banque garde souvent en mémoire des informations factuelles d'ordre commercial comme, par exemple, le résumé des entretiens avec le client et son conseiller. Celui-ci peut ainsi s'y référer lors d'un prochain contact ou pour contrôler l'état d'avancement d'un dossier ou d'une procédure. La CNIL contrôle régulièrement le contenu des « blocs-notes » et s'assure que les informations contenues sont objectives, en lien direct avec la gestion du compte, qu'elles ne portent pas atteinte à l'intimité de la vie privée du client ou à sa dignité et qu'elles ne contiennent pas des informations interdites (origine raciale, données de santé ou relatives aux mœurs, etc.).

Le *scoring*

Sur la base de variables prédéfinies (nombre d'enfants à charge, situation au logement et date d'entrée à l'adresse, ancienneté dans l'ouverture du compte bancaire, etc.) et de pondérations, une note censée représenter un certain niveau de risque est attribuée au client. Plus la note est basse, plus la vigilance de la banque à l'égard de son client sera grande.

C'est votre droit

Tout client bénéficie d'un droit d'accès aux données personnelles qui le concernent. La Fédération bancaire française (FBF), en collaboration avec la CNIL, vient ainsi de publier un mini guide sur le droit d'accès dans le secteur bancaire. Ce mini guide est accessible, ainsi que bon nombre d'autres informations, dans la rubrique « banque » du site internet de la CNIL : (www.cnil.fr).

« J'ai souscrit une carte de fidélité »

Un magasin dont vous êtes un client habituel vous a proposé de devenir un client privilégié en adhérant à son programme de fidélité. Les avantages de cette démarche vous ont été clairement exposés : l'utilisation de votre carte de fidélité vous permettra de cumuler des points vous ouvrant droit à des remises, à des bons d'achat, à des cadeaux …Cependant l'avantage ainsi accordé comporte une contrepartie qui n'est pas toujours clairement identifiable pour le consommateur.

Le point sur … les cartes de fidélité

Quelle contrepartie tire un magasin de la mise en place d'une carte de fidélité ?

L'avantage consenti par une entreprise mettant en œuvre un système de fidélisation est conditionné à une perte de son anonymat pour le client. Lors de la souscription de la carte de fidélité le client est amené à remplir un formulaire sur lequel lui sont demandées certaines informations à caractère personnel : nom, prénoms, adresse mais aussi sa situation familiale, ses habitudes de consommation, ses loisirs …

Quelles sont les données traitées dans le cadre d'un système de fidélisation ?

Les données détenues par une enseigne ne se limitent pas à celles figurant sur le formulaire de souscription. Leur base de données s'enrichira au fur et à mesure de l'utilisation de la carte. Ainsi pourront être conservées les données relatives au montant des achats effectués, à la nature et au lieu de ces achats, etc. La connaissance de la clientèle pourra être complétée grâce à un recoupement avec d'autres fichiers. L'enseigne pourra ainsi mettre à jour les adresses de ses clients en cas de déménagement …

En quoi ces données sont-elles utiles à l'entreprise ?

Ces données seront ensuite traitées par l'enseigne pour lui permettre de réaliser des opérations de prospection commerciale mieux ciblées. Pour ce faire les clients seront répartis en segments en fonction de leurs réponses ; ils se verront également attribuer des scores c'est-à-dire une note en fonction de variables prédéterminées comme par exemple leur adresse. Ces procédés permettent aux entreprises de

La CNIL veille

Dans la mesure où les contrôles effectués par les banques concernant leurs clients peuvent avoir pour conséquence d'exclure une personne de l'ouverture d'un compte bancaire ou de l'octroi d'un crédit, la CNIL veille à ce que les variables utilisées par les outils de contrôle soient conformes à la loi « Informatique et Libertés ». Ces fichiers doivent être autorisés par la CNIL pour être mis en œuvre.

Questions à …

Philippe NOGRIX

Sénateur de l'Ille-et-Vilaine
Commissaire en charge du secteur « Monnaie et crédit »

Comment un banquier utilise-t-il les informations qu'il détient sur ses clients ?

Les informations que possède le banquier servent principalement à trois choses : la gestion du compte, la réalisation d'opérations commerciales, la gestion du risque.

• La gestion du compte au quotidien :

La banque utilise les données personnelles qu'elle détient sur son client afin de pouvoir faire correctement fonctionner son compte : fabrication des chéquiers ou de la carte bancaire, réalisation des virements, envoi du relevé de compte à domicile, etc.

• Les opérations commerciales :

Les données personnelles permettent à la banque de mieux comprendre le fonctionnement d'un compte bancaire et d'adresser au client des propositions commerciales adaptées (nouvelle carte de paiement, offre de crédit ou d'assurances, etc.). À cette fin, la banque utilise des techniques dites de « segmentation comportementale » qui la conduisent à personnaliser ses offres commerciales, identifier les clients à forte potentialité, et, d'une façon générale à améliorer sa rentabilité. La banque utilise aussi le contenu des entretiens qu'elle a avec un client et qu'elle conserve souvent dans un « bloc-notes ».

• L'évaluation du risque :

Lors de l'ouverture d'un compte ou lorsqu'un client demande un produit bancaire (moyens de paiement, crédit, etc.), la banque souhaite généralement s'assurer que la prise de risque liée à la réalisation de l'opération demandée est limitée. Pour apprécier ce risque, la banque utilise les données qu'elle détient sur son client de plusieurs façons :

– la banque est habilitée à consulter plusieurs fichiers centraux détenus par la Banque de France (FCC et FICP), afin de vérifier si le client n'a pas rencontré des difficultés dans l'utilisation de ses moyens de paiement ou dans le remboursement d'un crédit ;

– chaque banque interroge généralement un fichier interne de risque qui référence les clients vis-à-vis desquels une difficulté a pu être rencontrée : incidents de paiement, etc. ;

– les banques sont tenues par la loi de s'assurer que les opérations financières qu'elles engagent ne sont pas utilisées pour financer des activités de financement du terrorisme ou de blanchiment d'argent. En général, elles ont mis en place des systèmes automatiques de surveillance des comptes qui analysent la cohérence des flux financiers enregistrés sur les comptes de ses clients et qui génèrent des alertes (par exemple en cas de virement vers certains pays, d'opérations financières dépassant un seuil prédéfini, etc.). ;

– les banques réalisent aussi un scoring, c'est-à-dire un calcul automatisé de l'appréciation du risque lié à un client.

mieux communiquer vers leur clientèle ; ainsi, s'il ressort de l'historique de votre consommation que vous avez acheté des produits au rayon bébé, il sera possible pour une enseigne de déterminer que vous avez un enfant et de vous proposer des offres concernant du matériel de puériculture.

À propos des fichiers

Le FCC

Le fichier central des chèques recense les personnes faisant l'objet d'un incident de paiement de chèque pour défaut de provision, les interdictions bancaires ou judiciaires d'émettre des chèques, ainsi que les décisions de retrait de cartes bancaires.

Le FICP

Le fichier des incidents de remboursement des crédits aux particuliers recense les incidents de paiement caractérisés liés aux crédits accordés à des personnes physiques pour des besoins non professionnels ainsi que les situations de surendettement.

À qui ces données sont-elles destinées ?

Ces informations sont normalement destinées à l'enseigne ayant mis en place le système de fidélité. Cependant il lui est toujours possible de céder vos données si vous avez été préalablement informé et mis en mesure de vous y opposer. Par ailleurs, dans le cadre de programmes conçus en partenariat entre plusieurs grandes enseignes, les informations relatives au client de la société A pourront être transmises aux sociétés B, C et D partenaires du programme. Dans ce cas, le client de A pourra recevoir des prospections en provenance B, de C ou encore de D. Certains systèmes de fidélisation reposent ainsi sur des bases de données centralisées dans lesquelles sont déposées toutes les données relatives à l'ensemble des clients de tous les partenaires.

Comment se protéger d'éventuels abus

La loi « Informatique et Libertés » reconnaît des droits aux personnes : droit à l'information sur les finalités du traitement et les destinataires des données, droit d'accès qui permet à la personne fichée de demander à l'enseigne quelles sont les données à caractère personnel qu'elle détient, droit de s'opposer au traitement des données et à leur cession à des organismes extérieurs.

QUELLES DÉRIVES ?

Le cas des fichiers de police

Depuis sa création, la CNIL a reçu **10656 demandes de droit d'accès indirect** qui ont donné lieu à plus de **17000 investigations**. En 2004 la Commission a été confrontée à une hausse spectaculaire des saisines : 70% en un an (soit 1970 requêtes) alors même que ses moyens n'ont pas augmenté. Au cours de l'année 2004, 2457 vérifications ont été effectuées dont 89% opérées dans les fichiers du ministère de l'Intérieur.

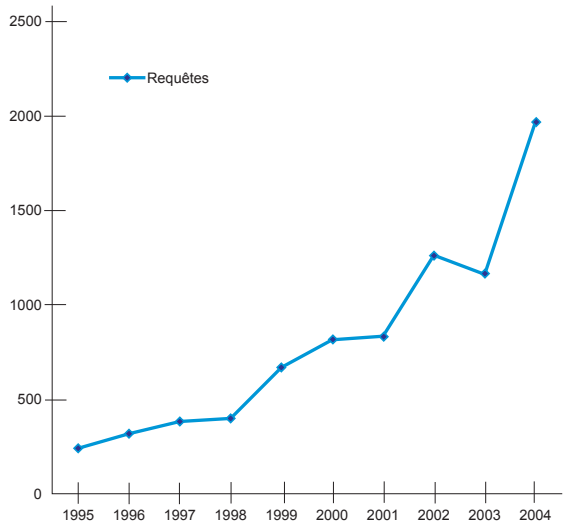
La recherche, par les services du ministère de l'Intérieur et la CNIL, d'une éventuelle fiche porte non seulement sur les fichiers nationaux de police mais également sur les fichiers locaux des commissariats ou des services des renseignements généraux, ce qui prend parfois plusieurs mois et impose de nombreuses investigations notamment pour le contrôle des mises à jour et des suppressions. À titre d'exemple, les **1970 demandes reçues en 2004** induisent plus de 5000 vérifications portant sur les données informatisées mais aussi sur tous les dossiers « papier » à l'origine de l'enregistrement (compte rendu d'enquête, procès-verbal d'audition ...) et détenus dans les directions départementales et régionales des services de police. En l'état actuel de ses moyens, la CNIL a la capacité d'effectuer environ 2500 vérifications par an.

C'est votre droit

Le droit d'accès indirect

En application de l'article 41 de la loi de 1978 modifiée en 2004, toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique. Aucun fichier de cette nature n'échappe à ces vérifications.

Évolution des demandes de droit d'accès indirect reçues depuis 1995



Ce travail de vérification nécessite de la part des services concernés du ministère de l'Intérieur et du ministère de la Défense un travail de regroupement des différentes pièces conservées tant au niveau local que central.

La forte progression constatée en 2004 est la conséquence directe et logique des décisions prises en 2001

Questions à ...

Guy ROSIER

Conseiller-maître honoraire à la Cour des comptes
Commissaire en charge notamment du droit d'accès indirect

Qu'est-ce qui conduit les personnes à s'adresser de plus en plus à la CNIL pour exercer leur droit d'accès aux fichiers de police et de gendarmerie ?

L'augmentation importante des demandes d'exercice du droit d'accès présentée par les citoyens à la CNIL est imputable aux refus d'assermentation, d'autorisation de port d'armes de sécurité ou d'embauche (par exemple dans les sociétés de gardiennage) ou encore des licenciements résultant d'enquêtes administratives défavorables.

La simple et seule consultation d'un fichier de police peut conduire, sans plus d'éléments, à ne pas renouveler un contrat de travail ou à rejeter une candidature, alors même que, comme cela est constaté régulièrement par la CNIL, ces décisions sont prises sur la base des signalements parfois injustifiés ou périmés.

D'autres demandes peuvent aussi résulter d'un refus de délivrance de visa, d'une interpellation par les services de police ou de la gendarmerie, ou sont suscitées par des informations publiées dans la presse, ou diffusées à l'occasion d'émissions télévisées ou sur internet, ou encore relèvent de la simple curiosité.

À propos des fichiers

STIC

Le « système de traitement des infractions constatées » (STIC) est un fichier central de police judiciaire tenu par la Direction générale de la police nationale, sous le contrôle du procureur de la République compétent. Ce fichier répertorie des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause dans ces procédures et les victimes des infractions concernées.
Au 1er janvier 2004, le STIC recensait :
– plus de 23,5 millions de procédures ;
– plus de 26 millions d'infractions ;
– plus de 5 millions d'individus mis en cause ;
– plus de 18 millions de victimes ;
– plus de 8 millions d'objets.

JUDEX

Le « système d'information judiciaire JUDEX » est un fichier similaire au STIC, tenu par la Gendarmerie nationale. Cette application centralisée comprend trois bases différentes : « JUDEX-AFFAIRES » et « JUDEX-PERSONNES MISES EN CAUSE », qui recensent, respectivement, les dossiers décrivant des affaires judiciaires traitées par la gendarmerie et des dossiers relatifs à des personnes mises en cause dans des affaires judiciaires. Ces deux traitements sont mis en œuvre au niveau national. Le traitement « JUDEX-GROUPEMENT », qui lui est mis en œuvre de façon déconcentrée dans chaque département, regroupe des informations sur les affaires et les personnes mises en cause dans le département concerné. Les personnels de la police peuvent accéder aux informations figurant dans le fichier JUDEX et ceux de la Gendarmerie nationale peuvent accéder à celles enregistrées dans le STIC.

et 2003 par le législateur pour encadrer plus étroitement les conditions de recrutement aux emplois touchant à la sécurité. En effet, depuis les lois du 15 novembre 2001 sur la sécurité quotidienne et du 18 mars 2003 sur la sécurité intérieure, les enquêtes administratives réalisées pour l'accès à certaines catégories d'emploi publics ou privés relevant notamment du domaine de la sécurité ou de la défense donnent lieu à consultation de fichiers nationaux de police judiciaire, **STIC** et **JUDEX**.

Tout fichier de grande dimension engendre naturellement des erreurs. Dans le cas du STIC, les erreurs telles que celles qui viennent d'être citées en exemple n'ont pas de graves conséquences quand le fichier est utilisé conformément à sa vocation initiale, l'enquête policière, car celle-ci amènera nécessairement à vérifier tous les faits. Tel n'est pas le cas de la consultation du fichier dans le cadre d'enquêtes administratives, qu'ont autorisée les lois sur la sécurité quotidienne et sur la sécurité intérieure. L'infaillibilité du fichier est rarement mise en doute. Le « signalement » tombe comme un couperet. Et pourtant … Depuis le dernier trimestre 2004, le ministère de l'Intérieur a mis en œuvre un programme automatique d'épurement des données touchées par la limite de durée de conservation. La mise en œuvre de cette procédure automatique en octobre et novembre 2004 a abouti à la suppression de 1 241 742 fiches relatives à des personnes mises en cause.

Ça la **fiche** mal

Gros plan sur le STIC

➤ Un agent d'exploitation aux aéroports de Paris, lors d'une enquête d'assermentation, a appris qu'il était fiché. Il était, en effet, signalé dans le STIC en tant qu'auteur de violences avec arme par destination, alors qu'il était intervenu pour interpeller quelqu'un dans l'exercice de ses fonctions ; la CNIL a obtenu la suppression de ce signalement.

➤ Un agent du département environnement et sécurité de la RATP s'était vu refuser une autorisation de port d'arme de service, étant signalé dans le STIC pour de vol simple. Il avait été interpellé par une patrouille de police alors qu'il transportait dans sa voiture des cadres de fenêtres ramassés sur la voie publique, pensant qu'ils avaient été déposés là pour être enlevés par les services de la voirie. En l'absence de plainte ; il avait toutefois été convoqué au tribunal dans le cadre d'une procédure de médiation pénale. Le signalement a été supprimé à la demande du procureur de la République, saisi par la CNIL.

➤ Une personne dans une situation très précaire, bénéficiant du RMI depuis plusieurs années, se voyait refuser toute embauche en tant qu'agent de sécurité. Elle était signalée dans le STIC pour deux affaires (vol simple et violences volontaires légères). Ces deux signalements ont été supprimés car dans la première affaire, la personne n'était pas mise en cause et dans la deuxième, les faits constitutifs d'une contravention de quatrième classe n'étaient pas susceptibles de donner lieu à enregistrement dans le STIC.

➤ Un postulant au concours de gardien de la paix s'était vu refuser cet emploi au motif qu'il était signalé dans le STIC comme « mis en cause » dans une affaire de recel d'objet volé datant de 1994. La CNIL a saisi le procureur de la République du tribunal de grande instance auquel avait été, semble-t-il, transmise la procédure pour connaître la suite judiciaire. Or, il est apparu qu'aucune procédure se rapportant à cette affaire n'avait été enregistrée. Il a donc été procédé à l'effacement du signalement dans le STIC.

➤ Un jeune homme de 25 ans, en formation pour devenir agent de la surveillance à la SNCF, était signalé dans une affaire de dégradations de biens privés qui avait donné lieu à un classement sans suite pour insuffisances de charges. À la demande du procureur, saisi par la CNIL, il a été procédé à la radiation de la fiche de police judiciaire.

Les fichiers visés par les vérifications faites en 2004 au titre du droit d'accès indirect

Ministère de l'Intérieur	2 175
– Renseignements généraux (RG)	682
– Police judiciaire (PJ)	638
– Sécurité publique (SP)	257
– Direction de la surveillance du territoire (DST)	50
– Système d'information Schengen (SIS)	548
– Direction de la sûreté et de la protection du secret du CEA (DSPS)	–
Ministère de la Défense	**282**
– Gendarmerie nationale (GEND)	231
– Direction de la protection et de la sécurité de la défense (DPSD)	26
– Direction générale de la sécurité extérieure (DGSE)	25
Total	**2 457**

Les fichiers autres que ceux des renseignements généraux, de la police judiciaire (STIC) et de Schengen

Les investigations menées en 2004 sur les fichiers autres que ceux des renseignements généraux, de la police judiciaire-STIC et du système d'information Schengen sont au nombre de 589 ; le résultat est le suivant :

Fichiers	SP	DST	DSPS	GEND	DPSD	DGSE	Total
Pas de fiche	139	37	–	147	16	20	359
Fiche sans suppression	116	13	–	76	10	5	220
Suppression totale ou partielle	1	–	–	5	–	–	6
Mise à jour	1	–	–	3	–	–	4
Total	257	50	–	231	26	25	**589**

Le fichier de la police judiciaire (STIC)

Pas de fiche	145
Signalement en tant que mis en cause sans suppression	187
Signalement en tant que mis en cause supprimé en partie	3
Signalement en tant que mis en cause supprimé	64
Signalement en tant que victime sans suppression	233
Signalement en tant que victime supprimé	6
Total	**638**

La CNIL vous défend

Les investigations dans le fichier STIC ont conduit la CNIL à faire procéder dans 26 % des cas (67 saisines sur les 254 requérants fichés en tant que mis en cause) à des mises à jour (3) ou à la suppression (64) de signalements erronés, manifestement non justifiés ou dont le délai de conservation était expiré.

Les fichiers des renseignements généraux

Le décret du 14 octobre 1991 a fixé les modalités d'exercice du droit d'accès aux fichiers des renseignements généraux et de communication des informations.

En pratique, trois situations peuvent se présenter :

1) si les renseignements généraux ne détiennent aucune information nominative concernant un requérant, la CNIL en informe alors ce dernier, en accord avec le ministre de l'Intérieur ;

2) si les renseignements généraux détiennent des informations nominatives concernant un requérant qui ne mettent pas en cause la sûreté de l'État, la défense et la sécurité publique, celles-ci lui sont communiquées, en accord avec le ministre de l'Intérieur : le requérant peut alors demander d'éventuelles suppressions ou mises à jour des données ;

3) si les informations concernent la sûreté de l'État, la défense et la sécurité publique, elles ne sont pas communiquées au requérant qui se voit cependant informé, par la CNIL, qu'il a été procédé aux vérifications. Il convient de noter que lors de ces vérifications, le magistrat de la CNIL en charge des investigations, procède à un examen approfondi du dossier et demande, s'il y a lieu, aux lieu et place du requérant la rectification ou l'effacement de données.

Les investigations de la CNIL portent à la fois sur le fichier informatique d'indexation et sur le dossier individuel, sur les extraits des dossiers collectifs contenant des données nominatives relatives aux demandeurs, ainsi que sur les dossiers conservés dans les sections spécialisées de la direction centrale des renseignements généraux.

Le résultat des 682 investigations menées en 2004 dans les fichiers des RG est le suivant :

	Investigations aux fichiers des RG	% sur le nombre de requérants
Requérants non fichés aux RG	510	75 %
Requérants fichés aux RG	172	25 %
Total	682	**100 %**

Sur les 172 requérants fichés, 157 dossiers ont été communiqués soit 91%. Il doit être relevé que, de même que les années précédentes, le ministre de l'Intérieur n'a refusé aucune des propositions de communication de dossier faites par les magistrats de la CNIL. Parmi les 157 communications effectuées en 2004, seuls quatre requérants ont présenté des observations qui ont donné lieu à des suppressions ou modifications.

Par ailleurs, il a été procédé à la suppression totale de 21 dossiers et à la suppression partielle de 3 dossiers.

Évolution des investigations aux RG depuis 2000

Année	2000	2001	2002	2003	2004
Nombre de demandes traitées	365	576	1012	686	682
Absence de fiche	261	415	776	443	510
% sur le total	71%	72%	76%	65%	75%
Nombre de requérants fichés aux RG	104	161	236	243	172
% sur le total	29%	28%	23%	35%	25%
Dossiers non communicables	18	35	36	26	15
% sur le nombre de fichés	17%	22%	15%	11%	9%
Communication acceptée par le ministre de l'Intérieur	86	126	200	217	157
% sur le nombre de fichés	83%	78%	85%	89%	91%
Communication totale	85	126	199	217	157
Communication partielle	1	–	1	–	–

Les investigations au système d'information Schengen

Depuis l'entrée en vigueur du décret du 6 mai 1995 relatif au système informatique national du système d'information Schengen dénommé N-SIS, la CNIL a traité 3002 demandes de droit d'accès (dont 548 au cours de l'année 2004).

Évolution du nombre de demandes de droit d'accès au N-SIS par année

	Nombre	Total cumulé
2000	397	897
2001	297	1194
2002	661	1855
2003	599	2454
2004	548	3002

Sur les 3002 demandes de droit d'accès indirect au système d'information Schengen, 913 personnes étaient signalées.

Ces 913 signalements proviennent par ordre décroissant des pays suivants

Pays signalant	Nombre de signalements	par rapport au nombre de signalements
Allemagne	372	41,0%
France	365	40,0%
Italie	119	13,0%
Espagne	31	3,0%
Grèce	15	1,5%
Pays-Bas	6	0,6%
Belgique	2	0,35%
Autriche	2	0,35%
Suède	1	0,20%
Total	913	**100**%

À la suite des démarches entreprises par la CNIL, 337 signalements ont été supprimés du N-SIS (soit 37%) dont 242 par l'Allemagne, 64 par la France, 17 par l'Italie, 7 par l'Espagne, 3 par les Pays-Bas, 1 par la Belgique, 3 par la Grèce.

