COMMISSION
NATIONALE DE
L'INFORMATIQUE
ET DES LIBERTÉS

26e RAPPORT D'ACTIVITÉ 2005

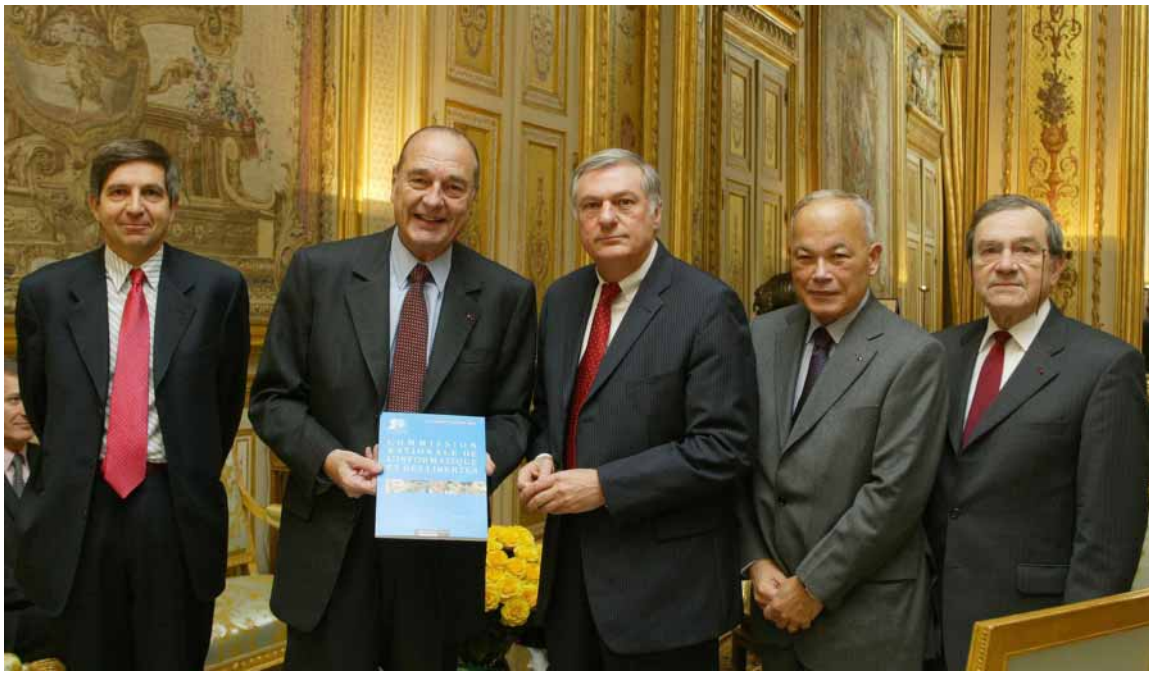
ISBN : 2-11-006058-1

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

26e RAPPORT D'ACTIVITÉ 2005

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

Sommaire



M. Alex Türk, président de la CNIL remet le rapport d'activité 2004 à M. Jacques Chirac, président de la République, accompagné de Guy Rosier, vice-président délégué, François Giquel, vice-président et Christophe Pallez, secrétaire général.

Avant-propos

L'année 2004 a été marquée par le vote de la nouvelle loi « informatique et libertés » mettant en application la directive européenne de 1995 et réformant en profondeur la loi fondamentale de 1978. Cette année aura donc été celle de la prise de conscience de la nouvelle donne juridique et de la mesure des défis qui nous attendaient.

L'année 2005 qui a vu paraître le décret d'application de la nouvelle loi a été, elle, celle de la mise en action.

• Mais, pour agir, il faut d'abord réunir des moyens. C'est pourquoi je me félicite que notre démarche auprès du Premier ministre tendant à renforcer très sensiblement l'effectif de notre commission pour faire face à de nouvelles missions, ait abouti, fin 2004, à un accord de principe mis en œuvre par le nouveau gouvernement dans le courant 2005.

C'est ainsi qu'il nous est possible de procéder à une partie du recrutement nécessaire, durant l'année 2006, pour engager les premières inflexions et les initiatives indispensables : par exemple, création d'un nouveau service d'accueil et d'orientation en prise directe avec l'usager, création d'une structure dédiée aux correspondants « informatique et libertés » en liaison constante avec les acteurs du monde informatique (entreprises, collectivités locales et administrations), développement du service des contrôles conformément à l'esprit même de la nouvelle loi.

Bien entendu, il ne s'agit là que de la première phase d'un plan de rattrapage qui devrait, en quatre ans, nous rapprocher de la moyenne européenne. À ce sujet, je me réjouis que le président de la République, lors de la présentation de notre rapport annuel 2004, ait manifesté son soutien ardent à ce plan et son intention de faire connaître cette préoccupation au Premier ministre.

• Pour agir, il faut également une méthode : nous avons choisi celle de la pédagogie, de la communication, du dialogue. Tel était le sens notamment de la refonte complète de notre rapport annuel qui a, je crois pouvoir le dire, rencontré un véritable succès. De même, nous avons engagé une vaste opération appelée « Les rencontres régionales de la CNIL » qui nous a amenés à nous rendre en région Nord-Pas-de-Calais en janvier, en Bretagne en avril, en Midi-Pyrénées en juin, en Franche-Comté en octobre, et enfin en Provence-Alpes-Côte d'Azur en décembre 2005.

Chaque fois notre équipe, composée de commissaires et de nombreux spécialistes de la commission, a pu échanger avec l'ensemble des acteurs « informatique et libertés » : magistrats, avocats, associations, consommateurs, syndicats, entreprises, professionnels de la recherche et de la santé, administrations, collectivités locales, milieux éducatifs, etc.

Ajoutons à ces initiatives, l'organisation d'un colloque extrêmement enrichissant, en novembre dernier, en collaboration avec le Sénat et l'université de Paris II, le développement de notre site internet ainsi qu'une multiplicité d'interventions en matière de formation.

• Pour agir, enfin et surtout, il faut un objectif ! Le nôtre n'a pas changé…mais il a beaucoup évolué !

La CNIL a toujours eu pour mission d'évaluer, conformément à la loi, au service de la société française, les données de l'équilibre fondamental entre les impératifs de progrès ou de la sécurité et ceux de la protection de la vie privée et des données personnelles.

Mais l'exercice est, chaque jour, plus périlleux car il ne s'agit pas de nous déterminer dans le présent seul. Il nous faut repérer, comprendre et exprimer des dérives qui peuvent survenir lors de la mise en œuvre de telle ou telle innovation dans les cinq ou dix ans à venir.

C'est en cela que notre objectif change parce qu'il évolue au gré des innovations techniques à une vitesse toujours plus grande, mais aussi parce que les enjeux sont toujours plus massifs et plus internationaux, mais encore parce que les usagers sont, comme consommateurs, de plus en plus avides des applications de ces nouvelles technologies de l'informatique et, comme citoyens, de plus en plus soucieux quant à la défense de leurs droits à la protection de leurs données personnelles.

Au fil des pages de cette deuxième édition du rapport annuel, « nouvelle formule », le lecteur découvrira l'écho ou le reflet de ces (ses) contradictions, de ces défis, de ces (ses) aspirations et il pourra prendre la mesure des actions que nous avons entreprises, en 2005, pour aider à la résolution des unes, à la maîtrise des autres, à la réalisation, enfin, de ces dernières.

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 chargée de prononcer des sanctions.

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)

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.

Jean-Marie COTTERET, professeur émérite des universités
Secteurs « Collectivités locales et 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.

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. Il siège à la Commission d'accès aux documents administratifs (CADA) en tant que personnalité qualifiée en matière de protection des données à caractère personnel.

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 la CNIL depuis août 2002.

Jean-Pierre de LONGEVIALLE, conseiller d'État honoraire
Secteur « Santé »
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, président-directeur général de Laser et de COFINOGA
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.

Jean MASSOT, président de section honoraire au Conseil d'État
Secteur « Finances publiques »
Jean Massot est membre de la CNIL depuis avril 2005[1]. Il siège à la Commission d'accès aux documents administratifs (CADA) en tant que personnalité qualifiée en matière de protection des données à caractère personnel.

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.

Commissaires du Gouvernement

Pascale COMPAGNIE[2]
Catherine POZZO DI BORGO, adjointe

---

1. En remplacement de M. François Bernard.
2. En remplacement de Mme Charlotte-Marie Pitrat, depuis le 18 octobre 2005.

LES SERVICES AU 31 DÉCEMBRE 2005

Président

Alex TÜRK

Secrétaire général

Christophe PALLEZ

SECRÉTARIAT DE LA PRÉSIDENCE
- Odile BOURRE, chef du secrétariat
- Évelyne LE CAM, Ghislaine MERTES

Conseiller du Président pour la prospective et le développement
- Marie GEORGES

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 documentation générale
- Solène BELEDIN

SERVICE DES AFFAIRES EUROPÉENNES ET INTERNATIONALES
- Chef de service
- N.
- Secteur privé
- Clarisse GIROT
- Secteur public
- Pascale RAULIN-SERRIER
- Assistance et secrétariat
- Marie LEROUX

COMMUNICATION
- Responsable
- Elsa TROCHET-MACÉ
- Brigitte BARBARANT, assistante communication

DIRECTION DES AFFAIRES JURIDIQUES
- Directeur : Sophie VULLIET-TAVERNIER
- Assistance de la Direction
- Audrey BACQUIÉ

DIVISION DES AFFAIRES ÉCONOMIQUES
- Chef de division
- Sophie NERBONNE
- Banque – Crédit Assurances
- Olivier COUTOR
- Nathalie METALLINOS
- Travail Affaires économiquess
- Laurent LIM
- Mathias MOULIN
- Télécommunications Commerce Affaires culturelles
- Thomas DAUTIEU
- Leslie BASSE
- Françoise PARGOUD
- Assistance et secrétariat
- Barbara BAVOIL
- Valérie GAUTIER
- Halima GOUASMIA
- Brigitte HUGER

CORRESPONDANTS
- Responsable Nathalie METALLINOS
- Hervé GUDIN

DIVISION DES AFFAIRES PUBLIQUES ET SOCIALES
- Chef de division
- Jeanne BOSSI
- Finances publiques Collectivité locales Libertés publiques
- Guillaume DELAFOSSE
- Olivier LESOBRE
- Justice – Sécurité Droits d'accès indirect
- Norbert FORT
- Bérengère MONEGIER DU SORBIER
- Santé – Affaires sociales
- Fatima HAMDI
- Daniéla PARROT
- Assistance juridique et secrétariat
- Valérie GAUTIER
- Catherine MANDINAUD
- Eugénie MARQUES
- Brigitte SAGOT
- Malika KHELLAF
- Bertrande PIAT-TAMBAREAU

SERVICE DES PLAINTES ET DES REQUÊTES GÉNÉRALES
- Chef de service
- Clémentine VOISARD
- Associations – Partis politiques – Internet – Banque – Fichiers centraux d'impayés
- Émilie PASSEMARD
- Michèle SAISI
- Travail-Social Sécurité sociale – Santé Éducation nationale Fiscal
- Caroline PARROT-FRANCIS
- Marketing – Sollicitations commerciales Assurances Télécommunications
- Xavier DELPORTE
- Assistance et secrétariat
- Anna BENISTI
- Véronique BREMOND
- Véronique JENNEQUIN
- Siré BARRY

GESTION DES SANCTIONS
- Responsable
- Guillaume DESGENS-PASANAU

DIRECTION DES AFFAIRES ADMINISTRATIVES
- Directeur : Thierry JARLET
- Adjoint : David TRIVIÉ
- Secrétariat de la direction
- Brigitte BARBARANT, chef du secrétariat

SERVICE DES RESSOURCES HUMAINES
- 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
- Responsable
- David TRIVIÉ
- Comptabilité
- Liliane RAMBERT, comptable
- Sébastien BOILEAU, gestionnaire

CELLULE LOGISTIQUE
- Responsable
- Pierre RIHOUAY
- Secrétariat voyages
- Véronique FOUILLET
- Huissiers
- Jérôme BROSSARD
- Mickaël MERI
- Conducteurs
- Alain HOUDIN
- Joël LEPAGE
- Patrick MAHOUDEAU
- Accueil et standard
- Marie-Christiane BENJAMIN
- Noëlle CHAUMETTE
- Entretien
- Félisa RODRIGUEZ

DIRECTION DE L'EXPERTISE ET DES CONTRÔLES
- Directeur : Roger NGÔ
- Secrétariat de la direction
- Nathalie JACQUES

EXPERTISE
- Yann LE HEGARAT, expert informaticien
- Jean-Luc BERNARD, expert informaticien

SERVICE DES CONTRÔLES
- Chef de service
- Florence FOURETS
- Michel GUEDRE, informaticien contrôleur
- Bernard LAUNOIS, informaticien contrôleur
- Jean-Paul MACKER, informaticien contrôleur

LES MOYENS

Le personnel

La CNIL dispose de quatre-vingts postes budgétaires en 2005 auxquels il faut ajouter un équivalent temps plein travaillé (ETP) pour un poste d'informaticien de haute technicité (IHT) et un (ETP) pour un vacataire. L'entrée en vigueur de la loi organique sur les lois de finances (LOLF) au 1er janvier 2006 a pour effet une comptabilisation systématique des effectifs en (ETP), plus précise et plus souple.