Quand aucun signalement n'est enregistré dans le système d'information Schengen et que le requérant qui s'est vu refuser la délivrance d'un visa n'est pas un ressortissant de l'espace Schengen, la CNIL poursuit ses investigations en saisissant le ministère des Affaires étrangères afin de connaître le motif de refus de visa et en particulier l'inscription éventuelle du requérant dans un fichier d'attention. Ces fichiers gérés par les postes consulaires sont intégrés dans le nouveau système informatique de délivrance des visas (RMV2), créé par un arrêté du 22 août 2001 pris après avis favorable de la CNIL.

Le droit d'accès aux informations contenues dans le RMV2 est indirect ou direct selon que les informations figurant dans les fichiers d'attention (fichier central comme fichiers locaux) concernent ou non la sûreté de l'État, la défense et la sécurité publique.

C'est votre droit

Le droit de rectification

Toute personne identifiée dans le STIC en qualité de victime peut s'opposer à la conservation, dans ce fichier, d'informations nominatives la concernant dès lors que l'auteur des faits concernés a été condamné de façon définitive. Pour obtenir la suppression de la fiche correspondante, il convient d'adresser sa demande, accompagnée d'une attestation du tribunal ayant condamné l'auteur des faits, au : ministère de l'Intérieur, Direction générale de la police nationale 11, rue des Saussaies 75008 Paris.
Toute personne identifiée dans le STIC en qualité de personne mise en cause dans une enquête judiciaire ouverte à la suite de l'une des infractions donnant lieu à inscription au STIC (crime, délit et certaines contraventions de Ve classe) peut demander la rectification ou la suppression de la fiche la concernant en s'adressant au procureur de la République territorialement compétent ou au procureur général près la cour d'appel en cas de décision prononcée par cette juridiction, dans les cas suivants :
1) les faits ayant donné lieu à l'enregistrement de la personne dans le STIC ont fait l'objet d'une requalification judiciaire (ex. : une procédure pénale a été ouverte pour vol aggravé ; le juge d'instruction ou la juridiction de jugement considère qu'il s'agit d'un vol simple) ;
2) la personne concernée a été acquittée ou relaxée ;
3) la personne concernée a bénéficié d'une décision de non-lieu ou d'un classement sans suite pour insuffisance de charges ;
4) l'intéressé peut demander que la fiche le concernant soit complétée par une référence à cette décision ou soit même effacée. La mise à jour de la fiche est de droit ; en revanche, son effacement relève du pouvoir d'appréciation du procureur de la République qui peut s'y opposer.

Le cas des fichiers d'impayés (FICP)

En 2003, la CNIL avait déjà délivré 4 avertissements à des établissements financiers qui n'avaient pas respecté la réglementation relative au fichier national des incidents de remboursement des crédits aux particuliers (FICP), géré par la Banque de France. Cette action s'est prolongée en 2004, puisque la Commission a délivré en mars et juin 5 nouveaux avertissements à des banques ou établissements de crédit. Ceci porte à 9 le nombre d'établissements « avertis » par la CNIL à la suite d'une inscription abusive ou d'un « défichage » tardif d'un de leurs clients au FICP.

Les banques utilisent parfois le FICP comme un fichier commun de « clients indésirables » : en litige avec leur client, elles l'inscrivent au FICP alors qu'il ne remplit pas les conditions pour y figurer. Ainsi, ce fichier, initialement créé pour lutter contre le surendettement des particuliers, devient un moyen de pression qu'utilise la banque contre son client.

Établissements avertis par la CNIL à la suite d'inscriptions abusives au FICP	Date de l'avertissement
Banque française et commerciale d'Antilles-Guyane (BFCAG)	3 juin 2004
Caisse de crédit mutuel du Dauphiné (CAFIDA)	3 juin 2004
Caisse régionale de Crédit agricole mutuel de Charente-Maritime (Deux-Sèvres)	3 juin 2004
Compagnie générale de location d'équipements (CGL – CGI)	25 mars 2004
FINAREF	25 mars 2004

Les établissements avertis par la CNIL ont pris des mesures pour rappeler à leurs collaborateurs, les règles relatives aux inscriptions et aux mainlevées d'inscriptions au FICP. Ils ont en outre modifié leurs règles de gestion des réclamations de leurs clients, afin d'isoler et de traiter plus rapidement les contestations d'inscriptions au FICP.

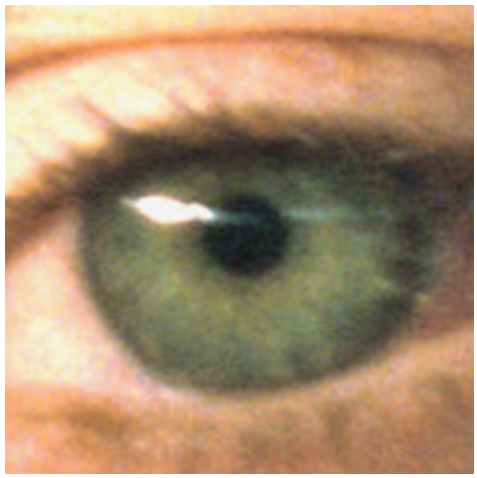
Ainsi, le nombre des réclamations déposées auprès de la CNIL contre la plupart de ses établissements a nettement diminué par rapport à 2003. Toutefois, la CNIL ne « baisse pas la garde » sur ce sujet qui concerne de nombreux particuliers et qui entrave parfois, de façon injuste, leur vie quotidienne.

TEMPS FORTS DE L'ANNÉE 2004

L'IDENTIFICATION BIOMÉTRIQUE DES VOYAGEURS

L'idée de renforcer l'identification des personnes par l'usage de la biométrie dans les documents de voyage est une retombée directe de la tragédie du 11 septembre 2001.

D'une part les États-Unis ont adopté une législation fixant au **26 octobre 2004** la date à laquelle les 28 pays exemptés de l'obligation de visa doivent, pour continuer à bénéficier de cette exemption, *« certifier qu'ils disposent d'un programme visant à délivrer à leurs ressortissants des passeports lisibles à la machine, inviolables et contenant des éléments d'identification biométriques conformes aux normes d'identification biométriques établies par l'Organisation internationale de l'aviation civile »*. Ainsi l'OACI a établi des normes qui ont deux caractéristiques. Sur les choix des données biométriques la position américaine est consacrée : seule la photographie du détenteur du passeport est rendue obligatoire, toute autre donnée biométrique est laissée au choix des États. La photographie doit être visible mais également numérisée dans un support électronique, une puce sans contact. La norme adoptée cependant ne comporte pas de mesures destinées à prévenir qu'un tiers accède à de telles données.



D'autre part le Conseil européen de Thessalonique des 19 et 20 juin 2003 a invité la Commission européenne à présenter des propositions qui permettent d'appliquer des solutions harmonisées et cohérentes en ce qui concerne les identificateurs ou les données biométriques pour les ressortissants des pays tiers (visa et titre de séjour) et pour les passeports des citoyens de l'Union européenne.

Le passeport et le visa européens

La délivrance des passeports est de compétence nationale mais, depuis 2000, des normes minimales de sécurité ont été adoptées sur le plan européen pour les passeports. La proposition de règlement de la Commission du 18 février 2004 vise à les actualiser en *« établissant des normes pour les dispositifs de sécurité et les éléments de biométrie intégrés »*. Elle prévoit donc à titre obligatoire la photographie numérisée dans un support électronique inséré dans le passeport et de manière optionnelle la photo numérisée de deux empreintes digitales. Elle évoque, par ailleurs, dans l'exposé des motifs, l'intérêt que présenterait, pour prévenir l'acquisition frauduleuse de tels documents, la constitution sur le plan européen *« d'un registre communautaire des passeports, centralisé, et fondé sur les empreintes digitales des personnes ayant demandé un passeport »*.

Le groupe « de l'article 29 » a fait part de ses préoccupations à la Commission, au Conseil et au Parlement européens par lettre en date du 18 août de son président. Celles-ci concernent l'ensemble des garanties destinées à s'assurer que les données de biométrie ne serviront qu'à la vérification de l'identité du détenteur d'un passeport par les autorités compétentes. Ainsi cette finalité et les objectifs des mesures de sécurité qui la garantissent devraient-ils être précisés dans le règlement, cela signifie que les données seront chiffrées pour prévenir la captation des données par des tiers et signées électroniquement par l'autorité de délivrance pour garantir leur authenticité et leur intégrité. Ces deux préoccupations ont été reprises par le **Parlement européen** et par le **Conseil**.

Par ailleurs, le groupe a demandé que ne soit pas constituée **une base de données des passeports** centralisant les photographies et les empreintes digitales, qui ouvrirait nécessairement la porte à d'autres usages. Cette préoccupation a été reprise par le Parlement européen. L'objet de la réglementation ne portant que sur les caractéristiques techniques des documents de voyages, le Conseil n'a pas eu à statuer sur la question. Le débat sur ce point ne fait que commencer.

Enfin, considérant les risques graves d'atteinte à la vie privée des personnes, le groupe a également demandé d'une manière générale, c'est-à-dire s'agissant de

l'approche de l'intégration d'éléments numérisés de biométrie dans l'ensemble des documents de voyage (visa, titre de séjour, passeport), que lui soit fourni l'ensemble des éléments factuels et d'étude mettant en évidence la nature et l'ampleur des problèmes justifiant cette intégration et l'absence d'alternatives moins attentatoires à la vie privée, afin de démontrer la nécessité impérieuse de recourir à ces techniques. À ce jour de tels éléments n'ont pas été portés à sa connaissance.

Le 24 décembre 2004, le Conseil a modifié de manière substantielle la proposition de la commission en décidant qu'outre la photographie, l'image de deux empreintes digitales serait également numérisée de manière obligatoire.

La Commission européenne avait présenté le 24 septembre 2003 deux propositions de modification des règlements relatifs aux modèles de visa et de titre de séjour prévoyant l'insertion dans ces documents d'une puce sans contact comportant notamment deux éléments biométriques, la photographie numérisée et deux empreintes digitales. Parallèlement le Conseil définissait ses orientations quant à une base de données européenne de visas (système VIS) destinée à lutter contre le « visa *shopping* » et la fraude à l'identité. Rassemblant toutes les données relatives aux demandeurs de visas, cette base contiendrait à terme, plusieurs dizaines de millions de personnes.

Dans son avis du 11 août 2004 le groupe dit de « l'article 29 » a reconnu la légitimité de la finalité de l'insertion des éléments biométriques en vue de vérifier l'identité du détenteur du titre tout en soulignant la nécessité de garanties techniques en matière de sécurité et de fiabilité. En revanche le groupe a exprimé les plus grandes réserves sur la conservation de donnée biométriques dans des bases de données, au-delà de la période nécessaire aux contrôles légaux pour la délivrance, la production et la remise aux demandeurs des documents en cause, dans la mesure où les éléments biométriques concernés sont des éléments dont la personne laisse des traces dans la vie quotidienne (empreintes digitales).

L'expérimentation des visas biométriques en France

La loi du 26 novembre 2003 relative à l'immigration prévoit la possibilité de procéder au relevé, à la mémorisation et au traitement des empreintes digitales ainsi que de la photographie, non plus seulement des demandeurs de titres de séjour et des étrangers en situation irrégulière mais aussi des demandeurs de visas.

En application de ces dispositions, le ministère de l'Intérieur a saisi la Commission d'un projet de décret en Conseil d'État visant à autoriser, à titre expérimental et pour une durée de deux ans, la création d'une base de données alimentée par les empreintes digitales et la photographie numérisée des personnes sollicitant un visa dans sept postes consulaires et prévoyant l'inscription, dans certains de ces consulats, de ces données biométriques dans une puce électronique associée au visa délivré.

Consultée sur ce texte, **la CNIL s'est prononcée le 5 octobre 2004** sur cette expérimentation (avis publié au *Journal officiel* du 4 décembre 2004). Si l'enregistrement des empreintes digitales dans une puce électronique apposée sur le visa ne soulève pas de difficultés de principe dès lors que les mesures de sécurité adéquates sont prises, en revanche les conditions de réalisation de cette expérimentation s'agissant notamment de la constitution de la base centralisée appellent plusieurs réserves et objections de fond de sa part.

Ainsi la Commission a considéré que la création d'un fichier comportant les données biométriques des personnes ayant obtenu un visa pouvait être admise à titre expérimental dans le cadre envisagé, à des fins de comparaison, sous réserve que soient strictement définies les conditions de mise en œuvre, d'alimentation, de consultation, de mise à jour et d'effacement de cette base. Un tel fichier ne saurait en tout état de cause être pérennisé sans que la Commission soit précisément informée de ses avantages et de ses inconvénients tout particulièrement sur le plan de la protection des droits des personnes.

En revanche, la Commission a estimé qu'au vu de l'objectif présenté, de contrôle aux frontières, la conservation, dans le fichier, des données biométriques des personnes s'étant vues opposer un refus de visas n'était pas justifiée : en effet, pour celles d'entre elles qui se présenteraient à la frontière sans visa, la consultation du fichier central ne ferait que confirmer l'absence de visa.

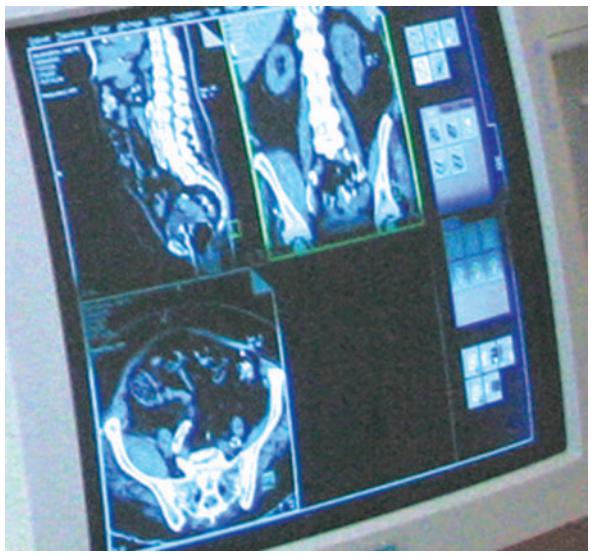
Le décret d'application de l'article 8-4 de l'ordonnance du 2 novembre 1945, qui a été publié au *Journal officiel* du 26 novembre 2004, ne reprend que **partiellement** les observations et recommandations de la CNIL. Certes, conformément à sa demande, les finalités de cette expérimentation ont été précisées et le dispositif fera l'objet d'une évaluation, sans autre précision toutefois. Certes le décret, prévoit désormais que les informations traitées ne seront pas conservées au-delà de la fin de l'expérimentation si cette dernière n'est pas pérennisée.

Mais ce dispositif expérimental continue de reposer sur une base centrale dans laquelle seront enregistrées les empreintes digitales de l'ensemble des demandeurs de visa, qu'ils aient ou non obtenu le visa demandé. La Commission estime que ce choix fait courir le risque d'une stigmatisation des étrangers demandant un visa sans l'obtenir, alors qu'il s'agit, somme toute, d'une procédure administrative normale dont l'issue défavorable ne préjuge par des résultats d'une nouvelle demande et qui ne fait pas pour autant du « refusé » un suspect.

LE PARTAGE DES DONNÉES MÉDICALES PERSONNELLES

Le dossier médical personnel

La loi relative à l'assurance maladie qui crée le dossier médical personnel a été adoptée le 13 août 2004. La CNIL avait été saisie pour avis par le Gouvernement du projet de loi et s'est prononcée, dans une **délibération du 10 juin 2004**, plus particulièrement sur les dispositions du texte relatives au dossier médical personnel et à la reconnaissance au bénéfice des médecins d'un accès en ligne, *via* la carte vitale, aux feuilles de soins. Elle a également porté son attention sur les dispositions du projet de loi portant création d'une haute autorité de santé et d'un institut des données de santé.



Gros plan sur ...

Le DMP

Le contenu du DMP

Le dossier médical personnel (DMP) doit être tenu dans le respect du secret médical. Il sera composé de l'ensemble des données recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, notamment des informations qui permettent le suivi des actes et prestations de soins. Le DMP comportera également un volet spécialement destiné à la prévention. Il sera hébergé chez un organisme spécialement agréé.

L'accès au DMP

Dans le respect des règles déontologiques applicables et des dispositions du code de la santé publique, chaque professionnel de santé exerçant en ville ou en établissement de santé, quel que soit son mode d'exercice, devra reporter dans le DMP, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge. En outre, à l'occasion du séjour d'un patient, les professionnels de santé habilités des établissements de santé reporteront sur le DMP les principaux éléments résumés relatifs à ce séjour. La loi consacre également la possibilité pour les médecins, à l'occasion des soins qu'ils délivrent, de consulter l'historique des remboursements détenus par l'organisme dont relève l'assuré. En pratique, le patient donnera son accord en permettant au professionnel de santé d'utiliser la carte Vitale. Le législateur prévoit qu'un identifiant peut être utilisé pour l'ouverture et pour la tenue du dossier médical personnel dans l'intérêt de la personne concernée et à des fins exclusives de coordination des soins.

Du côté de l'assuré

Pour pouvoir être complètement remboursé, l'assuré devra accepter que son médecin accède à son dossier personnel, le professionnel de santé devant lui-même attester, lors de l'établissement de la feuille de soins, qu'il a bien été en mesure de consulter le dossier. Dés lors le consentement de l'assuré est déterminé par l'enjeu financier.
Par ailleurs, la loi consacre la possibilité pour les services administratifs des établissements de santé de demander à l'assuré d'attester de son identité par la production d'un titre d'identité comportant sa photographie.

La nouvelle carte Vitale

L'obligation de faire porter la photographie de l'assuré sur sa carte Vitale est désormais consacrée par l'article L. 161-31 du Code de la Sécurité sociale. Il est également prévu que la carte électronique comporte un volet d'urgence destiné à recevoir les informations nécessaires aux interventions urgentes.

Les garanties reprises par le législateur

Les accès au dossier médical personnel sont encadrés : l'accès est interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties.

Le dossier médical personnel n'est pas accessible dans le cadre de la médecine du travail. Tout manquement à ces dispositions est passible des sanctions pénales prévues à l'article 226-13 du Code pénal.

De même, le souci exprimé à plusieurs reprises par la CNIL et, en particulier dans sa délibération du 10 juin 2004 de voir affirmé dans la loi le principe de l'interdiction de toute commercialisation des données de santé de santé a été repris par le législateur : *« Tout acte de cession à titre onéreux de données de santé nominatives, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions prévues à l'article 226-21 du Code pénal »*.

La mise en œuvre du dossier médical personnel

La mise en œuvre du dossier médical personnel reste toutefois subordonnée à l'adoption d'un certain nombre de **textes d'application** destinés à préciser l'ensemble du dispositif et qui doivent être soumis préalablement à l'avis de la CNIL. Ainsi en est-il du texte destiné à encadrer l'activité des hébergeurs de données de santé et de celui relatif aux règles de conservation et de transmission par voie électronique entre les professionnels de santé des informations médicales. Ce projet de décret vise en particulier à déterminer les cas dans lesquels l'utilisation de la carte de professionnel de santé (CPS) est obligatoire. Les modalités selon lesquelles les médecins pourront consulter les données issues des procédures de remboursement ou de prise en charge par l'organisme d'assurance maladie dont relève le bénéficiaire devront avoir été précisées.

La CNIL se prononcera également sur les modalités d'accès aux différentes catégories d'informations qui figureront au DMP et sur les conditions dans lesquelles un identifiant pourra être utilisé pour l'ouverture et pour la tenue du DMP dans l'intérêt de la personne concernée et à des fins exclusives de coordination des soins.

Questions à …

François BERNARD

Conseiller d'État honoraire
Commissaire en charge du secteur « Santé »

Quelle a été la position de la CNIL sur le projet de loi ?

La Commission a estimé que les dispositions du projet de loi instituant le dossier médical personnel et liant le niveau de remboursement des soins à l'accès du professionnel de santé à ce dossier étaient justifiées par un motif d'intérêt public important qui est, aux termes mêmes du texte soumis à son avis, « la coordination, la qualité et la continuité des soins » et l'amélioration de « la pertinence du recours au système de soins », l'ensemble du projet de loi visant à sauvegarder l'assurance maladie.
Elle rappelle néanmoins qu'aux termes mêmes des dispositions de l'article 8 de la directive précitée du 24 octobre 1995, la possibilité de déroger au principe selon lequel des données de santé ne peuvent être traitées sans le consentement du patient est subordonnée à l'introduction de garanties appropriées.

Quelles sont les recommandations formulées ?

La Commission a estimé que la loi devrait être complétée par une mention particulière indiquant que les données susceptibles d'être portées dans le dossier médical personnel sont couvertes par le secret professionnel tel que celui-ci est défini par le Code pénal et que quiconque aura obtenu ou tenté d'en obtenir la communication en violation des dispositions du présent article s'exposera à des sanctions pénales, de même que quiconque aura modifié ou tenté de modifier les informations portées sur ce même dossier.

Qu'en est-il des normes de sécurité ?

La CNIL considère que, dès lors qu'il serait envisagé de recourir au réseau internet pour permettre l'accès à ce dossier médical personnel, une telle utilisation, compte tenu des risques de divulgation des données, ne peut être admise que dans la mesure où des normes de sécurité extrêmement strictes sont imposées tant aux professionnels de santé qu'aux organismes appelés à héberger les données.
À cet égard, le principe de l'interdiction de toute commercialisation des données de santé directement ou indirectement nominatives devrait être posé dans la loi.

Que propose la CNIL en matière d'information des personnes ?

La CNIL rappelle la nécessité d'une information claire de la personne sur les modalités de constitution, de mise à jour et d'utilisation et de conservation de ses données médicales ainsi que des conditions dans lesquelles elle pourra elle-même accéder à ses données. Les modalités retenues pour l'identification et l'authentification, en particulier le recours à la carte de professionnel de santé, devront aussi être définies.

Les conditions d'application du volet d'urgence de la carte Vitale ainsi que les conditions d'accès aux différentes informations figurant dans ce volet d'urgence devront également être précisées par décret après avis de la CNIL.

Il appartiendra à la CNIL, tout en accompagnant le calendrier annoncé par le Gouvernement, de recueillir les observations de l'ensemble des acteurs intéressés sur les questions pratiques soulevées par la mise en place d'un tel dispositif. Ainsi, la Commission prévoit-elle de rencontrer les représentants des usagers, **les représentants des professionnels de santé et des industriels et sociétés de service en informatique.**

La transmission de données à l'assurance maladie complémentaire

Pour permettre à l'assurance maladie obligatoire de rembourser l'assuré, les feuilles de soins électroniques comportent notamment le code des médicaments, des actes et prestations réalisés. Or, ces codes sont susceptibles, dans certains cas, de révéler la pathologie d'un assuré. Actuellement, la loi n'autorise que les caisses d'assurance maladie obligatoire à accéder à ces informations.

Les organismes d'assurance maladie complémentaire (AMC) qui prennent en charge une partie des dépenses de soins et de biens médicaux en complément du régime obligatoire d'assurance maladie souhaiteraient également disposer de tout ou partie de ces codes afin de pouvoir mieux identifier les soins remboursés et ainsi améliorer leur politique de tarification à l'égard de leurs assurés. Les assureurs complémentaires pourraient ainsi proposer des garanties contractuelles modulées tel que le remboursement des médicaments non pris en charge par le régime obligatoire ou inciter les assurés à adhérer à des actions de prévention. Il s'agit pour l'assurance maladie complémentaire, alors que les pouvoirs publics procèdent au déremboursement de certains produits ou prestations, de « ne plus payer en aveugle » et de jouer un rôle accru en matière de maîtrise des dépenses de santé.