Les réformes organisationnelles et techniques ont permis un accroissement important de la productivité par agent. En 1995 la CNIL traitait 15 000 dossiers pour un effectif de 57 agents, soit 250 dossiers par agent. En 2005, 34 000 dossiers ont été traités par 85 agents soit 580 par agent.

Néanmoins, dans un rapport au Premier ministre de mars 2005, le président de la CNIL a présenté un programme de doublement de ses effectifs sur la période 2006-2009 afin de faire face à ses nouvelles missions. Au titre de 2006, dix emplois ont été obtenus, au lieu des vingt demandés qui, sans répondre totalement aux besoins de la CNIL, lui permettront notamment d'accroître ses actions de contrôle et d'information du public.

	2004		2005		2006		2004-2005	2005-2006
Catégories	«Poste LFI»	«ETP Budget»	«Poste LFI»	«ETP Budget»	Effectif	«ETP Budget»	«ETP Budget»	«ETP Budget»
A	48	49,6	50	50	56	53	0,8%	6,0%
B	18	17,4	18	18	22	20	3,4%	11,1%
C	16	15	17	17	17	17	13,3%	0,0%
Total	82	82	85	85	95	90	3,7%	5,9%

Le budget

Le budget 2005 augmente de 3,17% par rapport à 2004. Celui voté pour 2006 est en augmentation de 26,37% par rapport à 2005. Cela résulte en particulier de la forte hausse des dépenses d'immobilier en 2006 liée au regroupement, longtemps attendu, des services de la CNIL sur un site plus grand, facilitant l'accueil du public et des correspondants « informatique et libertés ». Après une forte progression des dépenses d'informatique sur la période 2001-2005 en raison du programme de rénovation de l'informatique centrale de la CNIL, ce poste marquera une pause au profit du projet immobilier.

En millions d'euros	2004	2005	2006	2004-2005	2005-2006
Budget total voté (LFI)	6,902	7,121	8,999	3,17%	26,37%
Budget délégué		7,315	8,812		20,46%
Dépenses de personnel	4,567	4,848	5,325	6,15%	9,84%
Dépenses de fonctionnement	2,335	2,467	3,487	5,65%	41,35%

Exécution du budget

	2004	2005	2006	2004-2005	2005-2006
Immobilier	0,933	0,934	2,023	0,08%	116,66%
Informatique	0,548	0,589	0,405	7,44%	-31,26%
Dépenses courantes	0,891	0,945	1,060	6,06%	12,12%
Total Fonctionnement	2,372	2,467	3,487	4,03%	41,33%

LES CHIFFRES CLÉS

Les délibérations de la CNIL

Au cours de l'année 2005, la CNIL a siégé 41 fois, au cours de 30 séances plénières, 8 formations restreintes et 3 bureaux délibératifs. Ces réunions ont conduit à l'adoption de 317 délibérations[3], soit un volume de décisions en augmentation de 200% par rapport à 2004.

Parmi les délibérations 2005, il convient de relever :

Au titre du conseil et de l'expertise

17 avis sur des projets de loi ou de décret, parmi lesquels l'avis sur le projet de loi relatif à la lutte contre le terrorisme, mais aussi celui sur le projet d'ordonnance relatif à la réutilisation des informations publiques et encore un avis sur la conservation des données de communications électroniques.

2 avis sur des règles professionnelles, à savoir sur le code de déontologie du Syndicat national de la communication directe relatif à la communication directe électronique, et sur le code de conduite présenté par l'Union française du marketing direct relatif à l'utilisation de coordonnées électroniques à des fins de prospection directe.

2 recommandations, l'une concernant l'archivage électronique, dans le secteur privé, de données à caractère personnel, l'autre encadrant la mise en œuvre par des particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle.

Au titre des sanctions

36 mises en demeure.

10 avertissements dans le secteur de la banque et du crédit.

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

Comment ça marche ?

Les délibérations

Les membres de la CNIL se réunissent en séance plénière environ trois 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. Parfois, c'est le bureau de la CNIL, constitué du président et des deux vice-présidents, qui adopte ces délibérations. Avant la modification de 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 CNIL, composée de six de ses membres. 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. Celle-ci 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.

Au titre de la simplification

5 normes simplifiées destinées à alléger les formalités déclaratives :
– des organismes publics et privés pour la gestion de leurs personnels ;
– des traitements de données personnelles liés à l'utilisation de services de téléphonie fixe et mobile sur les lieux de travail ;
– des fichiers de clients et de prospects ;
– des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet ;
– des traitements des collectivités locales visant à lutter contre la vacance des logements.

3 dispenses de déclaration exonérant de toute formalité déclarative :
– les traitements mis en œuvre par les organismes publics dans le cadre de la dématérialisation des marchés publics ;
– les fichiers de fournisseurs comportant des personnes physiques ;
– les sites web diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle.

3 autorisations uniques auxquelles peuvent se conformer d'autres traitements de même nature :
– les traitements des dispositifs d'alerte professionnelle ;
– les traitements de gestion des aides ponctuelles allouées aux étudiants ;
– certains traitements destinés à lutter contre le blanchiment de capitaux et le financement du terrorisme.

1 acte réglementaire unique auquel peuvent se rattacher les traitements des demandes de validation des attestations d'accueil mis en œuvre par les maires.

Au titre des formalités déclaratives

21 refus d'autorisation concernant en particulier des dispositifs biométriques de contrôle des salariés, des traitements de scoring et des traitements visant à mutualiser la détection d'incohérences dans des demandes de crédit, certains traitements destinés à constater des délits de contrefaçon commis par le biais du réseau internet, enfin un traitement basé sur la géolocalisation de véhicules.

20 avis sur des traitements sensibles ou à risques, tels que des dispositifs de vote électronique, le système de traitement des infractions constatées STIC, le système d'information judiciaire JUDEX, le fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS) ou encore le téléservice de demande d'acte de naissance.

Les saisines de la CNIL

En 2005, la CNIL a reçu 7 056 saisines qui se répartissent en :
– 1 760 demandes de droit d'accès indirect ;
– 3 834 plaintes ;
– 1 462 demandes de conseil.

Saisines	2004	2005	Variation 2004-2005
Demandes de droit d'accès indirect	1 970	1 760	- 10%
Plaintes	3 591	3 834	+ 6%
Demandes de conseil	1 595	1 462	- 8%
Totaux	7 156	7 056	- 1%

Comment **ça marche ?**

La saisine

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.

Les chiffres à la **loupe**

En 2005, la CNIL a :

- **enregistré 80 677 nouveaux traitements de données nominatives**
  ▲ *+ 20% de déclarations de fichiers par rapport à 2004*
- **reçu 3834 plaintes**
  ▲ *+ 6% de plaintes par rapport à 2004*
- **adopté 317 délibérations**
  ▲ *+ 200% de décisions par rapport à 2004*
- **effectué 96 contrôles**
  ▲ *+ 113% de contrôles par rapport à 2004*
- **adressé 36 mises en demeure**
  ▲ *c'est une compétence nouvelle de la CNIL*
- **prononcé 10 avertissements**
  ▲ *c'est un nombre record d'avertissements sur une année !*

Demandes de droit d'accès indirect

En 2005, la CNIL a procédé à 98 missions de vérifications qui ont porté sur 2 624 dossiers, soit une augmentation de 6% du nombre de dossiers vérifiés par rapport à 2004.

Demandes de conseil

Secteurs d'activité qui, par ordre décroissant, ont suscité le nombre le plus important de demandes de conseil : travail ; santé ; télécommunications.

Objet le plus fréquent des demandes de conseil : information sur les formalités préalables.

Plaintes

Secteurs d'activité qui, par ordre décroissant, ont suscité le nombre le plus important de plaintes : prospection commerciale ; banque ; télécommunications ; travail.

Objet le plus fréquent des plaintes : opposition à figurer dans un traitement.

Les plaintes fondent les deux tiers des dossiers examinés par la formation restreinte de la CNIL qui est en charge de prononcer des sanctions. De même, 22% des missions de contrôle effectuées par la CNIL trouvent leur origine dans des plaintes de personnes. En 2005, la CNIL a au total contrôlé près d'une centaine d'organismes.

Les déclarations de fichiers à la CNIL

Pour la période du 1er janvier au 31 décembre 2005, la CNIL a enregistré 80 677 nouveaux traitements de données nominatives. Ce sont au total 1 088 593 de fichiers qui ont été déclarés à la CNIL depuis 1978.

LA CNIL EN EUROPE ET DANS LE MONDE

Maintenir et consolider la protection des personnes en France implique pour la CNIL un investissement fort et quotidien sur le plan international. Cet investissement se décline en activités bilatérales et multilatérales.

Activités bilatérales

En 2005, les activités bilatérales se sont maintenues à un rythme très soutenu : accueil de délégations parlementaires américaine et russe, de représentants d'administrations en provenance d'Algérie, Albanie, Croatie, Mexique, États-Unis ; échanges bilatéraux entre homologues au niveau de la présidence et visites de collaborateurs ; participation à des manifestations organisées par ses homologues notamment au Canada, en Espagne et en Pologne ; intensification des échanges d'information ou de coopération sur place avec des pays de la francophonie en Afrique : Bénin, Burkina Faso, Maroc et Sénégal, ainsi qu'avec la Corée du Sud et le Japon.

Activités multilatérales

Activités européennes

La CNIL travaille conjointement avec ses homologues européens dans différents groupes de travail institutionnels ou informels. Dans le domaine communautaire elle est extrêmement impliquée dans les travaux du groupe dit « de l'article 29 ».

Un tel investissement au niveau européen se justifie à divers titres. De nombreuses initiatives sont désormais prises au niveau européen qui ont un très fort impact sur la protection des données au niveau national (exemples : base de données VIS, passeports biométriques, communication des données PNR des passagers des compagnies aériennes aux autorités américaines, etc.). En outre, les grandes entreprises et les organisations ou associations les représentant sollicitent le groupe de plus en plus fréquemment pour qu'il adopte des solutions globales, applicables dans tous les pays européens aux problèmes de protection des données liés à l'intégration de leurs structures, de leurs modes de fonctionnement, au développement de technologies nouvelles, etc. Ces différents facteurs militent pour une présence renforcée de la CNIL au niveau européen, comme de l'ensemble des autorités de protection des données européennes. Celles-ci sont d'ailleurs de plus en plus soucieuses de la cohérence de leurs actions respectives et tendent à accroître leurs échanges au niveau européen.

Les sujets abordés et les documents adoptés par le groupe sont, comme chaque année, d'une très grande diversité[4]. Ils sont révélateurs des grandes tendances mondiales, en premier lieu des questions de sécurité et de lutte contre le terrorisme.

➥ Ainsi, le G29 s'est prononcé sur la durée de conservation des données de communications électroniques fixée par un projet de directive européenne, en prônant une période maximale harmonisée d'un an pour les communications téléphoniques et de six mois pour l'internet. Le Parlement a proposé en première lecture une durée de conservation de six à vingt-quatre mois.

Des représentants du groupe de l'article 29, dont la CNIL, ont mené aux côtés de la Commission européenne, la première révision annuelle de l'Accord international Union européenne/États-Unis qui crée depuis mai 2004, une obligation de transfert de données passagers (PNR) aux autorités américaines : vérification du niveau de protection adéquat sur le terrain et de la mise en place (effective depuis peu) des conditions de filtrage et de blocage

Qu'est-ce que c'est ?

Le groupe de l'article 29 ou G29

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 indépendante 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 européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles. Le G29 se réunit à Bruxelles en séance plénière tous les deux mois environ. La CNIL est représentée dans les quatorze sous-groupes de travail en activité et qui ont la charge de préparer les travaux de la séance plénière.

4. Les documents adoptés par le groupe sont disponibles à l'adresse suivante : http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_fr.htm

Qu'est-ce que c'est ?