Les complémentaires santé s'intéressent principalement aux informations relatives aux domaines où le régime obligatoire n'intervient pas ou peu (dentaire, optique, appareillage, produits ou prestations non remboursés …).

Dans la mesure où les données de santé figurant dans les feuilles de soins électroniques relèvent de l'intimité de la vie privée, il convient de concilier l'accès des complémentaires santé à ces données avec le respect du **secret médical** et des dispositions de la loi « Informatique et Libertés ».

À cet effet, un rapport[6] a été établi à la demande du ministre de la Santé en **mai 2003** sur ces questions.

6. Rapport établi par un groupe de travail présidé par Christian Babusiaux, Conseiller maître à la Cour des comptes.

Il préconise plusieurs solutions juridiques et techniques, parmi lesquelles l'expérimentation d'un procédé de **transmission anonyme des données** de santé aux assureurs complémentaires.

La CNIL suit avec attention l'ensemble des expérimentations envisagées par les assureurs complémentaires. Ainsi, elle a , le **9 novembre 2004**, autorisé pour une durée d'un an, la Fédération nationale de la mutualité française (FNMF) à traiter, pour le compte de ses mutuelles adhérentes volontaires, sous forme anonymisée, les codes des médicaments et les codes des produits et prestations figurant sur les feuilles de soins électroniques, sur le fondement de l'article 8-III de la loi de 1978 modifiée en 2004.

L'expérimentation présentée par la FNMF sera réalisée avec des pharmaciens et des mutuelles volontaires et aura pour seule finalité d'effectuer des statistiques sur les données de santé anonymisées issues de feuilles de soins électroniques.

À cet effet, les pharmaciens transmettent, *via* un flux électronique sécurisé, les données sous une forme cryptée. Le chiffrement des données de santé sera réalisé à la source sur le poste du professionnel de santé à l'aide d'une clé de chiffrement fournie par le GIE SESAM Vitale.

À la réception des données sur le système informatique de la FNMF, celles-ci feront l'objet d'un traitement spécifique, consistant à anonymiser, de façon irréversible, les données de santé. La procédure d'anonymisation ainsi mise en place transformera les données d'identification en un numéro d'anonymat irréversible, en recourant à un algorithme de hachage.

La Commission a demandé que cette procédure fasse l'objet d'une évaluation par la Direction centrale de la sécurité des systèmes d'information (DCSSI) et qu'un **bilan de l'expérimentation** lui soit transmis.

La CNIL explique

L'anonymisation

La CNIL peut autoriser des applications comportant des informations sensibles, telles que les données de santé, dès lors que celles-ci font l'objet « à bref délai » d'un procédé d'anonymisation reconnu conforme à la loi.
Depuis de nombreuses années, la CNIL préconise le recours à de telles techniques d'anonymisation notamment dans le domaine statistique. De tels procédés ont ainsi été employés dans des domaines aussi divers que la surveillance sanitaire (déclarations obligatoires du sida), les statistiques d'activité hospitalières (PMSI), le système national d'information sur l'assurance maladie ou encore les transports (analyse anonyme des trajets avec la carte Navigo dans la région parisienne).

LE TARIF SOCIAL DE L'ÉLECTRICITÉ

Dans la nuit du 17 au 18 août 2004, un père et sa fillette de six ans ont péri à Saint-Denis dans l'incendie de leur appartement. Hors, celui-ci était éclairé à la bougie car EDF avait coupé l'électricité de leur logement en raison du non-paiement des factures.

À la suite de cet événement, le ministre délégué à l'Industrie a annoncé la mise en place, dès le 1er janvier 2005, d'un **« tarif social » de l'électricité** ainsi que la création d'un groupe de travail chargé de réfléchir sur les voies d'amélioration des dispositifs d'aide sociale en matière d'électricité.

Le principe d'un tarif réduit de l'électricité pour les foyers les plus modestes n'est pas nouveau car il découle d'une loi votée en février 2000[7], dont le décret d'application n'est intervenu qu'en 2004.

La CNIL, qui n'a pas été consultée sur le projet de décret lui-même alors que des transmissions de données à caractère personnel y sont pourtant clairement prévues, a autorisé le traitement informatique nécessaire à l'application du tarif social à titre provisoire pour une durée de six mois, tout en se déclarant réservée sur ses modalités de mise en œuvre, qui aboutissent, de fait, à la création d'un **fichier central des bénéficiaires de la couverture maladie universelle détenu par un opérateur privé**.

Présentation du dispositif

Le décret du 8 avril 2004 prévoit qu'à compter du 1er janvier 2005, les familles à revenus modestes peuvent bénéficier d'une tarification spéciale pour leur consommation d'électricité. Les ménages ayant des ressources annuelles inférieures à 5 520 € peuvent demander à bénéficier d'une tarification spéciale de l'électricité consistant en une réduction de 30 % à 50 % (selon le nombre de personnes composant le foyer) du montant de la facture sur les 100 premiers kWh mensuels de consommation.

À cet effet, il a été prévu que les organismes d'assurance maladie communiquent à un prestataire privé opérant pour le compte des distributeurs d'électricité la liste des personnes remplissant les conditions de ressources. Ce prestataire procédera à leur exploitation informatique pour envoyer aux familles concernées une attestation à compléter et à renvoyer à leur fournisseur.

En pratique, ces listes sont extraites des fichiers de bénéficiaires de la couverture maladie universelle complémentaire (CMU-C), qui comportent notamment le montant des ressources annuelles et le nombre de personnes composant le foyer. Les données transmises sont les nom, prénoms, date de naissance, adresse et nombre de personnes du foyer des personnes répondant au critère de ressources fixé qui est proche de celui d'attribution de la CMU.

La création d'un fichier national des bénéficiaires de la CMU confié à un opérateur privé aurait pu être évitée

La Commission s'est prononcée sur le dispositif le **18 novembre 2004**. Elle a estimé que les modalités d'organisation du dispositif devaient être revues compte tenu de la sensibilité des données traitées.

La CNIL a en effet toujours été très attentive aux conditions dans lesquelles des fichiers centraux comportant des informations à caractère social sont créés. Or, dans le cas du dispositif retenu pour le tarif social de l'électricité, la centralisation par un prestataire privé de données transmises par l'ensemble des organismes d'assurance maladie **issues de leurs fichiers** conduit à créer, en pratique, un nouveau fichier national de bénéficiaires de la couverture maladie universelle complémentaire.

De plus, les données des bénéficiaires potentiels seraient conservées dans le fichier pendant une durée d'au moins un an et tant que la personne concernée dispose de droits à la CMU-C, y compris dans le cas où elle ne manifeste pas son souhait de bénéficier du dispositif.

Suite à cette décision, le Gouvernement a présenté, à l'occasion de l'examen du projet de loi de programmation pour la cohésion sociale par l'Assemblée nationale, un amendement visant à ce que la transmission par les organismes d'assurance maladie des fichiers aux distributeurs d'électricité ou à un organisme prestataire désigné à cet effet soit désormais prévue par la loi elle-même.

7. Loi n°2000-108 du 10 février 2000 relative à la modernisation et au développement du service public de l'électricité.

Contrairement à ce qui a été indiqué lors des débats parlementaires[8], la CNIL a très clairement émis les plus grandes réserves vis-à-vis de la constitution d'un fichier national des bénéficiaires de la CMU et de sa transmission à un prestataire privé et déplore cette intervention législative quelque peu hâtive, malheureusement intervenue sans même qu'ait pu être examinée la solution alternative proposée qui prévoit l'envoi direct par les organismes de protection sociale des attestations aux bénéficiaires.

La CNIL s'est toujours montrée très vigilante à l'égard de la création de fichiers centraux comportant des informations sociales. Elle s'est prononcée, au fil des années, sur la mise en place de plusieurs de ces grands fichiers sociaux et elle a dégagé des limites.

La CNIL conseille

La CNIL n'a cependant autorisé ce fichier qu'à titre provisoire (pour une durée de six mois), afin qu'une solution alternative reposant sur la transmission directe par les organismes d'assurance maladie d'attestations puisse être examinée dans ce délai. Elle a également demandé qu'un bilan de l'expérimentation du dispositif mis en œuvre et des résultats de l'étude menée sur la solution alternative. Elle devrait être saisie à nouveau du dispositif finalement retenu.

À propos des fichiers

Les grands fichiers sociaux

La centralisation n'est acceptable que si elle est nécessaire

La CNIL, saisie de la création par la Caisse nationale d'assurance maladie des travailleurs salariés du répertoire de ses bénéficiaires propres (fichier « Rénovation – référentiel individus (RFI) »), a notamment veillé à ce que ce fichier ne soit pas centralisé au niveau national mais uniquement au niveau régional (délibération n° 04-059 du 1er juillet 2004), dès lors que cette centralisation n'apparaissait pas nécessaire.

L'anonymisation des données doit être, dans la mesure du possible et des finalités envisagées, recherchée

La CNIL s'est prononcée sur le fichier central visant à améliorer la qualité des soins et la gestion des dépenses de l'assurance maladie (système national d'information interrégimes de l'assurance maladie – SNIIRAM), en exigeant des garanties d'anonymisation (délibération n° 01-04 du 18 octobre 2001).

Les possibilités d'utilisation du fichier à des fins de recherche de personnes physiques doivent être limitées

Le Répertoire national d'identification des personnes physiques (RNIPP) est, en premier lieu, le fichier national de la sphère sociale. La CNIL a encadré ce fichier d'identification par deux délibérations n° 81-68 du 9 juin 1981 et 82-103 du 22 janvier 1982. Outil de vérification de l'état civil des personnes, le RNIPP permet notamment la mise à jour du fichier national d'identification détenu par la Caisse nationale d'assurance maladie des travailleurs salariés.

Le répertoire national de l'ensemble des assurés des organismes d'assurance maladie ou « RNIAM » a été également soumis à la CNIL, qui a veillé à ce que ce répertoire, principalement utilisé à des fins de certification du rattachement des bénéficiaires aux organismes servant les prestations, ne comporte pas notamment l'adresse des personnes concernées.

Ces deux répertoires ne peuvent pas être utilisés à des fins de recherche d'une personne physique hormis les cas spécifiquement prévus par la loi.

L'intégration de l'adresse dans les fichiers centraux doit, dans la mesure du possible, être évitée

La CNIL a considéré, à propos du fichier « RFI-rénovation » précité que l'inscription de l'adresse dans la base de données nationale aurait pour conséquence de reconnaître à l'application de la CNAMTS la qualité d'un fichier national de domiciliation qui, par nature, comporte des risques excessifs pour les libertés individuelles eu égard aux objectifs poursuivis.

Limitation des possibilités d'accès direct et de la durée de conservation des données

La CNIL veille à ce que les possibilités d'accès direct aux fichiers et la durée de conservation maximale soient limitées. À titre d'exemple, l'accès direct par la caisse nationale d'allocations familiales au fichier national de contrôle des bénéficiaires du RMI a été refusé, dans la mesure où chaque caisse disposant d'un accès direct, il suffit de leur adresser directement des demandes de droit d'accès (délibération n° 97-052 du 30 juin 1997).

Information des personnes concernées

La CNIL a rappelé, à l'occasion de l'examen des conditions de mise en œuvre du répertoire national des allocataires détenu par l'UNEDIC, la nécessité d'une information individuelle préalable lorsque des échanges d'information sont prévus (délibération n° 94-104 du 6 décembre 1994).

8. Cet amendement a été présenté comme *« ayant pour objet de répondre aux demandes de la CNIL, qui a jugé nécessaire d'assurer une base légale à la constitution de ce fichier et à son transfert à l'organisme chargé de gérer le dispositif »*.

CONFLITS TRANSATLANTIQUES DE LOIS

Le *Sarbanes-Oxley act* et ses incidences sur la profession française de commissaire aux comptes

La globalisation des flux financiers et des échanges commerciaux a pris une dimension inédite au cours de la dernière décennie, à la faveur de préoccupations concernant la transparence financière au sein des sociétés cotées.

Des événements récents tels que la révélation de pratiques comptables critiquables qui ont affecté des entreprises de taille mondiale, ruiné des actionnaires, des salariés et conduit à la disparition d'un des tout premiers cabinets d'audit, sont à l'origine d'une grave crise de confiance dans l'essence même de l'économie de marché : la fiabilité des comptes qui sont le lien entre la réalité de l'entreprise et les actionnaires, institutionnels ou individuels.

Seule une approche de **reconnaissance mutuelle** serait de nature à établir les principes d'un contrôle de la transparence financière au niveau international dans le respect des contraintes légales définies par les différents États, s'agissant en particulier des règles relatives à l'informatique et aux libertés. Ces travaux de reconnaissance mutuelle s'appuieraient, en France, sur la **loi de sécurité financière adoptée le 1er août 2003** et, au niveau européen, sur les travaux en cours concernant la huitième directive du Conseil 84/253/CEE du 10 avril 1984 relative à l'agrément des personnes chargées du contrôle légal des documents comptables. De fait, comme la

Questions à …

Patrick DELNATTE

Député du Nord
Commissaire en charge du secteur « Justice »

En quoi consiste le *Sarbanes-Oxley Act* ?
En vigueur aux États-Unis depuis le 30 juillet 2002, le *Sarbanes-Oxley Act* (SOA), adopté en réaction aux affaires Enron et Worldcom, marque pour le droit américain, une véritable révolution. Les sujets traités dans ce texte sont multiples : transparence comptable, nouvelles règles imposées aux avocats d'affaires, règles de communication financière, création de nouveaux délits boursiers, durcissement des sanctions existantes et surtout réforme de la profession des auditeurs (commissaires aux comptes), notamment au moyen de la mise en place d'un organe public de contrôle des auditeurs, le *Public Company Accounting Oversight Board* (PCAOB), rattaché à la *Securities and Exchange Commission* (SEC). Conformément à la réglementation nouvelle, tous les commissaires aux comptes appelés à émettre des rapports d'audit sur des sociétés cotées aux États-Unis doivent s'enregistrer auprès du PCAOB.

Peut-on parler de loi extraterritoriale ?
Cette réforme en profondeur du droit américain des sociétés ne concerne pas que les sociétés américaines. Les nouvelles règles qu'elle prescrit s'appliquent à tous les émetteurs, américains ou non, dont les titres ont été cotés sur les marchés américains.

Quelles en sont les conséquences en France ?
En application de la réglementation définie par le PCAOB et du fait de leur extraterritorialité, un certain nombre de cabinets d'audit français (35 cabinets pour 40 entreprises françaises cotées aux États-Unis) sont tenus de s'enregistrer auprès du PCAOB. À cet effet, ces cabinets avaient l'obligation de transférer au PCAOB avant le 19 juillet 2004 un formulaire contenant de nombreuses informations personnelles relatives à leurs associés et responsables, soit une population d'environ 1 000 à 2 000 personnes.

Pourquoi la CNIL s'est-elle intéressée à cette question ?
Il est évident que le problème en cause est essentiellement de sécurité financière. Toutefois, parce qu'il s'agit également d'une communication de données à caractère personnel, la Compagnie française des commissaires aux comptes (CNCC) a saisi la CNIL afin de recueillir ses observations sur les incompatibilités éventuelles entre les exigences du PCAOB et les réglementations françaises et européennes de protection des données personnelles. Il y a là un véritable conflit de législation.

Commission européenne et le PCAOB l'ont confirmé à la CNIL, des travaux ont été engagés en ce sens par les autorités concernées, qui devraient aboutir à moyen terme.

Dans l'immédiat, plusieurs cabinets d'audit européens se sont inscrits auprès du PCAOB en faisant usage de la faculté accordée par celui-ci dans sa dite « Rule 2105 », qui permet aux cabinets d'audit étrangers de s'abstenir de communiquer au PCAOB toute information pouvant créer un conflit de lois, à la condition qu'ils fournissent notamment un avis juridique sur la violation des lois nationales qui résulterait de cette communication. Cette règle permet ainsi aux cabinets établis dans l'Union européenne d'éviter d'avoir à enfreindre une loi européenne ou nationale de protection des données, ainsi que certaines règles de droit du travail et relatives au secret professionnel.

D'autres problèmes relatifs à la protection des données sont susceptibles d'émerger quand, une fois les cabinets d'audit français enregistrés, le PCAOB aura l'intention de diligenter des mesures de contrôle et d'inspection sur ceux-ci, comme le prévoit le SOA. Toutefois, en l'état des informations que la Commission européenne a communiquées à la CNIL, le PCAOB ne compte pas lancer de telles opérations avant 2007, ce qui devrait laisser suffisamment de temps aux travaux de reconnaissance mutuelle évoqués plus haut d'aboutir.

La CNIL, ainsi que ses homologues européens réunis au sein du groupe dit « de l'article 29 », se satisfaisant de cette perspective, suivront toutefois avec attention la progression de ces travaux, afin de s'assurer que les questions de protection des données personnelles y seront prises en compte de manière adéquate.

La CNIL recommande

La Commission a conclu que la communication d'informations nominatives imposée par la réglementation américaine n'était conforme ni à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ni à la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel et à la libre circulation de ces données.
Elle a en effet estimé que les principes de finalité, de proportionnalité, de légitimation du traitement et de confidentialité des informations ainsi que les règles de collecte de données relatives aux infractions, condamnations et mesures de sûreté, principes et règles dont le non-respect est passible des peines visées aux articles 226-17, 226-19, 226-21 et 226-22 du Code pénal, ne seraient pas, en l'espèce, respectés. En conséquence, le traitement que seraient obligés de mettre en œuvre les cabinets d'audit français pour se conformer aux exigences du PCAOB apparaissant comme illégal au regard des droits français et européen de la protection des données personnelles, la communication de données découlant de ce traitement vers le PCAOB l'aurait été tout autant. La commission a fait connaître sa position sur ces questions au ministère français de la Justice, au Haut Conseil du commissariat aux commissaires aux comptes (HCCC) et à la Commission européenne, mais également au PCAOB. Ce faisant, elle leur a également fait part de son souhait que soit privilégiée une approche de reconnaissance mutuelle entre les systèmes d'encadrement de la profession de commissaires aux comptes français et européens d'une part, et américains d'autre part.

Le recensement américain en France

La CNIL a eu à connaître d'une autre forme de conflit de lois entre le droit français et le droit américain en 2004. Le bureau du recensement des États-Unis (le *Census Bureau*) homologue de l'Institut national de la statistique et des études économiques (INSEE), a en effet, fin 2003, saisi la Commission d'une demande de conseil concernant la réalisation en France en 2004 d'un test pour recenser « les citoyens américains résidant en France ».

L'objet du test étant de préparer le recensement général de la population américaine prévu en 2010 et plus particulièrement de vérifier la praticabilité d'un recensement de tous les citoyens américains résidant hors des États-Unis, le bureau du recensement a demandé à être informé des modalités selon lesquelles la loi « Informatique et Libertés » était applicable à cette opération, dans la mesure où un traitement automatisé de données personnelles sera mis en œuvre.

La collecte des données a eu lieu de février à avril 2004. Les questionnaires étaient disponibles auprès de l'ambassade et des consulats américains en France.

La Commission a dans un premier temps, au vu des éléments portés à sa connaissance, informé le bureau du recensement que, dès lors que le recueil de données nominatives est effectué sur le territoire français, les personnes concernées, quelle que soit leur nationalité, bénéficient des droits qui leur sont reconnus par la loi de 1978 et par la directive européenne du 24 octobre 1995. Elles doivent être, lors de la collecte des données, informées du caractère obligatoire ou facultatif des réponses, des destinataires des informations ainsi que de l'existence du droit d'accès, c'est-à-dire du droit d'obtenir communication des données qui sont recueillies sur elles. Il a donc été demandé, d'une part, que les questionnaires soient complétés par ces mentions et, d'autre part, que, conformément à l'article 4-2 de la directive, un représentant du bureau du recensement soit désigné en France.

La CNIL a ensuite considéré que la collecte envisagée de données sur les personnes habitant dans le logement de citoyens américains en France alors même qu'elles ne seraient pas de nationalité américaine n'était pas pertinente au regard de la finalité de l'opération qui vise les seuls citoyens américains. Elle a ensuite attiré l'attention des responsables du test sur les dispositions de la loi du 6 janvier 1978, en vertu desquelles, le recueil de données faisant apparaître les origines raciales des personnes ne peut être envisagé qu'avec leur accord exprès.

Par ailleurs, la Commission a souhaité que les éléments d'identification que sont le nom et le prénom, le numéro de passeport et le numéro de Sécurité sociale américains ne figurent pas dans le fichier informatisé résultant du traitement des questionnaires. En effet, si les données sont rendues anonymes avant leur transfert aux États-Unis à partir du territoire de l'Union européenne, le transfert en question n'est pas considéré comme un transfert de données à caractère personnel et donc l'exigence légale d'un niveau de protection adéquat s'appliquant aux données dans le pays de destination n'est pas requise.

Dés réception des observations de la CNIL, une réunion de travail a été organisée à l'issue de laquelle le bureau du recensement américain s'est engagé sur certains points (voir encadré).

Bons points !

– le test n'aura aucun caractère obligatoire

– une note d'information, rédigée par la CNIL, sur les droits qui sont reconnus par la loi du 6 janvier 1978 sera diffusée aux intéressés avec les questionnaires

– les personnes du foyer qui ne seraient pas de nationalité américaine ne seront pas tenues de répondre

– les données nominatives collectées en France ne seront conservées sur support automatisé que pendant un délai de douze mois

SIRIUS : UNE APPLICATION DU PROGRAMME COPERNIC

Un peu d'histoire

La CNIL et Copernic ...

La CNIL a déjà examiné plusieurs volets du programme Copernic : le paiement en ligne de l'impôt sur le revenu et des impôts locaux (*cf.* délibération n° 00-021 du 30 mars 2000) ; la déclaration et le paiement en ligne de la TVA (*cf.* délibération n° 01-037 du 12 juin 2001) ; la consultation des dossiers fiscaux en ligne et la transmission par internet des déclarations de revenus (*cf.* délibération n° 02-010 du 7 mars 2002) ; le service de consultation en ligne des données foncières destiné aux notaires (*cf.* délibération n° 03-009 du 27 février 2003) ; la base nationale de recensement des liens d'intérêts entre personnes physiques et sociétés (*cf.* délibération n° 03-048 du 30 octobre 2003).

... et retour à Sirius

Deux caractéristiques importantes du traitement : l'alimentation de la base est automatisée ; un contrôle, à l'entrée, de l'intégrité des données et de l'identification des déclarants est mis en place, les données étant reléguées en cas d'échec vers une base de rejet pour analyse ; les données enregistrées sont mutualisées entre environ 12 000 agents de la Direction générale des impôts (DGI) qui participent d'une manière ou d'une autre à la mission générale de contrôle en matière de fiscalité personnelle.

Sirius-fp fonctionne en infocentre, l'objectif est de permettre à des utilisateurs non-spécialistes de lancer leurs requêtes, facilement et rapidement. Ces requêtes visant à obtenir des listes de situations individuelles à contrôler, établies en fonction d'un contrôle de cohérence des éléments déclarés (impôt sur le revenu et/ou impôt de solidarité sur la fortune), de l'évolution de ces éléments ou de la constatation d'un écart entre ceux-ci et les ratios habituellement constatés.