LES PILIERS DE L'UNION EUROPÉENNE

Le premier pilier

Le premier pilier concerne la libre circulation des personnes, l'asile, l'immigration ainsi que la coopération judiciaire en matière civile. Les mesures prises dans ces domaines relèvent de la compétence partagée entre les États membres et l'Union. Le Conseil vote à la majorité qualifiée. La Commission européenne dispose d'un monopole d'initiative. Le Parlement européen intervient, soit au titre de la codécision, soit pour avis ou avis conforme.

Le deuxième pilier

Le deuxième pilier concerne le domaine de la politique étrangère et de sécurité commune.

Le troisième pilier

Le troisième pilier concerne le domaine de la coopération policière et judiciaire en matière pénale. Il couvre la coopération en matière de justice et affaires intérieures (JAI) non communautarisée. Il s'agit de procédures de coopération de type intergouvernemental et les décisions sont prises à l'unanimité. Le Parlement européen est au mieux consulté pour rendre un avis ou informé régulièrement des travaux menés dans ce domaine avec la possibilité d'adresser des questions et de formuler des recommandations au Conseil européen.

des données sensibles. Le groupe reste préoccupé par le système de *pull* (extraction de toutes les données des vols détenues par les compagnies par les autorités américaines) qui avait vocation à être rapidement remplacé par un transfert ciblé en mode *push* (envoi par les compagnies aériennes des informations sélectionnées vers les autorités américaines).

La proposition de règlement concernant le système d'information sur les visas (VIS) est actuellement examinée au sein du Conseil européen au vu des amendements proposés par le Parlement européen en première lecture. Cette proposition qui relève du premier pilier a amené le Parlement européen à suivre l'avis du G 29, notamment, sur la suppression de la saisie des coordonnées de la personne invitante.

En ce qui concerne l'utilisation de la biométrie dans les passeports et documents de voyage, la résolution de Montreux adoptée lors de la conférence internationale des commissaires à la protection des données en septembre 2005, a été reprise par le G 29, pour affirmer la nécessité de restreindre l'usage des données biométriques contenues dans les passeports à un strict objet de comparaison entre les données stockées dans le passeport et celles fournies par le détenteur du passeport.

➥ Le groupe a également adopté des documents contribuant à encadrer l'émergence de nouvelles technologies ou de nouveaux services à valeur ajoutée, de manière à ce que leur développement tienne compte des risques qu'ils présentent pour les libertés des personnes (exemples : RFID, gestion des droits numériques, services de géolocalisation, etc.). Dans ces domaines, la CNIL a joué le plus souvent un rôle de premier plan.

➥ En matière de transferts internationaux de données vers des pays tiers de nouvelles étapes ont été franchies par le G 29 : adoption de documents offrant une grille d'analyse et décrivant une procédure de coordination européenne pour l'adoption de règles internes d'entreprise ; interprétation commune des dérogations à l'article 26-1 de la directive à l'initiative de la CNIL (c'est-à-dire des dérogations à l'exigence d'un niveau de protection adéquate dans les pays destinataires d'informations), organisation avec le Département américain du commerce d'un séminaire sur le *Safe Harbor*, en vue de promouvoir le bon fonctionnement de ce dispositif. Le groupe a également poursuivi ses travaux de simplification de la mise en œuvre de la directive 95/46/CE du 24 octobre 1995, ainsi par exemple en matière de notification des traitements aux autorités de contrôle. La CNIL a enfin animé le réseau européen de coopération des autorités en charge de la lutte antispam (CNSA) et accueilli une des deux réunions annuelles du groupe d'information et de coordination des services des autorités européennes de protection des données.

Dans le domaine du « troisième pilier », la CNIL siège au sein des deux autorités de contrôle communes (ACC), Europol et Schengen. Elle s'est employée au cours de ses réunions annuelles (dix en 2005), à renforcer les actions d'inspections menées auprès de chaque base centrale de données. L'ACC d'Europol a encadré dans un avis les conditions d'accès au SIS, les accords d'échanges de données de l'office de police d'Europol avec le Canada et l'Australie, et œuvré aux conditions d'une plus grande transparence de ses activités pour 2006. L'ACC Schengen a activement travaillé à l'adoption d'un avis sur le « paquet législatif » du futur dispositif Schengen II ; elle poursuit son action, en cohérence avec le groupe article 29 et le contrôleur européen, pour influencer l'évolution de ces textes en matière de répartition des responsabilités entre la Commission et les États membres et de supervision.

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.

Activités internationales

La CNIL a intensifié en 2005 ses activités en direction des institutions de la francophonie en vue de donner plein effet aux engagements pris, sur sa suggestion, par les chefs d'État et de gouvernement réunis à Ouagadougou en novembre 2004, de développer la protection des données. Elle a notamment pris part à la réunion de l'assemblée parlementaire francophone en juillet 2005. Alex Türk, président de la CNIL, s'est rendu à Dakar, en août, à un séminaire préparatoire à l'élaboration d'une loi de protection des données par le Sénégal.

La CNIL a participé à la conférence internationale annuelle des commissaires à la protection des données, organisée en septembre 2005 par l'autorité fédérale suisse de protection des données à Montreux. Cette conférence a pris l'initiative de lancer un appel en direction de l'ONU, du Conseil de l'Europe et des gouvernements visant à l'élaboration d'une convention internationale dans le domaine de la protection des données.

Lors des travaux de la seconde phase du sommet mondial de la société de l'information (SMSI) en novembre 2005, la CNIL faisait partie de la délégation française. Seule autorité en charge de la protection des données présente dans cette enceinte, la CNIL a participé à trois tables rondes sur l'état de la protection des données dans le monde, sur l'administration électronique et sur la lutte antispam.

LA CNIL ET LES CITOYENS

Priorité n° 1 : Faire connaître les droits

L'image de la CNIL

Comme en 2004, une étude portant sur la perception et l'image de la CNIL a été menée en décembre 2005 par TNS SOFRES sur un échantillon de 1 000 personnes représentatives de la population française.