Questions à ...

J.-P de LONGEVIALLE

Conseiller d'État
Commissaire en charge du secteur « Finances publiques »

Copernic, qu'est-ce que c'est ?

Vaste programme – commun aux directions des impôts (DGI) et de la comptabilité publique (DGCP) – des refontes de leurs traitements informatiques, Copernic, qui a été planifié sur neuf ans (2001-2009), articule ensemble plus de 70 applications et représente un investissement total de 1,3 milliard €, est le plus important chantier d'administration électronique des administrations centrales.

Visant à substituer à une informatique éclatée et conçue en fonction des seuls besoins d'administrations cloisonnées par impôt et par métier, une informatique à la fois transversale (création de grandes bases de données nationales aux ressources partagées entre tous les services utilisateurs) et axée sur la relation avec le contribuable (développement de téléprocédures, mise en ligne du dossier fiscal personnel). Copernic facilitera l'actualisation et la mise à disposition à un grand nombre d'intervenants d'informations protégées par le secret fiscal ... ce qui nécessite que toutes précautions soient prises pour préserver la confidentialité de ces données et les droits des contribuables.

Et Sirius ?

Traitement d'aide au contrôle de la situation fiscale des particuliers, l'application Sirius, sur laquelle la CNIL a formulé un avis en 2004 correspond parfaitement aux objectifs de Copernic, puisqu'il repose sur la constitution, à partir des fichiers aujourd'hui dispersés dans environ 800 centres des impôts, d'un entrepôt national unique des données déclarées par les contribuables à l'impôt sur le revenu et à l'impôt sur la fortune et sur la possibilité, pour environ 12 000 agents de la DGI, d'exploiter la base ainsi constituée afin d'effectuer des tris des listes de situations individuelles à contrôler.

En somme, un puissant outil de ciblage que la CNIL se devait de regarder de près en fonction des missions que la loi lui a confiées.

Ces listes seront constituées, tant en ce qui concerne leurs critères de définition que les éléments y figurant, à partir de requêtes prédéterminées (plus d'une centaine) ou, plus rarement, directement rédigées par l'utilisateur.

L'examen du traitement par la Commission a permis de faire évoluer le projet Sirius-fp sur plusieurs points importants.

La question de l'anonymisation partielle de la base

La CNIL s'est interrogée sur les raisons de la présence dans Sirius-fp des noms des déclarants en plus de leur identifiant fiscal national SPI dont la vérification est systématiquement prévue. Plusieurs arguments étaient invoqués par l'administration : le nom doit dans quelques cas servir de critère d'interrogation ; les agents chargés des contrôles ont nécessairement besoin de cette information, ne serait-ce que pour distinguer les dossiers déjà contrôlés ou en cours de contrôle ; enfin ce traitement doit être d'une utilisation aisée.

Bons points !

Sans retenir la solution préconisée par la Commission, la DGI a accepté le principe d'une anonymisation partielle – par le retrait des noms des contribuables – des seules listes de restitution. Mais cette opération ne pourra pas intervenir avant 2007, ces délais étant justifiés par la nécessité de prévoir de nouveaux développements informatiques, notamment pour identifier dans les listes les dossiers déjà contrôlés ou en cours de vérification.

S'il a tout de suite semblé évident que la finalité de contrôle fiscal interdit l'anonymisation complète des informations relatives aux déclarants, la CNIL a marqué sa préférence pour une solution consistant à n'intégrer dans l'entrepôt de données que les identifiants fiscaux SPI (numéro individuel) et FIP (identifiant du foyer fiscal) et à prévoir la mise en place d'un lien avec d'autres applications directement nominatives pour limiter l'accès aux éléments d'identité des contribuables à la phase d'engagement actif du contrôle fiscal. En effet, les listes produites par l'application, dont la sensibilité ne saurait être négligée, ont vocation à circuler au sein de l'administration. En outre, l'identité des personnes n'a pas à être prise en compte pendant la phase de programmation des contrôles. Enfin, l'interrogation de la base sur un nom a semblé être en décalage par rapport aux finalités déclarées ou au moins être très marginale.

Les modalités d'interrogation et d'exploitation des données

Sur ces points également, l'instruction menée par la CNIL a permis d'enregistrer une amélioration du projet initial. La possibilité de lancer des requêtes libres fait toujours l'objet d'un examen attentif par la CNIL. En l'espèce, la DGI a d'abord accepté de rendre impossible toute extraction de listes en fonction de l'identité de sexe des personnes formant le foyer fiscal, critère à la fois sensible et sans pertinence fiscale. Elle a par la suite proposé de réserver le droit de lancer des requêtes libres à moins d'un quart des utilisateurs habilités de Sirius-fp. En outre, cette possibilité fera l'objet d'une surveillance particulière, notamment *via* un module de traçage. Parmi ces requêtes libres, celles effectuées à partir des noms des personnes seront soumises à un encadrement encore plus rigoureux.

Par ailleurs, si les listes de restitution pourront être éditées sur papier ou faire l'objet d'un enregistrement sous forme dématérialisée, la DGI a décidé d'en interdire la circulation entre services sur disquette ou support papier. Les listes de contribuables ne pourront circuler que sous forme de fichiers Excel, par messagerie et par l'intermédiaire du chef de service utilisateur afin d'éviter toute banalisation de leur circulation. Enfin, la longueur maximale des listes de restitution a été fortement réduite.

La définition des profils d'accès à la base

Il a été précisé que les utilisateurs de la base bénéficieraient d'une habilitation personnelle, l'accès à l'application étant géré automatiquement à partir d'une application dénommée annuaire DGI commun à l'ensemble des traitements Copernic. C'est aux chefs de service qu'il appartient d'attribuer et de définir les habilitations recensées dans l'annuaire DGI.

À l'examen, il est apparu que les règles d'habilitation retenues conduisaient à ce que les agents puissent disposer de possibilités d'interrogation de la base Sirius excédant leurs attributions notamment sur le plan géographique. La

Commission a donc préconisé la mise en place d'un dispositif plus serré de filtrage des requêtes. Ainsi les agents des services d'assiette des centres des impôts n'auraient plus physiquement accès aux informations relatives à l'ensemble des contribuables du département mais seulement aux dossiers relevant de leur service.

Mais une telle solution passant par une modification de l'application annuaire DGI n'aurait pu être mise en œuvre dans des délais rapides. À défaut l'administration s'est engagée à encadrer par une instruction interne les requêtes dans Sirius. Les chefs de service devront préciser aux agents placés sous leur responsabilité que le périmètre géographique des requêtes est normalement être limité en fonction de leurs attributions. Par exception, toute requête lancée sur un champ géographique plus large devra faire l'objet d'une autorisation spéciale du chef de service. La Commission a également souhaité que le dispositif mis en place prévoie d'alerter l'agent utilisateur, au moyen d'un clignotant inséré dans l'application, lorsqu'il effectuera une requête excédant son périmètre géographique d'affectation. L'administration a accepté d'étudier la faisabilité technique de ce signalement.

L'examen de ce traitement a, semble-t-il, été l'occasion d'une meilleure prise de conscience des implications des principes de la protection des données personnelles en présence d'une mégabase nationale de données dont la confidentialité est protégée par un secret instauré par la loi, tel que le secret fiscal. Une telle évolution est particulièrement nécessaire à l'heure où se multiplient dans les administrations comme dans les entreprises les entrepôts de données fonctionnant en infocentre au profit d'un grand nombre d'utilisateurs.

L'information des contribuables

La Commission a rappelé que les personnes devaient être informées de la finalité des traitements auxquels les données qui les concernent sont destinées (article 321 de la loi du 6 janvier 1978). Elle demande donc que les formulaires de déclaration mentionnent l'existence d'un traitement informatique permettant de procéder à un rapprochement des éléments déclarés par le contribuable avec ceux de ses déclarations précédentes et, le cas échéant, des éléments des déclarations de revenus avec ceux des déclarations en matière d'ISF.

Gros plan sur ...

Precar-It

Les solutions retenues pour Sirius-fp peuvent être rapprochées de celles retenues pour un traitement déclaré en 2004 par la direction des relations du travail du ministère de l'Emploi, du Travail et de la Cohésion sociale (*cf.* délibération n° 2004-104 du 14 décembre 2004).
La base de données nationale Precar-It a de nombreux points communs avec Sirius-fp. Elle a pour finalité la recherche et la constatation d'infractions pénales à la législation sur le travail temporaire et regroupe à cette fin l'ensemble des relevés de contrat de travail temporaire transmis par l'UNEDIC. Ses utilisateurs, les agents des services de l'inspection du travail, s'en serviront pour lancer des requêtes nécessaires à la préparation de leurs missions de contrôle dans les entreprises. À la différence de Sirius-fp, Precar-It comporte une fonctionnalité de détection automatique de certaines situations potentielles d'infractions. Dans les deux cas, l'informatique ne saurait apporter davantage qu'une simple aide à la détection des fraudes. La décision d'engager le contrôle ou de rédiger le procès-verbal appartient toujours à un agent.
Comme dans le cas de Sirius-fp, le projet initial du ministère du Travail ne prévoyait aucune limitation d'accès aux informations, alors que les inspecteurs du travail ne peuvent verbaliser qu'à l'intérieur de leur département d'affectation. La Commission a donc demandé que les utilisateurs de Precar-It ne puissent accéder qu'aux données relatives aux entreprises de travail temporaire, aux entreprises utilisatrices, aux lieux de travail et aux salariés temporaires domiciliés dans leur département d'affectation. Cependant, la Commission a admis que, pour la réalisation de contrôles concertés à l'égard des établissements d'une même entreprise établis sur plusieurs départements, après détection de fraudes, les inspecteurs puissent élargir leur enquête à l'ensemble des établissements de l'entreprise incriminée et s'échanger les informations en leur possession. En effet, on compte parmi les fraudes recherchées les échanges de contrats au sein d'un même groupe qui conduisent à confiner certains salariés dans un statut précaire. Cette faculté sera cependant limitée à des personnes spécialement habilitées. La Commission a , en revanche, refusé la création d'un profil national d'accès à la base.

OÙ EN EST-ON SUR…?

LE « SPAM »

La loi sur l'économie numérique

Prévue par une directive européenne de 2002, la loi pour la confiance dans l'économie numérique, adoptée le 21 juin 2004[10], vise notamment à lutter contre les spams en renforçant la protection des personnes utilisatrices d'une adresse de courrier électronique.

Pour le démarchage autre que de nature commerciale comme la prospection politique, associative, religieuse ou caritative (par exemple, collecte de dons), la loi de 1978 modifiée en 2004 reste applicable : information préalable sur l'utilisation de l'adresse électronique à de telles fins et droit de s'opposer gratuitement à cette utilisation.

10. Le suivi de ce projet de loi par la CNIL a été largement abordé dans ses précédents rapports annuels (*cf.* 23e rapport annuel, p.71 et p.78, 24e rapport annuel, p.63 à 66).

Les suites judiciaires de l'opération « boîte à spam »

En octobre 2002, la CNIL avait dénoncé au parquet, à l'issue de son opération « boîte à spams » (*cf.* 22e rapport annuel, p. 45), 5 sociétés pratiquant cette forme de prospection commerciale. Une seule de ces dénonciations a donné lieu à des poursuites devant le tribunal correctionnel de Paris qui a rendu sa décision par un jugement du 7 décembre 2004.

Le responsable de la société en cause était poursuivi pour avoir collecté des adresses électroniques par un moyen déloyal, à savoir en l'espèce *via* l'utilisation de logiciels « aspirateurs d'adresses électroniques » sur les espaces publics de l'internet, dans le but de constituer des fichiers de prospects.

Le tribunal a considéré que le fait de collecter des adresses électroniques sur internet à l'insu des intéressés,

Questions à …

Bernard PEYRAT

Conseiller à la Cour de cassation
Commissaire en charge du secteur « Commerce »

Quelle nouveauté apporte la loi sur l'économie numérique ?
Le principe nouveau introduit par la loi est celui du consentement préalable (principe dit de l'*opt-in*) : l'envoi d'un message commercial par courrier électronique, par SMS (*Short Message Service*) ou par MMS (*Multimedia Messaging Services*) est interdit si le destinataire du message n'a pas donné son consentement à recevoir ce message. Cet accord doit être donné en pleine connaissance de cause. À titre d'exemple, le fait d'accepter des conditions générales de vente ne signifie pas que la personne a donné son consentement à être prospecté. De plus, si cette dernière a consenti à être démarchée, elle doit être clairement informée de l'identité de l'entreprise à l'origine de l'envoi et doit pouvoir demander à ne plus recevoir de publicités.

Y'a-t-il des exceptions à la règle du consentement préalable ?
Dans le cadre d'une relation client-entreprise existante, le consentement préalable du client n'est pas exigé à la condition toutefois que les sollicitations commerciales adressées par l'entreprise portent sur des produits ou services analogues à ceux que le client avait antérieurement achetés ou souscrits auprès d'elle. De plus, l'entreprise doit lui offrir la possibilité, au moment de sa commande, de s'opposer gratuitement à recevoir de la publicité de sa part.

Qu'en est-il de l'*opt-in* dans le cadre du « *B to B* » ?
La question de savoir si le principe du consentement préalable est exigé dans le cadre de la prospection commerciale entre professionnels (« B to B ») a fait l'objet de nombreux débats au cours de l'année 2004. S'il n'est pas contesté qu'une adresse de courrier électronique attribuée par une société à ses employés reste une information nominative dès lors qu'elle permet l'identification d'une personne physique (exemple nom.prenom@nomdelasociété.fr), les professionnels ont toutefois souhaité que l'application du nouveau dispositif juridique soit assouplie dans le cadre professionnel. La position de la CNIL sur ce point doit être réexaminée au début de l'année 2005.

Comment les entreprises se sont-elles adaptées à l'*opt-in* ?
Le législateur avait aménagé une période transitoire afin que les propriétaires d'adresses de courriers électroniques puissent mettre leur base en conformité avec la loi. Ainsi, ceux-ci pouvaient jusqu'au 22 décembre 2004 contacter les titulaires d'adresses électroniques en utilisant leur messagerie afin de recueillir leur consentement à être prospecté. En l'absence de réponse de leur part pendant cette période, ils sont présumés avoir refusé d'être démarchés.

à des fins commerciales, ne constitue pas une infraction et a relaxé le prévenu en estimant que, *« compte tenu de l'accessibilité universelle de l'internet qui est la caractéristique et un des principaux atouts de ce réseau »*, l'opération de recueil des adresses électroniques sur les espaces publics de l'internet qui n'est pas interdite par une disposition expresse et n'implique l'usage d'aucun procédé frauduleux ne peut dès lors être considéré comme déloyale, du seul fait qu'elle serait effectuée sans que les intéressés en soient informés.

La CNIL recommande

La CNIL ne partage pas cette analyse et a donc souhaité que ce jugement soit réexaminé par la cour d'appel.
De son point de vue, le principe de loyauté de la collecte des informations personnelles impose l'obligation d'informer préalablement les personnes auprès desquelles sont recueillies des données. La collecte est déloyale dès lors qu'elle est faite à l'insu de l'intéressé qui n'est alors pas en mesure de faire jouer ses droits et en particulier son droit d'opposition.
Face au développement de l'internet, la CNIL a considéré que les caractéristiques de ce réseau qui facilitent en effet la captation et la réutilisation des données ne remettaient nullement en cause cette interprétation du principe de loyauté. Il est par ailleurs dommage que le non-respect du droit d'opposition à faire l'objet de prospections par la société incriminée n'ait pas été soumis au tribunal qui aurait probablement retenu ce manquement.
Ce jugement ne remet pas néanmoins en question la lutte contre le spam car celle-ci dispose désormais d'un fondement juridique incontestable avec la loi sur l'économie numérique qui subordonne la prospection par courrier électronique au consentement préalable des personnes.
Enfin, la CNIL va continuer son action contre le spam en utilisant notamment les pouvoirs de sanction dont la nouvelle loi « Informatique et Libertés » l'a dotée.

LE VOTE ÉLECTRONIQUE

Les récentes expérimentations : une volonté d'améliorer la sécurité des dispositifs

La CNIL a été saisie en 2004 de trois principales expériences de vote électronique :

1) La Commission a été amenée à se prononcer sur le vote électronique organisé pour l'élection des membres des chambres de commerce et d'industrie de Paris, Grenoble, Bordeaux, Nice et Alençon. Ce vote électronique concernait **340 000 électeurs** et s'est déroulé en **octobre 2004**. Il s'effectuait par le biais d'un site internet mis à disposition des électeurs par chacune des chambres concernées. Chaque électeur disposait d'un identifiant lui permettant de voter.

Dans son avis, la Commission a pris acte de la volonté d'appliquer sa recommandation portant sur la sécurité des systèmes de vote électronique mais a souligné l'insuffisance de l'expertise indépendante et a demandé qu'une autre expertise soit conduite sur le système de vote pendant les élections afin d'assurer l'effectivité des mesures de sécurité prévues.

La CNIL a estimé, compte tenu de la nature professionnelle des élections, que les dispositions prévues permettant d'assurer l'authentification de l'électeur par un identifiant et un mot de passe apportaient des garanties analogues à celles prévues par le vote par correspondance. **Une telle solution ne sera pas nécessairement transposable à tous types de scrutins**. La Commission estime également qu'en cas de généralisation du système de vote, la confidentialité du vote doit être renforcée par un chiffrement du vote sur le poste de l'électeur dès son émission.

La Commission a insisté sur la nécessité d'améliorer la surveillance des opérations électorales, à la fois par des experts indépendants et par des représentants du corps électoral, afin de veiller, par exemple, à la confidentialité du fichier des électeurs ou à l'intégrité de l'urne.

2) La CNIL a été saisie d'une expérience de vote électronique dans deux universités (**Lyon II et Nantes**) à l'occasion des élections aux conseils d'université. La CNIL s'est félicitée de la volonté de l'administration d'appliquer ses recommandations sur la sécurité. Néanmoins, elle a de nouveau considéré qu'une expertise complémentaire devait être réalisée pendant les élections. La Commission a aussi souhaité que la composition et les missions de la « cellule d'assistance technique », mise en place dans chaque université, soient renforcées afin qu'un réel contrôle des opérations de vote soit effectué par des experts indépendants chez le prestataire technique.

3) La Commission a été saisie d'une déclaration du système de vote électronique mis en place à l'occasion des élections professionnelles **des avocats du barreau de Paris** organisées fin **novembre 2004**. La CNIL a appelé l'attention du bâtonnier sur la nécessité de prendre en compte les mesures préconisées dans sa recommandation du 1er juillet 2003.

En effet, le dossier remis ne permettait pas d'apprécier si le dispositif de vote apportait des garanties suffisantes sur la séparation des données nominatives des électeurs et de celles relatives à leur vote. L'absence de chiffrement du bulletin de vote sur le terminal de vote posait une difficulté supplémentaire. La CNIL a demandé qu'un rapport d'évaluation du processus de vote prenant en compte l'ensemble de ses remarques lui soit envoyé postérieurement au scrutin afin de lever les interrogations concernant celui-ci.

Mauvais plan !

Les systèmes de vote électronique mis en place par les barreaux de Nanterre et de Lyon n'ont pas été déclarés à la CNIL. Elle n'a donc pas été en mesure d'apprécier la conformité à la loi de ces traitements.

Une période charnière pour le développement du vote électronique

Questions à ...

Isabelle FALQUE-PIERROTIN

Conseiller d'État
Présidente du Conseil d'orientation et déléguée générale du Forum des droits sur l'internet
Commissaire en charge du secteur « Libertés publiques »

Quel est le rôle de la CNIL en matière de vote électronique ?

Le vote électronique comporte, en général, des traitements informatiques de données à caractère personnel. À ce titre, la CNIL est compétente pour les examiner. Elle s'est prononcée à de nombreuses reprises sur des expérimentations depuis 2000 avec des avis favorables ou défavorables selon les cas. Surtout, la Commission a souhaité établir en juillet 2003 un guide à l'attention des promoteurs de systèmes de vote électronique sous la forme d'une recommandation « sur les sécurités des systèmes de vote électronique ». Ce texte incitatif constitue aujourd'hui une référence en la matière.

Où en est-on aujourd'hui ?

On se situe aujourd'hui à une période charnière dans le développement du vote électronique. Les dispositifs techniques ont progressé. La recommandation de la Commission est de plus en plus suivie. La vigilance doit cependant être permanente au moment où il est parfois question de généraliser ce vote électronique, sous des formes diverses, y compris à des scrutins politiques. La confiance des citoyens en de tels systèmes ne pourra, en effet, s'établir que lorsque toutes les garanties dans la protection de leurs données seront assurées.

La Commission recommande, enfin, qu'une évaluation globale des dispositifs de vote électronique soit établie par les pouvoirs publics sur la base des récentes expérimentations en matière de vote électronique.

TÉLÉBILLETTIQUE

La carte orange et le coût de l'anonymat

L'essor de la carte à puce associé au développement des dispositifs « sans contact », tels que la technologie de **radio-identification RFID (*Radio Frequency Identification*),** a permis aux exploitants de transports collectifs de mettre en œuvre des applications de télébillettique. Il s'agit d'utiliser une carte à puce comme support du titre de transport, l'un des avantages étant que le passage des contrôles d'accès (« tourniquets » et « portillons ») s'effectue **« sans contact »** *via* une transmission radio. L'une des plus ambitieuses applications télébillettiques développée à l'échelon national est le dispositif **« Navigo »**. Il s'inscrit au cœur de la généralisation de la billettique en Île-de-France et doit à terme être mis en œuvre par toutes les entreprises de transports collectifs de la région, sous le pilotage du syndicat des transports d'Île-de-France (STIF). Ce projet, qui doit s'échelonner jusqu'en 2007, a fait l'objet d'un examen par la Commission à chacune de ses étapes.

La seconde phase concerne l'extension du dispositif billettique « Navigo » aux abonnements mensuels et hebdomadaires du type « carte orange ». À l'initiative du STIF deux types de « cartes orange » billettiques seront ainsi commercialisées au cours du premier trimestre 2005 :

– des cartes nominatives gratuites avec remplacement en cas de perte ou de vol ;

– des cartes déclaratives sans recueil d'informations sur le porteur de la carte, comme à l'heure actuelle, mais commercialisées **au prix de 5 €**.

La RATP et la SNCF ont de nouveau saisi la Commission, en 2004, pour qu'elle se prononce sur les traitements devant être appliqués à ces « cartes orange » billettiques.

Hormis cette question de tarif, les traitements appliqués aux « cartes orange » billettiques étant semblables à ceux précédemment examinés par la CNIL, celle-ci a autorisé leur mise en œuvre par une décision du 8 avril 2004 pour la RATP et du 9 décembre 2004 pour la SNCF. À l'occasion de l'instruction qu'elle a menée, la Commission a jugé satisfaisant le dispositif technique destiné à rendre anonymes les données utilisées en dehors de la lutte contre la fraude.