Question : *Connaissez-vous ne serait-ce que de nom la CNIL ?*

	Juin 2004	Décembre 2005	Évolution 2004-2005
Oui	32	37	+ 5
Non	68	63	- 5
	100%	100%	

Question : *Connaissez-vous ne serait-ce que de nom la Commission nationale de l'informatique et des libertés ?*

	Juin 2004	Décembre 2005	Évolution 2004-2005
Oui	45	49	+ 4
Non	55	51	- 4
	100%	100%	

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

	Juin 2004	Décembre 2005	Évolution 2004-2005
Oui, tout à fait	3	5	+ 2
Oui, plutôt	18	24	+ 6
Sous-total oui	**21**	**29**	+ 8
Non, plutôt pas	39	38	- 1
Non, pas du tout	39	29	- 10
Sous-total non	78	67	- 11
Sans opinion	1	4	+ 3
	100%	100%	

Les interventions de la CNIL

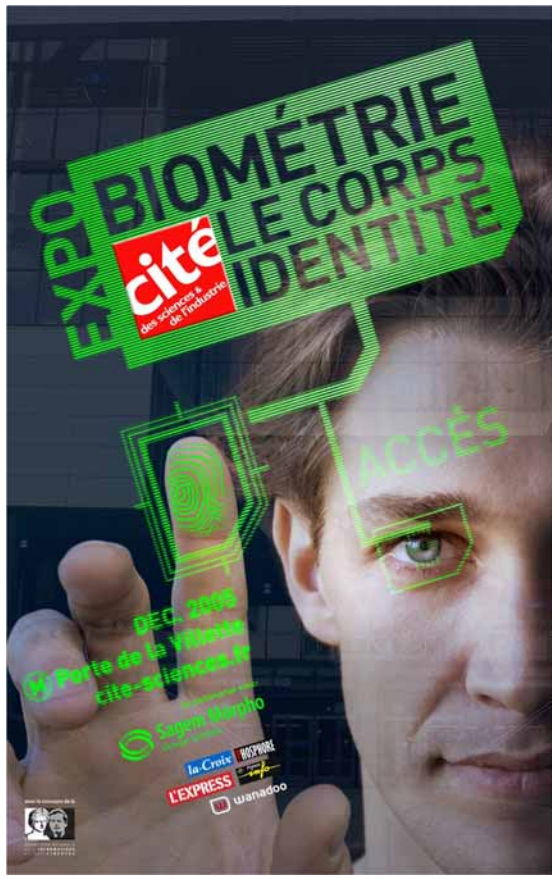
En 2005, la CNIL a assuré 145 interventions à des conférences/colloques/séminaires ou animations de formations qui ont mobilisé 517 membres ou agents. Au total, la CNIL a reçu 218 sollicitations d'interventions.

L'organisation d'un colLoque

En partenariat avec l'université Paris II et le Sénat, la CNIL a organisé un colloque intitulé « Informatique : servitude ou libertés ? » qui s'est tenu les 7 et 8 novembre 2005 au palais du Luxembourg. Ce colloque a réuni 255 participants et une vingtaine d'intervenants français ou étrangers d'horizons très divers (sociologues, universitaires, chercheurs, industriels …).

Le partenariat avec la cité des sciences

La CNIL a apporté un partenariat technique dans le cadre de l'organisation de l'exposition « Biométrie, le corps identité » qui se tient à la Cité des Sciences de la Villette, à Paris, du 25 novembre 2005 au 5 novembre 2006. Cette exposition rappelle l'histoire, les techniques existantes, les applications et aussi sur quels critères la CNIL est amenée à délivrer ou non une autorisation au cas par cas.



Le tour de France des régions

La CNIL a entamé en janvier 2005 une démarche inédite d'information et de communication de proximité qui a pour objectif de pallier l'absence de représentations régionales de la CNIL à ce jour et de développer sa mission de pédagogie auprès des professionnels et du grand public. Pendant deux ou trois jours, le président, accompagné de membres et d'agents de la CNIL, va à la rencontre de l'ensemble des acteurs locaux concernés par la protection des données personnelles : entreprises, administrations, collectivités locales, élus, associations, journalistes, citoyens, avocats, professionnels de la santé et de l'éducation, acteurs sociaux, etc.

En 2005, cinq régions ont été visitées : Nord-Pas-de-Calais, Bretagne, Midi-Pyrénées, Franche-Comté et Provence-Alpes-Côte d'Azur.

Les guides

En 2005, la CNIL a édité trois guides pratiques destinés aux professionnels : *Halte aux pubs*, *Associations ; Employeurs*.

Une plaquette de présentation de la CNIL destinée au grand public *La CNIL en bref* a aussi été réalisée.

Le site internet

Avec un volume de 9 millions de pages vues sur l'année 2005, soit 2 millions de plus que l'an passé, et en moyenne 3 300 visiteurs différents par jour, soit un gain annuel de 10%, l'audience du site de la CNIL poursuit sa progression. Par ailleurs, le nombre total de visites, qui comptabilise toutes les sessions même si plusieurs sont le fait d'une même personne, est en augmentation de 38% par rapport à l'année passée, ce qui atteste d'une fidélisation des internautes visitant le site de la CNIL. Mêmes tendances pour la lettre mensuelle d'information qui compte 12 900 abonnés au 31 décembre 2005, contre 8 642 abonnés au 31 décembre 2004, soit + 49% d'abonnés en 2005.

Après une refonte totale en mars 2004, le site de la CNIL continue d'évoluer et les principales nouveautés 2005 sont les suivantes :

– un fil RSS pour relayer l'actualité de la CNIL ;
– un « générateur automatique de courriers » pour exercer ses droits, qui donne lieu à la création de 1 500 modèles de courriers chaque mois, principalement pour demander à accéder à ses données ou pour se faire radier d'un fichier ;
– une carte interactive sur le niveau de protection des données assuré dans chaque pays du monde ;
– des FAQ, soit une soixantaine de questions-réponses en ligne ;
– une rubrique « Les grands fichiers en fiches » qui a vocation à fournir les caractéristiques des fichiers nationaux les plus importants.

Priorité n° 2 : AMÉLIORER LE DROIT D'ACCÈS INDIRECT

Après une explosion du nombre des saisines en 2004, due à l'entrée en vigueur des dispositions relatives à l'utilisation des fichiers de police dans des enquêtes administratives, ce nombre s'est stabilisé en 2005 à un niveau qui excède largement les capacités de traitement de la CNIL. En effet, ces demandes de droit d'accès indirect nécessitent plus de 4 500 vérifications, une même requête pouvant concerner plusieurs traitements (par exemple pour les fichiers de police consultés lors d'une assermentation, le fichier du système de traitement des infractions constatées - STIC -, les fichiers de sécurité publique des commissariats et le fichier JUDEX de la Gendarmerie nationale).