À propos de …

Navigo

La première phase, aujourd'hui achevée, portait sur le passage à la télébillettique des abonnements annuels « Intégrale » et « Imagine R ». La Commission a émis un avis favorable concernant les traitements mis en œuvre par la RATP le 27 février 2003. Elle a considéré qu'ils étaient de nature à garantir le respect de la liberté d'aller et venir anonymement des personnes. En effet, la RATP a procédé à la modification de son dispositif pour que les données relatives aux déplacements (date, heure, lieu de validation) ne puissent être associées à une personne qu'à l'occasion de la lutte contre la fraude et pendant deux jours au maximum. Parallèlement, la RATP s'est engagée à rendre anonymes les données utilisées dans tous les autres traitements. Par ailleurs, la Commission a émis un avis favorable le 12 novembre 2003 concernant un dossier strictement similaire présenté par la SNCF.

Mauvais plan !

Le prix de l'anonymat …

La Commission a souligné que le fait d'imposer un coût supplémentaire pour les usagers faisant le choix d'une « carte orange » billettique sans recueil d'information sur le porteur de la carte, remettrait en cause la possibilité d'aller et venir anonymement. En conséquence, elle a indiqué au STIF que le choix d'une « carte orange » billettique anonyme ne devrait pas s'accompagner d'un surcoût par rapport au choix d'une « carte orange » billettique nominative. Toutefois, le STIF ayant seul compétence pour définir la politique tarifaire des transports publics en Île-de-France, la CNIL ne peut lui imposer de modifier sa décision.

La répression de la fraude à Lille et à la RATP

La société des transports en commun de la métropole lilloise (Transpole) qui exploite le réseau des transports collectifs de la métropole lilloise connaît un taux de fraude important évalué en 2002 à 24 % des voyages effectués. Transpole a par ailleurs constaté qu'un nombre de plus en plus important de procès-verbaux n'étaient pas remis à leur destinataire consécutivement à l'indication d'une fausse identité ou d'une fausse adresse.

Afin de remédier à cette situation, Transpole a saisi la CNIL d'un projet visant à équiper certains de ses agents d'un **assistant électronique** lors des contrôles des titres de transport. Cet assistant électronique, mis à la disposition des seuls agents agréés et assermentés, devait héberger une copie du fichier des personnes ayant fait l'objet d'un procès-verbal au cours des deux dernières années. L'objectif poursuivi était de permettre à ces agents, face à un contrevenant fournissant des informations renvoyant à un procès-verbal ayant fait l'objet d'une contestation ou ayant été retourné par les services postaux, de faire appel à un officier de police judiciaire pour qu'il procède à une vérification d'identité.

En raison du caractère mobile du dispositif et compte tenu du fait que le fichier concerné porte sur des infractions, la Commission s'est tout d'abord assurée de l'existence de mesures de sécurité tendant à empêcher la communication des données à des tiers non autorisés. Elle s'est également attachée à ce que les données concernées ne puissent pas être utilisées à des fins étrangères à la finalité initiale. À cet égard, la Commission a considéré que seules les informations relatives aux dossiers comportant l'indication d'une fausse identité ou d'une fausse adresse et dont le délai de contestation du procès-verbal était échu devaient être enregistrées dans l'assistant personnel. Elle a également précisé que l'interrogation du fichier ne devait s'effectuer que sur la base d'un nom saisi dans son intégralité.

Enfin, elle a demandé à être rendue destinataire un an après la mise en œuvre du dispositif d'un bilan faisant notamment état de son impact tant sur le taux de recouvrement des procès-verbaux que sur le comportement des usagers des transports en commun de la métropole lilloise. TRANSPOLE s'étant engagé à prendre en compte l'ensemble des demandes émises par la Commission, ce dossier a fait l'objet d'un avis favorable de la CNIL le 8 avril 2004.

La RATP a soumis un dossier similaire à la CNIL. La Commission a alors fait part des mêmes réserves et demandes que lors de l'instruction du dossier TRANSPOLE. La RATP a estimé ne pas être en mesure de garantir la sécurité des données enregistrées sur l'assistant électronique et a renoncé au choix d'un dispositif mobile. Elle a alors proposé que les agents de contrôle accèdent aux fichiers des contrevenants *via* un poste fixe sécurisé et a pris en compte les autres demandes de la CNIL. La Commission a ainsi autorisé en application de la nouvelle loi « Informatique et Libertés », le 9 novembre 2004, la mise en œuvre des traitements proposés.

LES DONNÉES DES PASSAGERS AÉRIENS (PNR) : des transferts légalisés mais non sécurisés

Dans le cadre de la lutte contre le terrorisme et les actes criminels, les États-Unis mettent en œuvre depuis 2003 de nouvelles dispositions en matière de sécurité de l'aviation et du transport et des conditions d'entrée sur le territoire américain. Ces mesures imposent aux compagnies aériennes de communiquer aux services des douanes et de la sécurité américains des informations personnelles relatives à leurs passagers à destination des États-Unis. À défaut, les compagnies aériennes peuvent se voir imposer des contrôles renforcés, des amendes ou même un refus du droit d'atterrir.

Les informations concernées sont celles collectées par les compagnies aériennes et les agences de voyage auprès des passagers dans le cadre des services de réservation. Ces données prennent la forme d'enregistrements d'informations standardisés au plan international dénommés **« PNR »** ***Passenger Name Record.***

Le traitement de ces données et leur communication à des tiers sont encadrés par une directive européenne[11]. La communication de données collectées à des fins commerciales aux autorités américaines n'apparaissait pas conforme à cette directive. En particulier, l'Union européenne a toujours considéré que l'administration des États-Unis **n'offrait pas un niveau de protection adéquat** des données à caractère personnel. Dès lors, ce transfert d'information ne pouvait être envisagé que si les États-Unis prenaient des engagements internationaux pour garantir un niveau de protection adéquat des données relatives aux passagers.

Cet accord international a donné lieu à des discussions entre la Commission européenne, les États membres et les autorités américaines tout au long de l'année 2003, ainsi qu'à de nombreux avis des autorités de protection des données[12] et du Parlement européen. En effet, un premier projet d'accord entre la Commission européenne et les États-Unis leur a été soumis au mois de **janvier 2004**.

À cette occasion, le **« groupe de l'article 29 »** a rendu un avis le 29 janvier 2004 dans lequel il a confirmé le caractère toujours disproportionné des informations demandées, notamment celles relevant des données « sensibles » et indiqué que malgré quelques progrès, les termes de l'accord résultant des discussions avec les États-Unis ne permettaient pas d'assurer un niveau adéquat de protection des données. Pour sa part, le **Parlement européen** reprenant notamment l'ensemble des observations du groupe décidé d'interroger la **Cour de justice des Communautés européennes** (CJCE) afin qu'elle se prononce sur la légalité de l'accord envisagé.

Toutefois, la Commission européenne et les États membres ont décidé de ne pas tenir compte de ces positions. La Commission a ainsi adopté, le **14 mai 2004**, une décision reconnaissant que les données des passagers communiquées aux autorités américaines bénéficiaient d'une protection suffisante. Parallèlement, les États-Unis et l'Union européenne ont signé le 17 mai 2004 un accord international venant légaliser les transferts.

Que contiennent …

Les PNR :

– des renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée ;
– l'itinéraire du déplacement qui peut comporter plusieurs étapes ;
– les indications des vols concernés par l'itinéraire (numéro des vols successifs, date, heures, etc.) ;
– le groupe de personnes pour lesquelles une même réservation est faite, le contact à terre du passager (numéro de téléphone au domicile, professionnel, etc.) ;
– les services demandés à bord tels que le numéro de place affecté à l'avance, les repas (végétarien, asiatique, cascher, etc.) et les services liés à la santé (diabétique, aveugle, sourd, assistance médicale etc.).

11. Directive du 24 octobre 1995 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.

12. Les autorités de protection des données à caractère personnel des différents pays de l'Union dont fait partie la CNIL se réunissent au sein du groupe de travail institué par l'article 29 de la directive 95/46/CE (*cf.* p. 16).

Le « groupe de l'article 29 » a, quant à lui, indiqué que la Commission européenne n'avait que partiellement tenu compte de ses réserves. Par conséquent, il a demandé que des mesures pratiques, essentielles pour limiter les atteintes aux droits des passagers, soient adoptées dans l'attente de la décision de la CJCE.

Dans ce cadre, le 30 septembre 2004, le « groupe de l'article 29 » a émis un avis précisant les informations devant être communiquées par les compagnies aériennes et les agences de voyages aux personnes réservant un vol à destination des États-Unis. Il préconise de faire figurer une courte information sur les formulaires ou de la donner par téléphone et sur les sites internet de réservation, une information plus longue devant être accessible sur simple demande. Ces mentions d'informations précisent la nature des informations qui sont transmises aux autorités américaines, ainsi que les conditions dans lesquelles les personnes peuvent exercer les droits qui leur sont reconnus.

Par ailleurs, le groupe et les États membres ont commencé à examiner les demandes des autorités australiennes et canadiennes de même nature et des travaux d'harmonisation sont menés au sein de l'Organisation internationale de l'aviation civile (OACI) pour faire face aux demandes de même nature d'autres pays.

Au sommet de La Haye en décembre 2004, le Conseil européen a insisté pour que la Commission européenne présente prochainement une initiative visant à doter l'Europe d'un traitement de données PNR des personnes se déplaçant vers ou hors d'Europe. Le débat n'est donc pas clos mais bon nombre des éléments nécessaires à une réflexion plus approfondie sont présents pour définir la méthode propre à assurer la **sûreté aérienne** dans un plus grand respect de la **protection de la vie privée des personnes concernée**. L'approche américaine n'est pas la seule voie, comme le montre celle prise par l'Australie qui aboutit à ce que les seules données des personnes suspectes soient conservées. La sûreté des vols devrait pouvoir être assurée par les services de police du pays de départ des vols et non du pays de destination et plutôt sur la base d'une coopération policière transatlantique. Dès lors l'ensemble des données n'aurait pas besoin d'être transmis de manière systématique.

C'est votre droit

Les compagnies aériennes et les agences de voyages ont pour obligation de vous indiquer dès la collecte de vos données personnelles :
– l'identité du responsable du traitement ;
– la finalité poursuivie par le traitement auquel les données sont destinées ;
– les destinataires ou catégories de destinataires des données ;
– que vous disposez d'un droit d'accès, de rectification et d'opposition ;
– les modalités d'exercice de ces droits. Ainsi, s'agissant d'un voyage à destination des États-Unis, vous devez notamment être informé que vos données seront communiquées aux autorités américaines pour des impératifs de sécurité. Les autorités américaines en question sont le service des douanes et de la protection des frontières (*Customs and Border Protection*), ainsi que toute autre autorité gouvernementale américaine ou étrangère en charge de la lutte contre le terrorisme.

L'ANNUAIRE UNIVERSEL

L'annuaire que nous connaissons tous est devenu une source de renseignements de moins en moins complète puisque, sauf exception, seuls les abonnés à France Télécom y sont présents. Ainsi, n'y figurent pas les abonnés à la téléphonie fixe des autres opérateurs et, bien évidemment, les abonnés à la téléphonie mobile. L'idée de rassembler **l'intégralité** des coordonnées des utilisateurs de la téléphonie dans un même annuaire – dit « annuaire universel » – n'est pas neuve puisqu'elle est prévue depuis 1996 par la loi dite de réglementation des télécommunications. Pour autant, il a fallu attendre qu'un décret en date du 1er août organise la constitution de ces annuaires.

Dans le nouveau schéma, le marché des annuaires devient concurrentiel puisqu'à côté de l'obligation pour un prestataire, choisi sur appel d'offres, d'éditer un annuaire universel national (c'est l'une des composantes du « service universel »), se développeront des annuaires ou services de renseignements proposés par d'autres entreprises.

Le décret du 1er août 2003 a organisé les droits des personnes au regard de la constitution des annuaires ou service de renseignements universel, mais il laissait en suspens un certain nombre de questions. Parmi celles-ci, figurait le cas des abonnés à la **téléphonie mobile** : la CNIL avait estimé que les annuaires universels ne devraient contenir que les données des abonnés à la téléphonie mobile ayant expressément demandé à y figurer. Cette position rompait avec le schéma selon lequel les personnes figurent dans les annuaires sauf si elles s'y opposent. À la suite d'un revirement heureux des différents acteurs, la **loi du 9 juillet 2004** relative aux communications électroniques a finalement entériné une position conforme aux souhaits de la CNIL en adoptant le régime du **consentement préalable** pour les abonnés à la téléphonie mobile. Le Code des postes et télécommunications électroniques sera adapté en ce sens par un nouveau décret, qui devrait comporter d'autres adaptations mises au point dans le cadre d'un groupe de travail réuni à l'initiative de la CNIL. L'année 2005 devrait voir le nouveau décret publié.

Dès maintenant, on peut relever les points suivants.

Les opérateurs de téléphonie devront informer leurs abonnés de leurs droits :
– de figurer dans un annuaire (téléphonie mobile) ;

Questions à ...

Didier GASSE

Conseiller maître à la Cour des comptes
Commissaire en charge du secteur « Télécommunications et réseaux »

En définitive, êtes-vous satisfait des conditions dans lesquelles la protection des données personnelles a été prise en compte dans le projet d'annuaire universel ?

Je pense qu'il s'agit là d'un bon exemple d'une coopération fructueuse entre les services compétents de l'Autorité de régulation des télécommunications, du ministère de l'Industrie, des opérateurs téléphoniques et de la CNIL. En y mettant le temps, nos préoccupations essentielles ont été prises en compte dans la loi et dans le décret à intervenir, qu'il s'agisse notamment des conditions d'inscription des utilisateurs d'une ligne mobile, des effets liés à l'inscription en liste rouge (les données correspondantes devront être retirées des listes avant toute communication à un éditeur d'annuaire) ou de l'information qui devra être diffusée aux abonnés par les opérateurs.

Des problèmes subsistent-ils ?

En donnant son avis sur le dernier projet de décret, nous avons suggéré que soient encadrées les conditions d'inscription des employés titulaires d'une ligne téléphonique à titre professionnel en prévoyant que les informations nominatives les concernant ne puissent être inscrites dans l'annuaire universel qu'avec leur accord exprès. Une telle position se justifie dans la mesure où se développent des formules dans lesquelles les employés sont dotés d'une ligne de téléphonie mobile à usage mixte, à la fois professionnel et privé.

– de s'opposer à y être mentionnés (téléphone fixe) ;
– de la possibilité de ne pas faire figurer l'adresse complète de leur domicile ;
– de ne mentionner que l'initiale du prénom sous réserve d'absence d'homonymie ;
– de ne pas faire l'objet d'opérations de prospection directe (en s'inscrivant sur la liste antiprospection, anciennement liste « orange ») ;
– de ne pas pouvoir être identifiés à partir d'une recherche *via* le seul numéro de téléphone dite « recherche inversée » (en s'inscrivant sur la liste antirecherche inversée).

À leur demande, les abonnés pourront faire figurer :
– les données relatives aux autres utilisateurs de leur ligne ;
– leur profession (sous leur responsabilité).

En pratique, les abonnés à la téléphonie auront six mois à partir du moment où ils auront été informés par leur opérateur pour exprimer leur choix. Les premiers annuaires universels devraient donc voir le jour à la fin de l'année 2005.

LA REDEVANCE AUDIOVISUELLE

La CNIL s'était élevée en 2003 contre une disposition du projet de loi de finances pour 2004 qui risquait d'être interprétée comme autorisant l'administration fiscale à se faire communiquer les fichiers complets des abonnés des diffuseurs ou distributeurs de services payants de programmes de télévision. Cette disposition n'a pas été adoptée par le Parlement.

La question a été une nouvelle fois posée à l'occasion de l'examen de la loi de finances pour 2005 dans le cadre d'un **nouveau dispositif**, entièrement remanié. La solution retenue semble tenir compte des **objections** émises par la CNIL en 2003.

Par ailleurs, la loi ajoute un article L. 96 E au Livre des procédures fiscales qui prévoit que les diffuseurs ou distributeurs de services payants de programmes de télévision devront fournir à l'administration, sur sa demande, les éléments des contrats de certains de leurs clients qui sont strictement nécessaires à l'établissement de la redevance audiovisuelle. Ces informations se limiteront à l'identité du client, son adresse et la date de souscription du contrat.

Ce dispositif est organisé comme une nouvelle modalité du droit de communication du fisc. Il devra, en conséquence, en respecter les conditions générales d'exercice qui ont, cette année encore, été rappelées par la Commission (*cf.* délibération n° 2004-084 du 4 novembre 2004 concernant le traitement HÉLIOS de la direction générale de la comptabilité publique) : les demandes d'informations présentées à ce titre doivent être ponctuelles, avoir un fondement légal et ne concerner qu'une ou plusieurs personnes nommément désignées, sans jamais porter sur l'intégralité ou même une partie d'un fichier. La Commission a demandé à être consultée lors de la phase d'élaboration des textes pris pour l'application de cette disposition.

C'est nouveau

– le service de la redevance est supprimé ;
– la redevance devient un impôt dont le recouvrement, assuré par le Trésor public, est adossé à la taxe d'habitation ;
– la redevance ne sera due qu'une fois par foyer fiscal, quel que soit le nombre de postes qu'il détient dans l'ensemble de ses résidences ;
– les particuliers recevront, avec leur avis d'imposition à la taxe d'habitation, un avis d'imposition à la redevance audiovisuelle ;
– les particuliers devront désormais déclarer sur l'honneur sur une ligne de leur déclaration de revenus ne pas détenir de télévision dans leurs résidences principales ou secondaires ; dans le cas contraire, la condition de détention d'une télévision serait considérée comme remplie ;
– les personnes ne souscrivant pas une déclaration de revenus en leur nom devraient recevoir un courrier de l'administration fiscale leur demandant de déclarer s'ils ne détiennent pas de téléviseur.

LES LISTES NOIRES : le principe de « sectorisation » confirmé par le Conseil d'État

La CNIL avait invité en **novembre 2003** le gérant d'une société en formation qui envisageait de mettre en œuvre un fichier recensant des locataires auteurs d'impayés locatifs, accessible à partir d'un site internet, à limiter la diffusion des informations contenues dans le fichier aux seuls professionnels de l'immobilier et ce afin d'assurer le respect du principe de « sectorisation », ainsi qu'à renoncer à diffuser des informations sur les condamnations, civiles ou pénales. En rejetant la demande d'annulation formée par le gérant de cette société en formation à l'encontre de la mise en demeure adressée par la CNIL, le Conseil d'État, dans un arrêt du 28 juillet 2004 n° 262851, confirme la position de la CNIL sur ces deux points.

Les données à caractère personnel faisant l'objet d'un traitement doivent être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées. En application de cette règle de proportionnalité, la CNIL a défini un **principe de sectorisation**.

Dans le secteur locatif, la CNIL a estimé que la diffusion des informations relatives à des impayés locatifs à des propriétaires immobiliers qui n'ont pas la qualité de professionnels de l'immobilier n'était pas de nature à répondre de façon satisfaisante à l'obligation de sécurité et au principe de proportionnalité.

C'est cette appréciation, *« eu égard aux risques de discrimination et d'atteinte à la vie privée que comporte la diffusion, par l'intermédiaire du réseau internet, de fichiers automatisés recensant des ''personnes à risques'' »*, qui a été validée par le Conseil d'État.

L'auteur de la requête en annulation reprochait également à la CNIL d'avoir estimé que la diffusion d'informations relatives aux jugements ayant prononcé la condamnation d'un débiteur au paiement d'une créance locative relevait de l'interdiction faite aux personnes privées, par l'ancien article 30 de la loi de 1978 modifiée en 2004, de faire des fichiers de condamnations. Le Conseil d'État confirme nettement que cette interdiction s'applique non seulement aux condamnations pénales mais aussi aux condamnations civiles, comme la condamnation au paiement d'une créance locative. C'est une précision importante sur une règle fixée désormais par l'article 9 de la loi de 1978 modifiée en 2004.

Qu'est-ce que c'est ?

Le principe de sectorisation

La mise en œuvre et l'accès à un fichier de « mauvais payeurs » doivent être limités à un secteur et aux seuls professionnels du secteur. Ce n'est pas parce que l'on n'a pas payé son abonnement téléphonique que l'on ne peut louer un logement. Une large diffusion, tous secteurs confondus, des informations relatives à des « mauvais payeurs » serait une atteinte disproportionnée à la vie privée en raison du risque de détournement de finalité.

RÉFLEXIONS EN COURS

LE SECRET DE LA CORRESPONDANCE ÉLECTRONIQUE

Le secret de la correspondance électronique est mis à mal non seulement quand le contenu du message est lu mais aussi quand les données d'envoi et de réception sont traitées, conservées et communiquées à d'autres intervenants que les intermédiaires techniques. La CNIL, après avoir reçu la société Google qui lui a présenté son projet de messagerie gratuite (intitulé « G-mail »), a entamé, en juin 2004, une réflexion sur la question de l'analyse du contenu des messages électroniques.

À la différence de ses concurrents, la messagerie gratuite G-mail se financera sur la publicité mais ne sera pas basée sur l'établissement d'un « profil » de ses abonnés qui serait revendu ou exploité.

G-mail

Qu'est-ce que c'est ?

G-mail

En contrepartie de la fourniture d'un service « ergonomique », pratique, et à forte capacité de stockage, l'abonné G-mail donnera son consentement, lors de la souscription de son contrat, à ce que le contenu de tous les messages, entrant et sortant, de sa boîte aux lettres soit « analysé » par Google. L'abonné (et lui seul) verra alors apparaître, dans une fenêtre dédiée à l'écran, des bannières publicitaires ou des liens vers des sites, ciblés sur certains mots-clés reconnus par Google dans ses messages.

Comment ça marche ?

Lorsque l'internaute consulte sa messagerie, il « rapatrie » sur son ordinateur les données stockées sur le serveur de messagerie (Google en l'espèce). Lors de cette opération, en quelques secondes, le contenu de tous les messages est « scanné » par Google, qui va identifier certains mots-clés « pertinents » et donner l'instruction pour que tel message publicitaire ou tel lien s'affiche.

Quel est le problème posé ?

Le consentement de l'abonné G-mail suffit-il à lever le problème posé par le principe du respect du secret des correspondances, imposé aux opérateurs de l'internet ? En outre, qu'en est-il des personnes qui envoient des messages, dont le contenu est scanné, à des abonnés G-mail mais qui n'ont pas donné leur consentement ?

Le sujet a été largement débattu au sein des autorités de protection des données européennes, dans le cadre des travaux du **groupe « de l'article 29 »**, qui devrait adopter prochainement une position commune sur ces délicates questions.

Did they read it ? (l'ont-ils lu ?)

Qu'est-ce que c'est ?

Did they read it (l'ont-ils lu) ?

La société américaine « Rampell Software » propose, depuis la fin du mois de mai 2004, un service de suivi du courrier électronique intitulé *Did they read it ?* (en français « L'ont-ils lu ? »).

Comment ça marche ?

Ce service permet à un internaute, moyennant le paiement d'un abonnement, de savoir si les destinataires de ses messages électroniques les ont lus, à quel moment, combien de fois, pendant combien de temps, s'ils les ont transmis à d'autres personnes et depuis quel serveur de messagerie. Il permet également de connaître le navigateur utilisé par le destinataire ainsi que son système d'exploitation.

Quel est le problème posé ?