L'analyse des demandes montre comme les années précédentes que les requérants saisissent de plus en plus la CNIL à la suite d'un refus d'embauche (par exemple dans les sociétés de gardiennage et de sécurité) ou d'un licenciement résultant d'une enquête administrative défavorable ou encore du non-renouvellement d'une autorisation de port d'arme (notamment pour les agents de sécurité employés par la RATP ou la police ferroviaire). Les autres demandes résultent notamment d'un refus de délivrance de visa ou d'un titre de séjour du fait de l'inscription dans le système d'information Schengen.

Au cours de l'année 2005, 3 210 vérifications ont été effectuées dont 78% opérées dans les fichiers du ministère de l'Intérieur. Ces 3 210 vérifications concernent pour une large part des saisines reçues au cours des années précédentes car la recherche d'un éventuel signalement dans les différents fichiers prend plusieurs mois et nécessite de nombreuses investigations notamment pour contrôler les mises à jour et les suppressions.

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.

Les fichiers visés par les vérifications faites en 2005 au titre du droit d'accès indirect

Ministère de l'Intérieur	**2 513**
Renseignements généraux (RG)	430
Police judiciaire (PJ)	988
Sécurité publique (SP)	614
Direction de la surveillance du territoire (DST)	64
Système d'information Schengen (SIS)	410
Direction centrale de la sécurité du CEA (DCS)	7
Ministère de la Défense	**697**
Gendarmerie nationale (GEND)	631
Direction de la protection et de la sécurité de la défense (DPSD)	33
Direction générale de la sécurité extérieure (DGSE)	33
Total	**3 210**

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.

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 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. La troisième base est décentrée dans chaque département et 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.

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

Les 1 292 investigations menées en 2005 dans les fichiers autres que ceux des renseignements généraux, de la police judiciaire et du système d'information Schengen portent principalement sur les fichiers de la sécurité publique et la gendarmerie nationale.

Les fichiers de la police judiciaire STIC et JUDEX

Sur les 1 078 investigations menées en 2005 sur les fichiers de police judiciaire (STIC et JUDEX), 207 signalements en tant que mis en cause ont été supprimés.

La procédure de communication des fiches STIC aux personnes concernées, avec l'accord du ministère de l'Intérieur et du procureur de la République, qui est prévue par le décret du 5 juillet 2001 créant le STIC, a commencé à être mise en œuvre à partir du 1er août 2005. Mais la CNIL est toujours en attente de l'accord de communication des procureurs et ces dossiers ne sont donc pas pris en compte dans les statistiques de 2005.

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. Les membres désignés par la CNIL pour mener ces investigations peuvent, en accord avec le ministre de l'Intérieur, constater que certaines informations ne mettent pas en cause la sûreté de l'État, la défense et la sécurité publique et qu'il y a lieu, en conséquence de les communiquer au requérant. Les investigations portent à la fois sur le fichier informatique d'indexation et sur le dossier individuel, sur les extraits des dossiers collectifs contenant des informations nominatives sur les demandeurs, ainsi que sur les dossiers conservés dans les sections spécialisées de la direction centrale des renseignements généraux.

La CNIL vous défend

Les investigations dans les fichiers de police judiciaire (STIC - JUDEX) ont conduit la CNIL à faire procéder dans 44% des cas (207 saisines sur les 467 requérants fichés en tant que mis en cause à la police judiciaire) à des mises à jour ou à la suppression de signalements erronés, manifestement non justifiés ou dont le délai de conservation était expiré.

Bilan des 430 investigations menées en 2005 dans les fichiers des renseignements généraux

	Investigations aux fichiers des RG	% sur le nombre de requérants
Requérants non fichés aux RG	314	73%
Requérants fichés aux RG	116	27%
Total	430	100%

Sur les 116 requérants fichés, 109 dossiers ont été jugés communicables (98 totalement, 11 partiellement).

Il doit être relevé que, comme 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. La consultation des pièces communicables du dossier s'effectue au siège de la CNIL lorsque les requérants sont domiciliés dans la région Île-de-France. Dans tous les autres cas la communication est organisée au siège de la préfecture du département dans lequel est domicilié le requérant. Parmi les 109 communications qui ont été effectuées en 2005, 43 ont eu lieu au siège de la CNIL et 66 ont été effectuées par l'autorité préfectorale du lieu de résidence de l'intéressé. À la suite de ces communications, seuls 12 requérants ont adressé une note d'observation : 4 ont été insérées dans le dossier des renseignements généraux les concernant, 2 ont donné lieu à des suppressions partielles et 6 à des suppressions totales.

Évolution des investigations aux renseignements généraux depuis 2001

Année	2001	2002	2003	2004	2005
Nombre de demandes traitées	576	1 012	686	682	430
Absence de fiche	415	776	443	510	314
% sur le total	72%	76%	65%	75%	73%
Nombre de requérants fichés aux RG	161	236	243	172	116
% sur le total	28%	23%	35%	25%	27%
Dossiers non communicables	35	36	26	15	7
% sur le nombre de fichés	22%	15%	11%	9%	6%
Communication acceptée par le ministre de l'Intérieur	126	200	217	157	109
% sur le nombre de fichés	78%	85%	89%	91%	94%
Communication totale	126	199	217	157	98
Communication partielle		1		-	11

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 3 412 demandes de droit d'accès.

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

	Nombre	Total cumulé
2001	297	1 194
2002	661	1 855
2003	599	2 454
2004	548	3 002
2005	410	3 412

Sur les 3 412 demandes de droit d'accès indirect au système d'information Schengen, 1 059 personnes étaient signalées.

Ces 1 059 signalements proviennent par ordre décroissant des pays suivants :

Pays signalant	Nombre de signalements	% par rapport au nombre de signalements
France	431	41,0%
Allemagne	397	37,0%
Italie	167	16,0%
Espagne	35	3,3%
Grèce	15	1,4%
Pays-Bas	8	0,7%
Autriche	3	0,3%
Belgique	2	0,2%
Suède	1	0,1%
Total	**1 059**	**100%**

À la suite des démarches entreprises par la CNIL, 377 signalements ont été supprimés du N-SIS (soit 36%) dont 258 par l'Allemagne, 75 par la France, 28 par l'Italie, 9 par l'Espagne, 3 par les Pays-Bas, 3 par la Grèce et 1 par la Belgique.