Le processus se déroule entièrement à l'insu des destinataires des messages électroniques. À la différence des

L'avis de la CNIL

La CNIL a émis les plus vives réserves sur le procédé *« Did they read it »*. En effet sont enregistrées et transmises des informations détaillées sur le « comportement » du destinataire d'un message électronique. Une telle collecte, effectuée à l'insu des personnes, est contraire aux règles de protection des données et plus précisément à l'article 25 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui interdit la collecte de données nominatives opérée par tout moyen frauduleux, déloyal ou illicite.
La CNIL a ainsi rappelé que le non-respect de ces dispositions est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (article 226-18 du Code pénal).
Elle a publié un communiqué de presse en juin 2004 pour attirer l'attention des entreprises françaises, des administrations et plus largement du public sur le fait qu'en s'abonnant à *Did they read it ?* toute personne présente sur le sol français est susceptible d'encourir des poursuites pénales.

services d'accusé de réception fournis par les logiciels de messagerie « classiques », **le destinataire n'a pas le choix** d'accepter ou de refuser de retourner les informations à l'abonné à *Did they read it ?* Il n'en est même pas informé.

L'avis du G29 sur la conservation des données dites « de connexion »

On entend par « données de connexion », l'ensemble des données techniques produites par l'utilisation des moyens de communications électroniques. Chacun de nous crée, chaque jour, de nombreuses données de ce type en utilisant son téléphone fixe (Qui j'appelle ? Pour combien de temps ?), son téléphone mobile (D'où j'appelle ?) ou encore le réseau internet (Quels sites vais-je visiter ? À qui j'envoie des courriers électroniques ? Quel en est le contenu ?), etc. On le voit, ces données sont directement liées à notre vie privée et leur conservation par les opérateurs et leur accessibilité par les autorités publiques font l'objet d'une attention toute particulière.

La conservation des données dites « de connexion » est au centre des problématiques « informatique et libertés » actuelles. Au cours de l'année 2003, la CNIL avait rendu un avis important[13] sur un projet de décret encadrant la conservation de certaines de ces données par les opérateurs. Elle avait notamment estimé que les opérateurs ne devaient être obligés de conserver pour une durée n'excédant pas trois mois certaines de ces données pour les mettre, éventuellement, à la disposition des autorités judiciaires. Ce décret n'a, à ce jour, toujours pas été publié.

L'année 2004 a vu la question de la conservation des données « de connexion » posée au niveau européen par un projet de décision-cadre qui, à l'initiative de la France, de l'Irlande, de la Suède et de la Grande-Bretagne, vise à poser un cadre juridique unique pour l'ensemble des opérateurs européens. Au regard de ce projet, les opérateurs de communications électroniques seraient obligés de conserver certaines de ces données, pour une période d'un à trois ans, *« aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme »*.

Ce projet a conduit la CNIL à participer à la consultation publique lancée par la Commission européenne où elle a pu rappeler sa position qui vise à limiter strictement la durée de conservation de ces données, eu égard à leur sensibilité.

Cette position a été confirmée par l'avis du 9 novembre 2004 du G29 qui, en rappelant que ce projet *« s'appliquerait, non seulement à certaines personnes qui seraient surveillées en application de lois spécifiques, mais à tous les particuliers qui utilisent les communications électroniques »*, a considéré que la conservation de données « de connexion » ne devait s'appliquer que pour une durée limitée, appropriée et proportionnée au sein d'une société démocratique pour conclure que des périodes de conservation supérieures à six mois sont « manifestement disproportionnées ». Le G29 estime, enfin, que le projet de décision-cadre qui constitue une atteinte au secret des correspondances ne satisfait pas en l'état aux exigences posées par **l'article 8 de la Convention européenne des Droits de l'homme.**

Nul doute, dès lors, que la problématique de la conservation des données « de connexion » tiendra une place privilégiée dans l'agenda 2005 des autorités de protection européennes et que la CNIL se montrera très attentive quant à l'évolution de ce dossier.

13. Délibération n° 03-056 du 9 décembre 2003, 24e rapport d'activité p. 40 et 334.

LES « CENTRALES POSITIVES » : demain en France comme aux États-Unis ?

À l'heure où est relancé en France le débat relatif à l'introduction de « centrales positives » dans une optique de développement du crédit à la consommation, la CNIL a auditionné lors de sa séance plénière du 13 mai 2004, Joël Reidenberg, professeur de droit à l'université Fordham (États-Unis), sur l'état de la question aux États-Unis.

M É M O

90 % de la population adulte américaine est fichée par les « credit reporting agencies » (centrales positives)

Qu'est-ce que c'est ?

« Credit report », what does that mean ?

Le rapport de renseignements ou « *credit report* » ne concerne pas uniquement les crédits, mais le consommateur en tant que tel. Au côté des éléments « positifs » tels que les éléments d'identification de la personne, employeur, revenus, logement, informations de nature fiscale, type et historique des crédits et des remboursements, figurent des éléments « négatifs » tels qu'incidents de paiement, autres incidents (liquidation judiciaire, implication dans un procès, décisions ...), mais également les personnes à qui l'entreprise a diffusé le rapport sur le consommateur.
Ces fichiers sont alimentés par les informations communiquées par les établissements de crédit, mais également par une réutilisation des données publiques (cadastre, impôts, tribunaux) ou à partir des informations communiquées directement par la personne à son employeur, par exemple ou lorsqu'elle sollicite une bourse d'études ou loue un logement.
La mise à jour de ces fichiers est assurée par l'application d'un principe de réciprocité : pour consulter le fichier, il faut d'abord l'alimenter. En l'absence de contrôle ou même de responsabilité des « *credit reporting agencies* » du fait de la qualité des données, la fiabilité de l'information diffusée est très variable.

Une finalité sans cesse élargie

Une définition très large des finalités pour lesquelles des informations peuvent être collectées et diffusées à des fins onéreuses par les « *credit reporting agencies* » résulte de l'application du « *fair credit reporting act* » de 1970. Le « *credit report* » d'une personne peut être obtenu pour toute décision d'octroi de crédit, mais aussi pour le recrutement de salariés, la souscription de polices d'assurance, et toutes transactions effectuées par le consommateur. Des compagnies de téléphonie mobile et d'électricité, arguant que le paiement différé était assimilable à un crédit, accèdent ainsi aux informations sur les consommateurs.

Les réformes législatives de 1996 et 2003, se fondant sur des études macro-économiques très contestées dans leur méthodologie relative aux effets de la diffusion de renseignements sur les taux de crédit, ont eu pour effet notable d'autoriser la communication des informations à des fins de prospection commerciale ainsi que la diffusion des informations au sein des filiales des sociétés autorisées à y accéder.

L'immunité légale des « credit reporting agencies »

Afin de favoriser la création du marché national du renseignement, la loi a accordé dès l'origine une immunité à l'agence de renseignement. Ainsi, en cas d'inexactitude

La CNIL explique

Les fichiers « négatifs » ou « listes noires » renseignent sur l'historique des défauts et arriérés de paiement d'un emprunteur.

Les « fichiers positifs » ou « listes blanches » fournissent des rapports détaillés sur l'actif et le passif d'un emprunteur, ses capacités de remboursement, ses garanties, les statistiques de remboursement...

de l'information diffusée, seul le fournisseur de l'information peut être inquiété.

Le contrôle de l'application de la loi est pour l'essentiel du ressort des consommateurs qui intentent des procès privés pour refus d'embauche ou de crédit à cause de renseignements erronés. Enfin, nonobstant les réformes de 1996 et 2003 qui visaient à renforcer la protection contre le vol d'identité, les problèmes liés à l'usurpation d'identité sont une source constante de préoccupation.

Bien entendu, l'Europe offre d'autres modèles de « centrales positives », à travers par exemple les lois allemande ou belge.

Dernière minute !

La CNIL a examiné, lors de sa séance plénière du 18 janvier 2005, un rapport de synthèse sur les problèmes soulevés, au regard des principes de la loi du 6 janvier 1978, par les fichiers regroupant les informations sur la situation financière des individus, souvent appelés « centrales positives ». Elle relève les incertitudes des objectifs mis en avant pour justifier la nécessité de ce type de fichiers. Elle estime que si le législateur décidait la création d'un tel instrument, il conviendrait de définir une finalité aussi claire et précise que possible et de prévoir des garanties fortes pour prévenir le risque d'une utilisation non conforme et d'un détournement du fichier. Devraient ainsi être fixées dans la loi la nature des données recensées et diffusées, la forme de leur restitution aux organismes de crédit utilisateurs, les modalités de règlement des litiges et d'exercice du droit de rectification, une durée de conservation limitée. Enfin, comme pour le FICP, sa gestion devrait être confiée à la Banque de France.

DE L'INTERCONNEXION À LA NAVIGATION : nouvelle approche de la question des identifiants

La CNIL est née d'une crainte, celle d'une possible interconnexion généralisée grâce à un identifiant unique. Trente ans plus tard, après internet et les réseaux, ces enjeux d'interconnexion et d'identifiant ont évolué. La montée en puissance d'internet s'est accompagnée du déploiement de langages hypertextes et de procédures de navigation pilotées par les internautes. Pour la CNIL, il est important de regarder comment cette logique de la navigation se combine à celle de l'interconnexion.

Un peu d'histoire

L'informatique dans les années 70

L'informatique des années 70 se caractérise par une concentration encore forte de son utilisation dans les grandes structures (500 grandes entreprises concentrent 80 % des dépenses informatiques) et l'administration, par une technologie de gros systèmes centralisés ne supportant que des terminaux passifs et par une organisation des données sous forme de fichiers à structure fixe dont l'en-tête des enregistrements joue le rôle d'index.

Questions à …

Philippe LEMOINE

Coprésident du directoire des Galeries Lafayette
Président de Laser, Commissaire en charge du secteur « Technologie »

Qu'entendez-vous par « logique de navigation » ?
En utilisant les fonctionnalités nouvelles des architectures de réseaux, le web offre aux internautes des moyens de plus en plus fluides, de moins en moins heurtés dits « sans couture » (on ne voit pas qu'on passe d'une information située d'un endroit du monde à une autre stockée ailleurs sur la planète …), de « surfer » sur les grandes masses d'informations et entre les services qui y sont accessibles, notamment les services de l'administration électronique. Cette logique de « navigation », pilotée par les personnes, paraît se substituer à l'ancienne logique d' « interconnexion » mise en œuvre depuis le centre par les institutions et consistant en des relations occasionnelles entre les grandes applications.

Quelles sont les limites à cette logique ?
Le web – espace public – n'est pourtant pas la seule voie d'avenir pour l'administration électronique. Lorsqu'il s'agit d'applications complexes, entraînant des transferts de droits (dossier d'inscription, production de justificatifs de diverses origines, paiement, etc.), deux éléments limitent l'approche « navigation » : la simplicité et la sécurité. D'où l'idée de recourir à des systèmes de coffres-forts électroniques permettant de simplifier et de sécuriser les transactions grâce aux quatre fonctions de ces outils : gestion d'identité(s) et trousseau de clés (plusieurs pseudonymes), authentification d'une identité partagée par un tiers, anonymisation, archivage sécurisé pour le compte d'une personne. Dès lors que les opérations deviendront plus complexes, on peut se demander s'il ne faudrait pas, pour des raisons de sécurité, chercher des solutions hors de l'espace public, comme c'est déjà le cas avec le Réseau santé social (RSS).

Quel est le rôle de la CNIL dans ce contexte ?
Il apparaît ainsi que la CNIL doit non seulement maintenir sa doctrine sur l'interconnexion et les identifiants pour le monde « hors ligne » mais s'en inspirer pour raisonner sur internet et les réseaux. De manière générale, l'approche à privilégier est celle de la navigation pilotée par les personnes, les individus-acteurs. Lorsque des applications posent des problèmes de simplicité d'usage et de sécurité trop lourds, il est possible de conforter cette approche en utilisant des outils de type « coffre-fort », à condition d'en mesurer les limites et les biais. Il est important en particulier que les acteurs gardent le contrôle de leurs données.

Le vote de la loi « Informatique et Libertés »

La loi du 6 janvier 1978 provient d'une réaction au projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) de faire jouer un rôle d'identifiant unique au numéro INSEE, **le NIR (numéro d'inscription au répertoire national d'identification des personnes physiques),** communément appelé « numéro de sécurité sociale ». Elle encadre fermement le dispositif de l'identifiant unique. L'utilisation du NIR est subordonnée à une procédure solennelle, un décret en Conseil d'État pris après avis de la CNIL. La gestion même du répertoire national d'identification des personnes physiques fait l'objet de mesures de haute sécurité (destruction possible) sous le contrôle de la Commission. La CNIL a donc veillé à limiter l'utilisation du NIR et à promouvoir des identifiants sectoriels, jouant le rôle d'identifiants transversaux dans un domaine administratif répondant à des finalités homogènes.

L'évolution de l'informatique

Les évolutions des années 70 portaient sur la structure des données. Celles des années 80 et 90 portent sur l'architecture des moyens de traitement : l'informatique devient une informatique de réseau et plusieurs types d'architectures illustrent cette évolution par étape vers l' « intelligence répartie ». Dans l'architecture ordinateur central/terminaux passifs des années 70 les terminaux n'avaient pas de capacité de traitement ni de stockage et permettaient seulement d'interroger l'ordinateur central. Puis est arrivé le réseau en étoile, architecture maître/esclave où la base de données qui fait foi est celle qui est située sur l'ordinateur principal. Lui ont succédé le réseau local, architecture client/serveur où le serveur fournit des ressources et l'initiative est décentralisée, avec faculté de réplication, l'architecture « trois tiers », qu'on trouve actuellement dans l'administration, puis l'architecture « pair à pair » / *peer to peer* où les utilisateurs s'organisent entre eux et peuvent s'appuyer sur un logiciel qui leur donne toutes les listes d'indexation (le point important étant ici l'adressage).

La mise en place de ces architectures réparties sur des couches de communication efficaces (IP) permet de renverser la logique d'un centre gouvernant la périphérie pour y substituer une logique où chaque élément périphérique du réseau peut gouverner les échanges.

IMAGE ET INTERNET

La diffusion d'images par internet est un sujet qui a intéressé la CNIL tout au long de l'année 2004.

En premier lieu, la Commission a fréquemment été saisie de questions relatives à la diffusion, à partir du site web « Pages jaunes », des photos des immeubles des principales villes de France. Elle a veillé à l'application de la loi « Informatique et Libertés » à ce type de traitement. En effet, elle a considéré que la photographie d'un immeuble, associée à son adresse, permet éventuellement de rattacher à cette information le nom de la personne qui l'occupe. En ce sens, elle estime qu'un annuaire de photographies numériques de façades d'immeubles était constitutif d'un traitement automatisé de données à caractère personnel. Dans ce cadre, la société Pages Jaunes a satisfait aux dispositions de la loi de 1978 modifiée en 2004, notamment celles qui imposent d'effectuer auprès de la CNIL une déclaration préalable avant la mise en œuvre de ce traitement.

La CNIL informe

La diffusion à partir d'un site web ouvert au public de données à caractère personnel (le nom d'une personne ou son image) constitue un traitement automatisé de données à caractère personnel et reste, dans l'attente de l'adoption par la CNIL d'une norme d'exonération sur le sujet, soumise à l'obligation de déclaration prévue à l'article 22 de la loi.

Questions à …

Emmanuel de GIVRY

Conseiller à la Cour de cassation
Commissaire en charge du secteur « Gestion des risques et des droits »

La photographie est-elle une donnée à caractère personnel ?

En application de la directive du 24 octobre 1995 et de la loi de 1978 modifiée en 2004, la photographie d'une personne en tant que telle est une donnée à caractère personnel dès lors qu'elle permet d'identifier la personne à laquelle elle se rapporte (parce que cette photographie représente nettement un visage ou un détail physique assurément identifiable), quand bien même un nombre limité de personnes est capable d'associer à cette photographie le nom de la personne auquel elle se rapporte. À l'inverse, la photographie d'une silhouette, d'une ombre, d'un détail physique commun ou encore d'un groupe de personnes sans qu'il soit possible d'en identifier une précisément, ne constitue pas une donnée à caractère personnel.

Pour autant, diffuser des photos sur internet est-ce faire un traitement de données personnelles ?

Une décision de la Cour européenne de Justice a considéré l'opération consistant à faire figurer sur une page internet librement accessible des données à caractère personnel comme un traitement automatisé de données à caractère personnel. Cette solution, appliquée à l'image, revient à considérer que la diffusion à partir d'un site web de l'image d'une personne identifiable constitue, à elle seule, un traitement de donnée à caractère personnel et conduit à l'application des dispositions de la loi « Informatique et Libertés ».

Même quand on diffuse les photos de famille sur une *home page* ?

On relèvera que la loi « Informatique et Libertés » ne s'applique pas pour l'exercice d'activités purement personnelles ou domestiques. À titre d'exemple, la photographie d'un parent ou d'un ami par un appareil photographique numérique ou par un téléphone portable nouvelle génération et la diffusion de cette image par courrier électronique ou par MMS à un nombre limité de correspondants ou par l'intermédiaire d'un site web dont l'accès est restreint, ne rentrent pas dans le champ de compétence de la CNIL. De la même façon, la photographie et la publication de photographies de personnes identifiables aux seules fins de journalisme ou d'expression artistique ne sont pas soumises aux principales dispositions de la loi de 1978 modifiée en 2004 dans la seule mesure où ces exceptions s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

En second lieu, la Commission s'est intéressée à la question de l'application de la loi « Informatique et Libertés » à la diffusion sur internet d'images de personnes.

L'application, le cas échéant, des dispositions de la loi de 1978 modifiée en 2004 conduit à informer les personnes dont les images sont utilisées, de l'identité du responsable du traitement, de la finalité de celui-ci (diffusion de son image sur un intranet, sur internet, etc.), des personnes destinataires de cette image et de l'existence d'un droit d'accès et de rectification. Enfin, l'article 38 de la loi reconnaît à toute personne physique le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Ces dispositions rejoignent, dans une large mesure, les principes protecteurs du droit à l'image qui permettent à toute personne de s'opposer – quelle que soit la nature du support utilisé – à la reproduction et à la diffusion, sans son autorisation expresse, de son image. Dans le cas d'images prises dans les lieux publics, seule l'autorisation des personnes qui sont isolées et reconnaissables est nécessaire.

C'est votre droit

Le droit des personnes dont les informations sont traitées

En application de l'article 38 de la loi, les personnes nominativement rattachées à la photographie d'un immeuble d'habitation peuvent exercer, gratuitement, leur droit d'opposition à ce qu'apparaisse sur ce site la photographie de leur immeuble ou de leur maison. Pour autant, ce droit ne peut être exercé que par la personne occupant un immeuble (que celle-ci soit locataire ou propriétaire) et dont le nom y sera associé. Ainsi, en cas de résidents multiples (cas d'une copropriété par exemple), la photographie de l'immeuble ne saurait être considérée comme une information nominative – la photographie ne concerne pas une personne déterminée – et n'entraîne donc pas l'application de la loi de 1978 modifiée en 2004.

L'autorisation préalable des personnes dont la photographie de l'immeuble qu'elles occupent est diffusée

La loi « Informatique et Libertés » modifiée prévoit dans son article 7 qu' « un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes : [...] la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée ». Sous le régime de la loi du 6 janvier 1978 non encore modifiée, la Commission avait estimé qu'il n'y avait pas de violation des droits et libertés des personnes. Elle maintient cette analyse dans le cadre de la nouvelle loi. Ainsi, il apparaît que la société Pages Jaunes n'est pas tenue, au regard de la loi « Informatique et Libertés » modifiée, d'obtenir le consentement des personnes dont les noms peuvent être rattachés à la photographie d'un immeuble.
Enfin, au regard du droit qu'une personne dispose sur un bien dont elle est propriétaire, on peut rappeler que la Cour de cassation a estimé, dans une décision du 7 mai dernier, que « le propriétaire d'une chose ne dispose pas d'un droit exclusif sur l'image de celle-ci ; qu'il peut toutefois s'opposer à l'utilisation de cette image par un tiers lorsqu'il lui cause un trouble anormal ». En l'espèce, il appartient aux personnes de prouver le caractère « anormal » du trouble que leur cause la diffusion de la photographie de leur immeuble par la société Pages Jaunes afin d'obtenir la cessation de cette diffusion et, le cas échéant, d'en obtenir des dommages et intérêts.

AU PROGRAMME 2005

LA DESCRIPTION DES MINORITÉS

La question de la **lutte contre les discriminations** en raison de l'origine ethnique ou nationale des personnes ou de leurs convictions religieuses est devenue centrale en 2004. Plusieurs rapports et études ont en effet alimenté le débat sur les moyens à mettre en œuvre pour garantir le respect du principe d'égalité de traitement des personnes dans l'accès à l'emploi ou à un certain niveau de responsabilités professionnelles, dans l'accès au logement ou encore dans l'accès à certains services.

La Haute autorité de lutte contre les discriminations et pour l'égalité (HALDE), créée par la **loi du 30 décembre 2004**, constitue l'illustration la plus visible de la volonté des pouvoirs publics d'agir en ce domaine.

L'enregistrement, au sein des fichiers des services publics, d'indicateurs statistiques identifiant les populations étrangères ou issues de l'immigration est présenté par beaucoup, et en particulier par la Cour des comptes dans son rapport de novembre 2004 sur l'accueil des immigrants et l'intégration, comme l'un des moyens de disposer de données objectives sur la question afin de mettre notre société en position d'agir en connaissance de cause. Une idée comparable a pu être avancée par certains en matière de fichiers de gestion des ressources humaines afin de mieux cerner la réalité des discriminations dans le monde du travail.

Sur un plan plus particulier, l'attention portée sur ces questions s'est également traduite par la modification des modalités du recensement de la population jusqu'alors applicables en Nouvelle-Calédonie et en Polynésie française. Ce recensement avait jusqu'à une date récente comporté des questions relatives à la communauté d'appartenance, à la tribu d'appartenance ainsi qu'au statut des personnes qui pour la Commission répondaient à un motif d'intérêt public pour ces territoires.

Le point sur...

Le traitement de la nationalité

Anne DEBET

Professeur des universités
Commissaire en charge du secteur « Affaires sociales »

La nationalité est-elle une donnée sensible ?

Non au sens strict du terme car elle n'est pas visée dans la liste des données dont le traitement est *a priori* interdit (article 8 de la loi du 6 janvier 1978).

Oui car elle peut être source de discrimination pour les étrangers résidant en France.

Quelles sont les conditions de traitement de la nationalité des usagers par les organismes publics (État, collectivités, organismes de protection sociale, services statistiques) ?

La CNIL est régulièrement amenée à rappeler sa position sur la question du traitement informatique de la donnée « nationalité » par les organismes publics. Elle a ainsi été auditionnée en 1996 par la commission d'enquête de l'Assemblée nationale sur l'immigration clandestine et le séjour irrégulier d'étrangers en France et, plus récemment, consultée par la Cour des comptes dans le cadre de son rapport public sur la politique nationale d'accueil et d'intégration des immigrants. Comme pour l'ensemble des données personnelles, la CNIL a toujours veillé à ce que le traitement informatique de la donnée relative à la nationalité soit envisagé dans le respect des principes de finalité et de pertinence des données traitées établis par la loi « Informatique et Libertés ». Elle rappelle donc que l'enregistrement de la nationalité des usagers des services publics peut être réalisé si cette donnée s'avère nécessaire soit pour la gestion administrative de leur dossier, soit pour la production d'indicateurs statistiques.

Sous quelle forme la nationalité peut-elle être enregistrée ?

Dans le domaine de l'action sociale et de l'emploi, la CNIL recommande en général l'enregistrement de la donnée « nationalité » sous la simple forme : « Français, ressortissant d'un pays membre de l'Union européenne, ressortissant d'un pays tiers à l'Union européenne ». Contrairement à une idée trop répandue, elle ne s'est jamais opposée au traitement de la nationalité détaillée dans le cadre d'études statistiques dès lors que cette donnée s'avérait adéquate, pertinente et non excessive au regard des objectifs de l'étude.

À la suite des critiques formulées par le Président de la République sur le recueil de telles informations, de nouvelles modalités de recensement en Nouvelle-Calédonie ne prévoyant plus l'enregistrement des données ethniques ont été définies par l'INSEE et ont reçu un avis favorable de la CNIL dans le courant de l'année 2004.

Le caractère essentiel du recueil de ces données a toutefois été rappelé par plusieurs mouvements locaux notamment le FLNKS considérant que la suppression des questions sur l'appartenance ethnique ne permettrait plus de mesurer le rééquilibrage démographique entre les communautés et l'attribution importante de subventions, conformément aux accords de Matignon de 1988. Compte tenu du *boycott* d'une partie des opérations de recensement, l'INSEE a présenté à la CNIL, en décembre 2004, de nouvelles modalités permettant de calculer de façon fiable la population du territoire et de contribuer ainsi à la préservation de l'intérêt général.

Face à la complexité de ces questions touchant à l'identité de la personne et au respect de ses droits, la CNIL a décidé de contribuer, dans le cadre de ses compétences, à la réflexion nationale en cours en mettant en place un groupe de travail sur le traitement des données révélant l'origine raciale ou ethnique.

LE DÉBAT SUR L'INTRODUCTION D'UNE CARTE D'IDENTITÉ ÉLECTRONIQUE : l'exemple britannique

Résumé de l'intervention faite le 19 novembre 2004 par Richard Thomas, commissaire à l'information du Royaume-Uni, au colloque de l'université de Lille II, sur l'administration électronique présidé par Alex Türk.

La carte d'identité a, en Grande-Bretagne, une histoire plus ancienne qu'on ne le croit puisqu'elle fut introduite une première fois **en 1939**. Son utilisation était réservée au départ à trois ministères. Dix ans après, 39 administrations en avaient l'usage pour toutes sortes de motifs, c'est pourquoi elle fut abolie en 1952.

En 1995, une nouvelle tentative d'introduction échouait notamment face à l'opposition du commissaire à l'information.

En 2002 le gouvernement travailliste relançait un projet de carte d'identité biométrique qui a débouché sur l'examen d'un projet de loi par le Parlement. L'avant-projet de loi annonçait la création d'une carte d'identité avec une puce contenant des données biométriques, d'un registre national d'identité et d'un numéro national d'identité. Le commissaire à l'information, consulté sur cet avant-projet par la commission de l'intérieur de la chambre des communes, tout en reconnaissant l'existence d'avantages potentiels, a exprimé ses interrogations et même des inquiétudes. Interrogation sur le choix de technologies biométriques (empreintes digitales, iris, reconnaissance faciale) dont le Gouvernement britannique a admis qu'elles étaient encore en cours de développement. Interrogation sur les mesures de sécurité entourant l'accès aux informations contenues dans la carte.

À venir

La chambre des communes a adopté le 20 décembre 2004 le projet de loi en seconde lecture (examen avant passage en commission) *Identity Cards Bill* introduisant la carte d'identité biométrique facultative, créant le registre national d'identification et le NIRN (*National Identity Regisration Number*).

Interrogation sur les situations où le besoin de vérifier en ligne ces informations est incontestable. Inquiétudes sur l'étendue des informations qui seront enregistrées sur le registre national (Pourquoi toutes les adresses successives d'une personne ?) ou sur le grand nombre d'administrations qui pourraient y avoir accès (la police, les services secrets mais aussi des services fiscaux et d'autres). Apparaît comme un risque majeur – l'expérience de 1939-1952 l'a montré – un « glissement de fonctions », un dévoiement des finalités initiales.

Toutefois 80 % des Britanniques pensent que cette carte d'identité est *a good idea*. Il n'est pas interdit de penser que ce chiffre pourrait baisser si la population prenait conscience de toutes les implications du projet.

Le point sur...

Biométrie et titres d'identité : un enjeu de société majeur !

François GIQUEL

Conseiller maître à la Cour des comptes
Commissaire en charge du secteur « Sécurité »

Quelle est la particularité de la donnée biométrique ?
L'information biométrique, parce qu'elle signe une réalité biologique qui nous appartient en propre, parce que, numérisée, elle nous échappe aussitôt, se prêtant à toutes sortes de bons et mauvais usages, n'est pas une donnée personnelle comme une autre. Ce statut spécifique, la nouvelle loi « Informatique et Libertés » vient de le consacrer en soumettant les traitements de données biométriques au contrôle préalable de la CNIL.

Quelle est la position de la CNIL sur ce sujet complexe ?
Jusqu'à présent, la Commission s'est prononcée favorablement à de nombreuses reprises sur des dispositifs traitant les données biométriques, en particulier pour l'accès à des locaux sécurisés, tout en soulignant les risques particuliers liés aux empreintes digitales – car on en laisse un peu partout malgré soi – et en marquant sa préférence pour les solutions laissant à chacun la maîtrise et l'usage exclusif de ses données, conservées sur un support tel que la carte à puce. Elle s'est, en revanche, toujours montrée réservée sur la constitution de bases centrales de données biométriques.

Où en sommes-nous aujourd'hui en matière de biométrie ?
Aujourd'hui, le problème est en train de changer d'échelle : au niveau européen, des initiatives viennent d'être prises pour introduire la biométrie dans les visas et les passeports ; en France, il en est fortement question pour la future carte nationale d'identité, une expérimentation est en cours sur les visas.

Que préconisez-vous pour maintenir le point d'équilibre essentiel entre sécurité et liberté ?
Il est temps que s'engage un grand débat public sur les implications d'un usage massif de la biométrie comme principe d'identification de l'ensemble des citoyens, associé à de grandes bases de données nationales, européennes, demain, peut-être, planétaires. Il faut, avant tout choix politique, que les enjeux de société soient bien appréhendés, les risques, évalués, les garanties nécessaires, assurées. Le Parlement européen, en adoptant récemment une résolution sur le projet de règlement relatif au passeport biométrique, s'est engagé dans cette voie ; pour sa part, il a pris position contre le projet d'une base centralisée de données.
Le débat sur la biométrie ne doit pas être clos trop vite, comme si la biométrie était une solution de facilité : certaines décisions, apparemment techniques, apparemment dictées par les nécessités du moment, peuvent engager durablement et gravement l'avenir. À chacun de s'engager dans le débat qui s'ouvre.

LA « GÉOLOCALISATION » DES INDIVIDUS POTENTIELLEMENT DANGEREUX

Le FIJAIS

La Commission a été saisie à la fin de l'année 2004 du **projet de décret d'application prévu par l'article 706-53-12 du Code de procédure pénale**, qui doit définir les modalités et conditions d'application des **articles 706-53-1 à 706-53-12 du Code de procédure pénale** et préciser notamment les conditions dans lesquelles le fichier conserve la trace des interrogations et consultations dont il fait l'objet.

Au titre des garanties figurant dans la loi, on trouve notamment le rôle prépondérant du magistrat dirigeant le service du casier judiciaire en matière de contrôle de la légalité des informations enregistrées, lui permettant d'aller jusqu'à refuser les enregistrements qui ne seraient pas conformes aux exigences légales et réglementaires.

Afin d'empêcher toute inscription frauduleuse, les demandes d'inscription émanant des procureurs de la République et des juridictions feront l'objet d'une vérification par les services du casier judiciaire avant d'être accessibles aux différents destinataires ; de même, et afin d'éviter toute erreur d'homonymie pouvant avoir des conséquences graves pour les intéressés, l'identité des personnes devant être inscrites dans le FIJAIS fera également l'objet d'une vérification.

S'agissant des **demandes de rectification et d'effacement**, il est prévu, en cas de refus, une possibilité de recours à double degré devant deux juridictions différentes, à l'instar de la procédure déjà prévue par le décret relatif au **fichier national automatisé des empreintes génétiques (FNAEG).**

La Commission se prononcera au premier trimestre 2005 sur les dispositions de ce projet de décret ; le dossier de formalités préalables qui lui sera transmis lui permettra d'apprécier l'adéquation des mesures techniques adoptées, tant en ce qui concerne l'alimentation du fichier, sa confidentialité que ses conditions d'accès.

Il lui appartiendra de s'assurer que le cadre juridique proposé est de nature à garantir la confidentialité des informations inscrite au fichier, et tout particulièrement celle de l'adresse des intéressés, dont elle a souligné la sensibilité.

À propos des fichiers

Le FIJAIS (Fichier judiciaire automatisé des auteurs d'infractions sexuelles)

Les articles 706-53-1 à 706-53-12 du Code de procédure pénale, introduits dans ce Code par un amendement à la loi du 9 mars 2004, dite « loi Perben II », portant adaptation de la justice aux évolutions de la criminalité, définissent les conditions d'inscription, automatique ou sur décision expresse d'une juridiction, des auteurs de certaines infractions sexuelles.
Ces dispositions imposent en outre aux personnes inscrites dans le FIJAIS de justifier de leur adresse une fois par an et de déclarer leurs changements d'adresses dans les quinze jours ; les auteurs d'infractions les plus graves doivent, tous les six mois, justifier en personne de leur adresse.
L'inscription dans le fichier et l'obligation liée de déclarer son adresse ont pour objectif de réaliser la double finalité que la loi a assignée à ce fichier : d'une part, prévenir la récidive par des auteurs d'infractions sexuelles déjà condamnés et, d'autre part, identifier plus facilement les auteurs de ces mêmes infractions.

Le FNAEG (fichier national des empreintes génétiques)

Conçu à l'origine pour faciliter l'identification et la recherche des auteurs d'infractions sexuelles grâce à leurs empreintes génétiques, le FNAEG concerne aujourd'hui la quasi-totalité des crimes et délits d'atteinte aux biens et aux personnes ainsi que les trafics. Le FNAEG concerne aussi des personnes disparues, ainsi qu'avec leur accord, des ascendants ou descendants de ces personnes.
Le FNAEG contient environ 40 000 profils dont 24 000 condamnés, 13 000 suspects, 2 400 traces non identifiées relevées sur des scènes de crimes.
Les données sont conservées quarante ans pour les personnes définitivement condamnées et vingt-cinq ans pour les personnes mises en cause.

Il faut souligner pour finir qu'une proposition de loi sur le traitement de la récidive, récemment adoptée en première lecture par l'Assemblée nationale, prévoit l'inscription automatique au FIJAIS des décisions de non-lieu, de relaxe ou d'acquittement justifiées par l'irresponsabilité pénale de l'auteur de l'infraction concernée, alors que l'automaticité de cette inscription ne concerne aujourd'hui que les décisions relatives à une infraction passible d'une peine de prison supérieure ou égale à cinq ans.

Le traitement de la récidive

Dans le prolongement du rapport que la mission parlementaire d'information sur le traitement de la récidive des infractions pénales a rendu public le 7 juillet 2004, une proposition de loi reprenant les seules mesures préconisées qui impliquent des modifications législatives a été déposée le 1er décembre à l'Assemblée nationale et adoptée par celle-ci en première lecture.

L'une des ces dispositions prévoit notamment la possibilité de placer sous **surveillance électronique mobile** les personnes condamnées pour crimes et délits sexuels. Le dispositif envisagé est différent de celui déjà prévu par les **articles 138 et 723-7 à 723-14 du Code de procédure pénale**, qui peut être comparé à une « assignation à résidence électronique ».

Tout d'abord, il s'agit ici d'un dispositif mobile, « *dont le but est de s'assurer, en cas de besoin, de la localisation géographique du condamné libre par l'intermédiaire de la technique du GPS* » alors que le placement sous surveillance électronique « fixe » existant permet seulement de s'assurer de la présence de la personne porteuse du bracelet émetteur dans un périmètre restreint autour du récepteur.

Ensuite, et alors que le placement sous surveillance électronique fixe est conçu comme une alternative à l'emprisonnement (il concerne les personnes mises en examen, les personnes condamnées à une peine de prison inférieure à un an ou celles dont le reliquat de peine de prison est inférieur à un an), le dispositif mobile projeté, envisagé ici comme une mesure de sûreté, concernerait des condamnés ayant purgé leur peine.

Il convient évidemment d'apprécier ces deux aspects de ce dispositif au regard de la durée maximale de cette mesure de sûreté, soit « *vingt ans en matière correctionnelle et trente ans en matière criminelle* ».

Cette proposition de loi, de façon générale, et ce dispositif de placement sous surveillance électronique mobile, en particulier, ont suscité des réserves et des critiques de la part des parlementaires, à tel point que le ministre de la Justice a chargé Georges Fenech, député du Rhône, d'une mission d'étude approfondie « *du placement sous surveillance électronique mobile des détenus les plus dangereux* ».

La CNIL n'a pas été consultée sur cette proposition. Or, sans méconnaître aucunement la nécessité d'assurer un suivi notamment sociojudiciaire des délinquants sexuels susceptibles de présenter des risques de récidive, l'instauration d'un tel dispositif de surveillance électronique ne peut que susciter, en particulier au regard des principes de protection des données, des interrogations de fond.

Ces interrogations tiennent tout d'abord à la pertinence même du dispositif au regard des objectifs recherchés, la prévention de la récidive et la réinsertion des condamnés. Localiser à distance une personne dangereuse pour quoi faire ? Intervenir avant le passage à l'acte ? Identifier plus facilement et plus rapidement le coupable d'un crime ou d'un délit sexuel ? Et de ce fait dissuader une partie de ces récidivistes potentiels de passer à l'acte ? Le texte de l'Assemblé nationale qui prévoit seulement à titre d'option, l'interdiction d'accès à certains lieux, n'apporte pas de réponse claire à ces questions.

Dernière minute !

Lors de l'examen de la proposition de loi en première lecture, le 9 février 2005, le Sénat a décidé de supprimer les dispositions relatives à la surveillance électronique.

Au-delà, et encore une fois tout en prenant en compte les impératifs de sécurité en ce domaine, il convient aussi de réfléchir sur les implications en termes de libertés individuelles, de respect de la dignité humaine et de la vie privée que comporterait un tel dispositif de traçage et ce alors même que le texte de cette proposition de loi est muet sur les catégories de personnels qui auraient accès aux données de localisation des personnes concernées, cette question étant évidemment d'une grande importance au regard des enjeux en termes de liberté.

LE PEER TO PEER

Le *peer to peer* a été considéré comme un facteur du développement des contrefaçons sur l'internet et est accusé d'ébranler l'économie de l'industrie musicale et cinématographique. C'est dans ce contexte qu'une nouvelle disposition a été insérée dans la loi « Informatique et Libertés » par **la loi du 6 août 2004**. Il s'agit de **l'article 9 4°** qui donne la possibilité à certains organismes[15] représentant les auteurs, artistes et producteurs, de mettre en œuvre des traitements portant sur des données relatives à des infractions. Dans sa **décision du 29 juillet 2004**, le Conseil constitutionnel en validant cette disposition a indiqué que la mission de la CNIL sera de s'assurer que les garanties de nature à préserver l'équilibre entre le respect de la vie privée et la protection des droits de propriété intellectuelle sont assurées.

Les traitements qui seront mis en œuvre en application de cet article sont de deux natures et seront subordonnés à l'autorisation de la CNIL :

– **les traitements ayant pour finalité la constatation des infractions** : ils visent à recenser les actes de contrefaçon sur internet. Il s'agit d'utiliser des logiciels permettant de relever les adresses IP des internautes et d'identifier la nature des œuvres qu'ils mettent à disposition. L'objectif est de réunir des preuves en vue d'engager de poursuites pénales ou civiles ;

– **les traitements ayant pour finalité la prévention** : il s'agit d'adresser aux internautes concernés des messages de prévention sur les conséquences économiques de la contrefaçon, ainsi que sur les sanctions encourues.

15. Il s'agit des personnes morales mentionnées aux articles :
- L. 321-1 du Code de la propriété intellectuelle : les sociétés de perception et de répartition des droits d'auteur, des droits des artistes interprètes et des droits des producteurs de phonogrammes et de vidéogrammes constituées sous forme de sociétés civiles : la Société des auteurs compositeurs et éditeurs de musique (SACEM).
- L. 331-1 du Code de la propriété intellectuelle, à savoir : Les organismes de défense professionnelle régulièrement constitués, cette catégorie comprend des syndicats, des associations ou des sociétés de toute nature : l'Association de lutte contre la piraterie audiovisuelle (ALPA).

Qu'est-ce que c'est ?

Le peer to peer

Le terme *peer to peer* « pair à pair » désigne des protocoles de communication permettant notamment, aux internautes d'échanger gratuitement des œuvres musicales ou des films sur l'internet. Aujourd'hui, ces échanges s'effectuent d'internaute à internaute, via un logiciel offrant la possibilité à deux ordinateurs reliés à l'internet de communiquer directement l'un avec l'autre sans passer par un serveur central, on parle d'architecture peer to peer décentralisée.

La CNIL et ...

Le peer to peer

La CNIL veillera notamment à ce que l'identification des internautes *via* leur adresse IP ne s'effectue que dans le cadre d'une procédure judiciaire. Cette identification nécessite d'interroger le fournisseur d'accès à internet qui attribue à la machine de l'internaute un numéro d'identification (l'adresse IP) et détient les informations nominatives fournies par l'internaute lors de son abonnement. Par ailleurs, les traitements envisagés devraient avoir pour objectif de sanctionner les délits d'habitude. Dès lors, des critères tels que le nombre de récidives ou la quantité d'œuvres de l'esprit mis à disposition devraient être pris en considération. La CNIL sera attentive à la durée de conservation des informations recueillies.

LA VIDÉOSURVEILLANCE DANS LES LIEUX PRIVÉS

M É M O

La CNIL n'est pas compétente sur la vidéosurveillance dans les lieux publics. Mais la vidéosurveillance gagne le terrain de l'entreprise, de l'établissement scolaire et des résidences collectives.

Le point sur...

La vidéosurveillance

Hubert BOUCHET

Membre du Conseil économique et social
Commissaire en charge du secteur « Travail »

Où en est le développement de la vidéosurveillance en France ?

Que ce soit au coin de la rue, dans les gares, dans les couloirs du métro, sur les autoroutes, les parkings, les halls d'immeubles, les magasins ou encore au bureau, les caméras fleurissent. Leurs fonctionnalités sont de plus en plus sophistiquées et leur capacité de mémoire de plus en plus importante.

Quelles sont aujourd'hui les règles qui encadrent ces dispositifs ?

La vidéosurveillance installée sur la voie publique et dans les lieux ou établissements ouverts au public est réglementée par la loi du 21 janvier 1995[1], qui prévoit que ces dispositifs ne peuvent être mis en place dans les lieux publics que pour des finalités précises : protection des bâtiments et installations publics et de leurs abords, installations utiles à la défense nationale, régulation du trafic routier, constatation des infractions aux règles de la circulation et prévention des atteintes à la sécurité des personnes et des biens, y compris dans les lieux et établissements ouverts au public exposés à des risques d'agression ou de vol.

L'installation de tels dispositifs n'est possible qu'après une autorisation du préfet, prise après l'avis d'une commission départementale, présidée par un magistrat de l'ordre judiciaire.

La CNIL n'est donc pas compétente ?

La loi de 1995 a été modifiée par celle du 6 août 2004 qui réforme la loi « Informatique et Libertés ». Le nouveau texte dispose désormais que les enregistrements visuels réalisés grâce à un système de vidéosurveillance publique « qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques » sont soumis à la loi « Informatique et Libertés »[2].

Il prévoit également la remise par le Gouvernement d'un rapport annuel d'activité des commissions départementales à la CNIL. Ce changement bienvenu devrait permettre de renforcer les garanties prévues par la loi de 1995 et d'apporter une meilleure transparence sur l'état des systèmes de vidéosurveillance en France.

Qu'en est-il des systèmes de vidéosurveillance numérique installés dans des lieux privés ?

Ces systèmes sont soumis à la déclaration préalable prévue par la loi « Informatique et Libertés » de 1978 modifiée en 2004.

1 Loi n°95-73 du 21 janvier 1995 de programmation relative à la sécurité, complétée par le décret n°96-926 du 17 octobre 1996, ainsi que la circulaire du 22 octobre 1996 (*JO* du 7 décembre 1996).

2 *Cf.* l'article 10 de la loi du 21 janvier 1995 du 21 janvier 1995 modifiée par l'article 15 de la loi n°2004-801 du 6 août 2004.

La CNIL rappelle

Appliquant les critères qu'elle a dégagés [1], la CNIL considère qu'un système de vidéosurveillance mis en place dans un lieu public ou dans un lieu privé « ouvert au public », soit lorsqu'il utilise un procédé de reconnaissance des visages à des fins d'identification, soit lorsqu'il comporte l'existence d'une possibilité de rapprochement avec d'autres enregistrements d'informations nominatives, relève de la loi « Informatique et Libertés ». Mais neuf ans après la publication du rapport Voix, image et protection des données personnelles [2], la CNIL souhaite poursuivre en 2005 sa réflexion, en se rapprochant en particulier des différents acteurs en ce domaine (notamment le ministère de l'Intérieur, les fabricants et les prestataires) et en développant une veille technologique en ce domaine. Elle entend ainsi suivre avec une particulière attention l'émergence de nouvelles fonctionnalités techniques telles que la détection automatique de comportements anormaux (ex. : mouvements de foule) ou les procédés informatiques de reconnaissance faciale qui appellent un contrôle étroit. De tels systèmes doivent en effet être considérés comme des traitements automatisés de données biométriques au sens de la loi « Informatique et Libertés » modifiée. Ils relèvent dès lors de la procédure d'autorisation ou de la procédure de demande d'avis [3].

1. *Cf.* 24e Rapport annuel d'activité pour 2003, p. 128.
2. La documentation française – avril 1996.
3. *Cf.* articles 25 et 27 de la loi de 1978 modifiée en 2004.

LES PRINCIPAUX DÉCRETS D'APPLICATION DEVANT ÊTRE SOUMIS POUR AVIS À LA CNIL EN 2005

Décrets d'application de la loi relative à l'assurance maladie :

◆ Conservation et transmission électronique des informations médicales par les professionnels de santé.

◆ Conditions de mise en œuvre du Dossier médical personnel (DMP).

◆ Utilisation d'un identifiant pour l'ouverture et la tenue du dossier médical personnel.

◆ Consultation par les médecins des données détenues par les organismes d'assurance maladie.

◆ Conditions de mise en œuvre du volet d'urgence de la carte Vitale.

Loi relative à la politique de santé publique :

◆ Modalités de transmission et destinataires du certificat précisant les causes du décès des personnes.

Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel :

◆ Modalités d'application de la loi du 6 janvier 1978.

Loi pour la confiance dans l'économie numérique :

◆ Conservation par les prestataires techniques des données permettant l'identification des auteurs de contenus en ligne.

Loi portant adaptation de la justice aux évolutions de la criminalité :

◆ Fichier judiciaire national automatisé des auteurs d'infractions sexuelles.

Loi relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité :

◆ Traitement automatisé des demandes de validation des attestations d'accueil par les maires.

◆ Collecte et conservation des empreintes digitales des ressortissants étrangers pris en situation irrégulière ou sollicitant un titre de séjour en France.

Loi portant réforme des retraites :

◆ Utilisation du NIR par les organismes de retraite pour une mutualisation des informations sur les droits des assurés.

Loi pour la sécurité intérieure :

◆ Mise en œuvre par les services de la police et de la gendarmerie nationales de traitements concernant les crimes et délits (deux décrets : STIC et JUDEX).

◆ Accès des officiers de police judiciaire aux informations contenues dans les systèmes informatiques des organismes publics ou privés.

Loi relative à la sécurité quotidienne :

◆ Conservation par les opérateurs de télécommunications des données techniques de communication.

◆ Fichier national automatisé des personnes interdites d'acquisition et de détention d'armes.

PROPOSITIONS ET RECOMMANDATIONS DE LA CNIL

AU GOUVERNEMENT ET AU PARLEMENT

LES FICHIERS DE POLICE JUDICIAIRE

Mieux encadrer l'utilisation des fichiers de police judiciaire à des fins administratives

La consultation des fichiers de police judiciaire, à des fins d'enquête administrative, dans le cadre en particulier des procédures d'embauche et d'accès aux emplois touchant aux activités de surveillance et de gardiennage, désormais consacrée par **les lois du 15 novembre 2001 et du 18 mars 2003**, leur fait jouer, de fait, aujourd'hui le rôle d'un casier judiciaire parallèle, alors même qu'ils ne bénéficient pas, pour leur alimentation, l'effacement et la consultation des données, des garanties extrêmement rigoureuses prévues pour le casier judiciaire national.

Il apparaît aujourd'hui, au vu des constatations effectuées par la CNIL, notamment dans le cadre de l'exercice du droit d'accès indirect, que les dérives sont bien réelles, comme en témoignent les quelques exemples évoqués dans ce rapport annuel.

Malgré les consignes qui ont pu être données, trop souvent l'enquête administrative se limite à la seule consultation de ces fichiers, sans examen plus approfondi de la situation administrative de l'intéressé et cette consultation est considérée dans la plupart des cas comme un élément essentiel et probant de l'enquête conditionnant la décision d'embauche.

Il est primordial que ces fichiers soient fiables et qu'une mise à jour rigoureuse et systématique soit assurée. Or la mise à jour régulière et systématique des fichiers de police judiciaire qui devrait être réalisée, en particulier par la transmission des décisions de relaxe, d'acquittement, de non-lieu ou de classement sans suite pour insuffisance de charges, n'est pas pleinement effective aujourd'hui. Actuellement la communication des informations s'effectue principalement au moyen de fiches papier selon une périodicité variable en fonction de la taille des parquets. Les liaisons informatiques sécurisées qui devaient être mises en place entre les 181 parquets et le ministère de l'Intérieur ou la Gendarmerie nationale ne le sont toujours pas.

Il importe d'accélérer la réalisation de ces liaisons informatiques.

Au-delà, une réflexion devrait être menée sur le rôle du casier judiciaire et sur ses modalités actuelles de fonctionnement et en particulier de mise à jour.

Simplifier et accélérer l'accès aux fichiers de police judiciaire

Compte tenu de l'ampleur que prend l'exercice du droit d'accès indirect, de la nécessité pour la CNIL d'apporter au citoyen une réponse rapide et satisfaisante, il apparaît impératif de rechercher avec l'ensemble des partenaires institutionnels concernés des modes d'intervention et de collaboration plus efficaces qui permettent tout à la fois une simplification et une accélération des procédures.

La CNIL est confrontée à un nombre croissant de demandes résultant de refus d'embauche ou de licenciements prononcés à la suite de la consultation des fichiers de police judiciaire.

Il apparaît donc indispensable que les pouvoirs publics mettent en œuvre les moyens appropriés pour :

– d'une part permettre une instruction accélérée des saisines de façon à ce que les requérants puissent obtenir une réponse dans les meilleurs délais, en particulier en simplifiant les procédures de saisine du ministère de l'Intérieur (par exemple pour obtenir l'autorisation d'informer une personne que son signalement a été supprimé) ;

– d'autre part assurer enfin, de manière effective, la communication aux intéressés des informations les concernant dès lors que le principe de cette communication a été accepté par le ministère de l'intérieur comme le prévoit désormais **l'article 41 de la nouvelle loi « Informatique et Libertés »**. La Commission a fait part au ministère de l'Intérieur de propositions concrètes en ce sens.

Au-delà, dans le souci d'une plus grande transparence, ne conviendrait-il pas d'envisager certaines évolutions, comme le permet désormais l'article 41 de la nouvelle loi « Informatique et Libertés » et par exemple, reconnaître aux victimes un droit d'accès direct aux informations les concernant dans les fichiers de police judiciaire ?

LE FICHIER CENTRAL DES CHÈQUES

Modifier le régime de centralisation des retraits de carte bancaire dans le fichier central des chèques

Le traitement dénommé « centralisation des retraits de cartes bancaires » a été créé par un **arrêté du conseil général de la Banque de France du 16 juillet 1987**. Il est inclus dans le **Fichier central des chèques (FCC).**

Les règles de fonctionnement de ce fichier ont donc été commandées, lors de sa création, par la crainte des fraudes. Ainsi, les informations relatives à la décision de retrait de carte bancaire sont conservées dans le fichier pendant une période de deux ans à partir de la date de la décision. La levée de l'inscription au fichier avant l'expiration de ce délai de deux ans est à l'entière discrétion de l'établissement qui a procédé au retrait, que les incidents de fonctionnement du compte bancaire qui ont pu justifier ce retrait aient été régularisés ou non.

À l'époque, il avait été argumenté par le groupement des cartes bancaires que l'octroi d'une carte bancaire est régi par le principe de la liberté contractuelle, qui résulte de **l'article 1101 du Code civil**, qui permet à l'établissement bancaire de refuser ou d'accorder une carte de crédit à ses clients. Les modalités de retrait d'une carte bancaire accordée à un client figurent en outre dans les clauses contractuelles que le client signe librement avec son établissement bancaire (*cf.* contrat porteur carte bancaire).

Aujourd'hui, force est de constater que le contexte sociologique et juridique de l'utilisation des cartes bancaires a profondément changé. En effet, les transactions par carte bancaire dépassent désormais celles réalisées par chèque. La sécurisation des cartes bancaires a en outre fait ses preuves. Enfin, chaque établissement bancaire peut prendre des mesures propres pour limiter l'utilisation d'une carte par l'un de ses clients.

L'instruction des réclamations adressées à la CNIL, de plus en plus nombreuses sur ce sujet, montre que les établissements bancaires font aujourd'hui un usage quelque peu détourné du fichier de centralisation des retraits de carte bancaire.

Ainsi, au moindre incident de fonctionnement du compte bancaire (que celui-ci corresponde à un réel incident ou qu'il résulte d'un litige), certains établissements bancaires inscrivent leur client au FCC pour un retrait de leur carte bancaire, et le laisse fiché pendant deux ans. Parfois, cette inscription intervient alors que le client a quitté la banque, à la suite d'un litige. Il se trouve alors dans l'impossibilité d'obtenir l'ouverture d'un compte dans une autre banque, du fait de ce fichage.

Le client tente souvent, à maintes reprises, d'obtenir la mainlevée de cette inscription sans succès, bien souvent alors même qu'il a régularisé la situation de son compte. Seule l'intervention de la CNIL permet d'obtenir ce défichage. Le fichier de centralisation des retraits de carte bancaire devient ainsi parfois, pour certains établissements, une arme pour « faire pression » sur leurs clients.

Une telle situation n'est pas juridiquement satisfaisante. En effet, ce traitement, qui ne repose sur aucun fondement législatif, prévoit moins de garantie que les autres fichiers centraux gérés par la Banque de France et qui eux trouvent leur fondement dans la loi : le Fichier national des incidents de remboursement des crédits aux particuliers (FICP) et le Fichier central des chèques (FCC).

La CNIL estime que l'arrêté du conseil général de la Banque de France réglementant la centralisation des retraits de carte bancaire devrait être modifié afin de prévoir, à tout le moins, deux mesures complémentaires de nature à assurer le respect des droits des personnes fichées :

– une information préalable individualisée, avant l'inscription au fichier ou au moment de cette inscription ;

– une obligation, pour l'établissement bancaire qui a procédé à l'inscription, de la levée dès que les incidents de fonctionnement du compte bancaire qui ont pu justifier ce retrait ont été régularisés.

Annexe

LISTE DES DÉLIBÉRATIONS ADOPTÉES PAR LA CNIL EN 2004

Numéro Date	Objet
04-001 3 février 2004	Délibération portant élection du président de la Commission nationale de l'informatique et des libertés
04-002 3 février 2004	Délibération portant délégation d'attribution au président de la Commission nationale de l'informatique et des libertés
04-003 3 février 2004	Délibération portant désignation des membres de la Commission nationale de l'informatique et des libertés, chargés d'exercer le droit d'accès indirect en application de l'article 39 de la loi du 6 janvier 1978
04-004 19 février 2004	Délibération relative au projet de décret modifiant le Titre II du décret n° 98-247 du 2 avril 1998 relatif à la qualification artisanale et au répertoire des métiers
04-005 26 février 2004	Délibération portant élection du vice-président de la Commission nationale de l'informatique et des libertés
04-006 4 mars 2004	Délibération relative à une demande d'avis présentée par l'université Joseph-Fourer de Grenoble concernant la mise en place par le laboratoire de génétique d'une base de données génétiques anonymisées accessible sur internet
04-007 25 mars 2004	Délibération portant avertissement à FINAREF
04-008 25 mars 2004	Délibération portant avertissement à la Compagnie générale de location d'équipement
04-009 25 mars 2004	Délibération portant avertissement à la Banque Populaire Loire et Lyonnais
04-010 25 mars 2004	Délibération portant avis sur un projet de décret relatif à la mise en œuvre d'un fichier des personnes habilitées à procéder au démarchage bancaire ou financier
04-011 à 04-01630 mars 2004	Six délibérations décidant une mission de contrôle
04-017 8 avril 2004	Délibération relative à une demande d'avis de l'établissement public Aéroports de Paris concernant la mise en œuvre d'un contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy
04-018 8 avril 2004	Délibération relative à une demande d'avis présentée par le Centre hospitalier de Hyères concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels
04-019 8 avril 2004	Délibération décidant une mission de contrôle
04-020 8 avril 2004	Délibération portant avis sur un traitement de la Régie autonome des transports parisiens ayant pour finalité l'exploitation des données de validation des passes Navigo
04-021 8 avril 2004	Délibération portant avis favorable à la mise en œuvre par la société Transpole d'un dispositif relatif à la gestion des infractions à la police des services publics de transports terrestres
04-022 8 avril 2004	Délibération portant modification des articles 18 et 22 du règlement intérieur de la Commission
04-023 à 04-032 14 avril 2004	Onze délibérations décidant une mission de contrôle

Numéro Date	Objet
04-033 27 avril 2004	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978
04-034 27 avril 2004	Délibération décidant une mission de contrôle
04-035 27 avril 2004	Délibération relative à une demande d'avis présentée par le ministère de l'Emploi, du Travail et de la Cohésion sociale concernant la mise en œuvre d'un fichier national de suivi du dispositif de cessation d'activité de travailleurs salariés et à un projet de décret en Conseil d'État autorisant l'utilisation du numéro de Sécurité sociale dans le cadre de ce dispositif
04-036 à 04-040 13 mai 2004	Cinq délibérations décidant une mission de contrôle
04-041 27 mai 2004	Délibération concernant un projet de décret en Conseil d'État relatif aux conditions d'agrément des hébergeurs de données de santé à caractère personnel
04-042 à 04-047 03 juin 2004	Six délibérations décidant une mission de contrôle
04-048 03 juin 2004	Délibération portant avertissement à la Caisse de Crédit Mutuel de Charente-Maritime (Deux-Sèvres)
04-049 03 juin 2004	Délibération portant avertissement à la Caisse de crédit mutuel du Dauphiné
04-050 03 juin 2004	Délibération portant avertissement à la Banque française et commerciale d'Antilles-Guyanne (BFCAG)
04-051 03 juin 2004	Délibération portant avertissement à la Caisse d'épargne des Alpes
04-052 10 juin 2004	Délibération portant avis sur un traitement automatisé d'informations nominatives de la Société des autoroutes Paris-Rhin-Rhône ayant pour finalité la réalisation d'une étude expérimentale de fiabilité d'un système de télépéage automatique
04-053 10 juin 2004	Délibération portant avis sur un projet de décret en Conseil d'État encadrant les rapprochements de données personnelles relatifs aux salariés intermittents du spectacle et à leurs employeurs prévus à l'article L. 351-21, 5e alinéa, du Code du travail
04-054 10 juin 2004	Délibération portant avis sur le projet de loi relatif à la réforme de l'assurance maladie
04-055 24 juin 2004	Délibération portant avis sur la création par Électricité de France d'un système d'information pour la gestion des relations techniques avec les clients non résidentiels dénommé SI NR DEGS (DISCO NR)
04-056 24 juin 2004	Délibération portant avis sur la création par Gaz de France d'un système d'information pour la gestion des relations techniques avec les clients non résidentiels dénommé SI NR DEGS (DISCO NR)
04-057 24 juin 2004	Délibération portant avis sur : – un projet de décret en Conseil d'État autorisant l'Institut de radioprotection et de sûreté nucléaire (IRSN) à utiliser le répertoire national d'identification des personnes physiques dans un traitement automatisé d'informations nominatives, relatif à la surveillance des travailleurs exposés aux rayonnements ionisants ; – un projet d'acte réglementaire portant mise en œuvre au sein de l'IRSN du traitement automatisé d'informations nominatives ayant pour finalité la surveillance de l'exposition aux rayonnements ionisants de certaines personnes exposées ; – un projet d'arrêté relatif à la carte de suivi médical et aux informations individuelles de dosimétrie
04-058 01 juillet 2004	Délibération portant avis sur un projet de décret en Conseil d'État pris en application de l'article L. 1221-6-1 du Code de l'action sociale et des familles et fixant les modalités de recueil, de transmission et d'utilisation des données nominatives relatives aux personnes âgées et aux personnes handicapées bénéficiaires du plan d'alerte et d'urgence départementale en cas de risques exceptionnels

Numéro Date	Objet
04-059 01 juillet 2004	Délibération portant avis sur la demande d'avis présentée par la CNAMTS concernant la gestion individualisée des bénéficiaires de l'assurance maladie et dénommée « Rénovation – référentiel individu »
04-060 à 04-066 01 juillet 2004	Sept délibérations décidant une mission de contrôle
04-067 24 juin 2004	Délibération concernant les traitements automatisés d'informations nominatives mis en œuvre par les communes pour la gestion de l'état civil
04-068 24 juin 2004	Délibération portant avis sur le projet de décret du ministre de l'Intérieur modifiant le décret du 8 avril 1987 relatif au fichier automatisé des empreintes digitales
04-069 01 juillet 2004	Délibération portant avis sur un projet de décret relatif aux conseillers en investissements financiers
04-070 09 septembre 2004	Délibération portant délégation d'attribution au président de la Commission nationale de l'informatique et des libertés
04-071 09 septembre 2004	Délibération portant délégation d'attributions au bureau de la Commission nationale de l'informatique et des libertés
04-072 21 septembre 2004	Délibération portant autorisation par la Commission de la mise en œuvre du traitement prévention des impayés par la GIE Preventel
04-073 21 septembre 2004	Délibération relative à une demande d'avis portant sur la mise en œuvre d'un système de vote électronique à distance pour l'élection des membres des chambres de commerce et d'industrie
04-074 21 septembre 2004	Délibération portant adoption d'une norme simplifiée concernant les traitements automatisés de données personnelles mis en œuvre par les communes aux fins de consultation de données issues de la matrice cadastrale
04-075 05 octobre 2004	Délibération portant avis sur le projet de décret en Conseil d'État pris pour l'application de l'article 8-4 de l'ordonnance du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France et portant création à titre expérimental d'un traitement automatisé de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa
04-076 05 octobre 2004	Délibération portant avis sur un projet d'arrêté interministériel portant création d'un dispositif dénommé système « contrôle automatisé » visant à automatiser la constatation, la gestion et la répression de certaines infractions routières
04-077 05 octobre 2004	Délibération portant élection du vice-président et désignation du vice-président délégué de la Commission nationale de l'informatique et des libertés
04-078 05 octobre 2004	Délibération portant délégation d'attributions au vice-président délégué de la Commission nationale de l'informatique et des libertés
04-079 05 octobre 2004	Délibération portant autorisation de l'enquête « Handicaps-incapacité-dépendance à la Réunion » réalisée par l'INSEE
04-080 05 octobre 2004	Délibération portant autorisation d'une enquête de la Direction de la recherche, des études, de l'évaluation et des statistiques du ministère de la Santé relative aux recours urgents ou non programmées en médecine générale
2004-081 09 novembre 2004	Délibération portant autorisation d'une expérimentation présentée par la Fédération nationale de la mutualité française ayant pour finalité d'accéder, sous forme anonymisée, aux données de santé figurant sur les feuilles de soins électroniques
2004-082 09 novembre 2004	Délibération portant autorisation de la mise en œuvre par la RATP d'un traitement de données à caractère personnel relatif aux infractions à la police des services publics de transports terrestres
2004-083 04 novembre 2004	Délibération portant adoption d'une norme simplifiée concernant certains traitements automatisés mis en œuvre par les communes et les établissements publics de coopération intercommunale à partir des rôles des impôts directs locaux

Numéro Date	Objet
2004-084 04 novembre 2004	Délibération portant avis sur le traitement « Hélios » de gestion comptable, financière et budgétaire des collectivités locales et établissements publics locaux mis en œuvre par la Direction générale de la comptabilité publique
2004-085 09 novembre 2004	Délibération du bureau de la Commission nationale de l'informatique et des libertés portant habilitation de certains agents de la CNIL pour procéder à des vérifications
2004-086 09 novembre 2004	Délibération portant autorisation de la mise en œuvre par la société DIAC Location d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre portant création du système de contrôle automatisé
2004-087 04 novembre 2004	Délibération portant modification de l'article 13 du règlement intérieur de la Commission nationale de l'informatique et des libertés
2004-088 18 novembre 2004	Délibération portant modification des articles 55 à 62 du règlement intérieur de la Commission nationale de l'informatique et des libertés
2004-089 18 novembre 2004	Délibération portant autorisation d'un traitement de données à caractère personnel dans le cadre de la mise en œuvre du dispositif de tarification spéciale de l'électricité comme produit de première nécessité
2004-090 18 novembre 2004	Délibération portant autorisation d'un traitement présenté par la clinique générale du sport ayant pour finalité la gestion de l'information des patients opérés du genou dans cet établissement et exposés au risque infectieux à mycobactérie entre le 1er janvier 1988 et le 31 décembre 1993 et permettant la consultation du répertoire national interrégime des bénéficiaires de l'assurance maladie
2004-091 18 novembre 2004	Délibération portant avis sur la création par la direction générale des impôts du traitement « SIRIUS-FP » d'aide à la sélection et au contrôle des dossiers fiscaux des particuliers
2004-092 18 novembre 2004	Délibération portant élection de trois membres de la formation restreinte de la Commission nationale de l'informatique et des libertés
2004-093 02 décembre 2004	Délibération relative à une demande d'avis portant sur la mise en œuvre des représentants des usagers aux conseils des établissements publics à caractère scientifique, culturel et professionnel
2004-094 02 décembre 2004	Délibération portant autorisation de la mise en œuvre par la Banque de France d'une expérimentation concernant le comptage du nombre de chèques consultés sur un compte dans le cadre de la consultation du Fichier national des chèques irréguliers (FNCI)
2004-095 09 décembre 2004	Délibération portant autorisation d'un traitement automatisé de données à caractère personnel présenté par le vice-président du Conseil d'État et concernant la gestion des activités contentieuses du Conseil d'État, des cours administratives d'appel et des tribunaux administratifs
2004-096 09 décembre 2004	Délibération décidant la dispense de déclaration des traitements de gestion des rémunérations mis en œuvre par l'État, les collectivités locales, les établissements publics et les personnes morales de droit privé gérant un service public
2004-097 09 décembre 2004	Délibération décidant la dispense de déclaration des traitements de gestion des rémunérations mis en œuvre par les personnes morales de droit privé autres que celles gérant un service public
2004-098 09 décembre 2004	Délibération portant modification des articles 54 et 63 du règlement intérieur de la Commission nationale de l'informatique et des libertés insérant dans le chapitre III de ce règlement une section 5 nouvelle intitulée « Règles relatives à l'application des articles 45 et 46 de la loi du 6 janvier 1978 »
2004-099 09 décembre 2004	Délibération portant avis sur le projet de décret présenté par l'INSEE modifiant le décret n°82-103 du 22 janvier 1982 modifié relatif au répertoire national d'identification des personnes physiques et portant extension à l'outre-mer de l'identification au répertoire
2004-100 09 décembre 2004	Délibération portant autorisation de la mise en œuvre par la SNCF d'un traitement automatisé de données à caractère personnel relatif à la gestion des données de validation des passes « Navigo » chargés d'un abonnement annuel, mensuel ou hebdomadaire
2004-101 09 décembre 2004	Délibération portant autorisation d'un transfert de données à caractère personnel vers le Maroc à l'occasion d'un contrat de sous-traitance entre le GIE Comutitres et la société FEDASO *via* la société EXPERIAN

Numéro Date	Objet
2004-102 14 décembre 2004	Délibération portant avis sur un projet de décret modifiant le décret n°2003-752 relatif aux annuaires universels et aux services universels de renseignements et le Code des postes et des télécommunications électronique
2004-103 14 décembre 2004	Délibération portant avis sur le projet d'arrêté présenté par l'INSEE modifiant l'arrêté du 27 juillet 2004 créant un traitement automatisé réalisé à l'occasion du recensement général de la population en Nouvelle-Calédonie
2004-104 14 décembre 2004	Délibération portant avis sur le projet d'arrêté relatif à un traitement permettant l'utilisation par les agents de l'inspection du travail et des services de contrôle de la recherche d'emploi du ministère de l'Emploi, du Travail et de la Cohésion sociale des relevés mensuels de contrats de travail temporaire
2004-105 14 décembre 2004	Délibération portant autorisation unique de traitement de données à caractère personnel comportant un système d'information géographique mis en œuvre par les collectivités locales ou leurs groupements (cadastre et urbanisme)

Crédits photo :
© CNIL : p. 6, 14, 17, 23, 27, 29, 30, 43, 44, 54, 58, 61, 67, 70, 75, 85, 87, 91, 94, 98.
© Photo Christian Zachariasen (PhotoAlto) : p. 59, 63, 74, 75.
© Photo James Hardy (PhotoAlto) : p. 51, 98.
© Photo MAE / DCI - Labo4_2003 : p. 53, 97.
© Photo Goodshoot : p. 77.
© Photo Frédéric Cirou (PhotoAlto) : p. 93.