Dès lors qu'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 saisit 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 le ministère des Affaires étrangères et en particulier 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 mixte. Ainsi, les informations enregistrées lors de la demande de visa bénéficient d'un accès direct qui peut être exercé auprès du consulat ou de l'ambassade où la demande a été déposée. En revanche les informations figurant dans les fichiers d'attention (fichier central comme fichiers locaux) et dont la divulgation serait susceptible de porter atteinte à la sûreté de l'État, la défense et la sécurité publique, font l'objet d'un droit d'accès indirect. 66 interrogations ont été faites auprès du ministère des Affaires étrangères, aucun requérant n'était enregistré dans les fichiers d'attention des postes consulaires.

C'est votre droit

La CNIL a défini au mois de mai 2005, en concertation avec le ministère de l'Intérieur, le ministère de la Défense et la chancellerie, les modalités pratiques selon lesquelles les requérants peuvent obtenir communication de leurs fiches STIC ou JUDEX : ceci constitue une avancée notable mais sur ce point la CNIL entend aller plus loin. Dans son avis rendu le 8 septembre 2005 sur les nouveaux projets de décrets STIC et JUDEX, la CNIL préconise la reconnaissance au profit des victimes d'un droit d'accès direct aux informations les concernant dans les fichiers de police judiciaire ainsi que l'obligation de vérifier les mentions des informations de mise en cause avant toute utilisation administrative.

Questions à …

Jean MASSOT

Président de section honoraire au Conseil d'État

Commissaire en charge notamment du droit d'accès indirect

Quelles sont les difficultés rencontrées dans l'organisation de l'exercice du droit d'accès indirect ?

Actuellement, les délais d'instruction des demandes de droit d'accès indirect aux fichiers des renseignements généraux et de police judiciaire sont de l'ordre de plusieurs mois. Ces délais sont beaucoup trop longs. En effet, une large part des demandes provient de requérants exerçant des emplois de sécurité, qui se voient refuser une embauche ou se font licencier à la suite d'un signalement dans le STIC. Or, ils doivent attendre parfois plus d'un an avant de connaître les résultats des investigations opérées par la CNIL dans les fichiers de police. Entre-temps, ils ont perdu leur travail et se trouvent parfois dans une situation d'extrême précarité, ne pouvant retrouver un nouvel emploi dans leur domaine.

Comment s'explique la longueur des délais d'instruction des demandes de droit d'accès indirect ?

Sans méconnaître le manque de moyens en personnel de la CNIL, cette situation résulte essentiellement des délais d'instruction des demandes par les services du ministère de l'Intérieur et les parquets.

Les services de police judiciaire doivent en effet rechercher dans les différents fichiers un éventuel signalement, rassembler les procédures dans le cadre d'affaires signalées dans les fichiers de police judiciaire, interroger les procureurs pour connaître les suites judiciaires et recueillir leur accord de communication ou les dossiers papier conservés par les directions départementales des RG. Il faut donc compter en moyenne un délai d'un an pour avoir des réponses aux demandes transmises par la CNIL.

Quels sont les moyens envisageables pour raccourcir les délais et améliorer de l'exercice du droit d'accès indirect ?

Il faut tout d'abord souligner que le décret d'application de la loi du 6 août 2004 en date du 20 octobre 2005 impose désormais aux services de la CNIL un délai de quatre mois à compter de la réception de la saisine pour instruire la demande et notifier au requérant le résultat de ses investigations. À l'intérieur de ce délai de quatre mois, les ministères gestionnaires des fichiers disposent de trois mois maximum à compter de la date de réception de la transmission des demandes adressées par la CNIL. Soyons clairs : ces délais ne sont pas tenables sans un réexamen complet des procédures et un renforcement des moyens consacrés à ces fichiers tant par la CNIL que par l'institution judiciaire, l'intérieur et la défense.

Mais surtout, sur le fond, il est indispensable de limiter les effets ravageurs des mentions erronées, notamment sur les refus d'embauche. Constatant, comme il a été dit plus haut, que ces erreurs pouvaient concerner plus de 40% des cas vérifiés, la CNIL souhaite que l'utilisation de ces fichiers pour des enquêtes administratives ne soit désormais possible qu'après vérification de la pertinence et de l'actualité de ces mentions.

LA NOUVELLE LOI «INFORMATIQUE ET LIBERTÉS» EN PRATIQUE

LE DÉCRET D'APPLICATION : Le correspondant a un statut

Introduit en 2004 à l'occasion de la refonte de la loi du 6 janvier 1978, le correspondant à la protection des données ou «correspondant informatique et libertés» est désormais un personnage incontournable dans le paysage de la protection des données à caractère personnel. Tous les responsables de traitement, qu'ils soient publics ou privés, qu'ils aient le statut d'association, de collectivité territoriale ou d'administration de l'État, qu'il s'agisse de PME-PMI ou d'entreprises multinationales, sont concernés.

Avec la parution du décret d'application de la loi «informatique et libertés» le 20 octobre 2005, les entreprises, les collectivités locales, les établissements publics, les associations peuvent désormais désigner un correspondant informatique et libertés. Cette innovation majeure constitue un tournant dans l'application de la loi : l'accent est mis sur la pédagogie et le conseil en amont. En effet, désigner un correspondant permet certes de bénéficier d'un allègement des formalités déclaratives mais surtout de s'assurer que l'informatique de l'organisation se développera sans danger pour les droits des usagers, des clients et des salariés. C'est aussi, pour les responsables de fichiers, le moyen de se garantir de nombreux risques résultant d'une mauvaise application du droit en vigueur.

Un dispositif facultatif permettant d'alléger les formalités tout en assurant une meilleure application de la loi

La désignation d'un correspondant a pour effet d'exonérer les responsables des traitements de l'accomplissement de tout ou partie des formalités préalables leur incombant. Seuls les traitements relevant d'un régime d'autorisation ou comportant des transferts de données en dehors de l'Union européenne continueront à faire l'objet de formalités préalables.

La désignation du correspondant permet surtout au responsable de traitements de mieux remplir les obligations qui lui incombent en application de la loi : sécurité, transparence, proportionnalité, respect de la finalité des traitements et des droits des personnes. De lourdes sanctions sont encourues en cas de manquements. En recourant au mécanisme du correspondant, le responsable de traitement dispose d'un interlocuteur spécialisé à même de le conseiller, d'émettre des recommandations, de faire de la pédagogie, voire de l'alerter en cas de dysfonctionnements graves.

Les principales caractéristiques de la fonction de correspondant

Une personne pouvant agir de manière indépendante

Le correspondant est avant tout la personne pouvant répondre aux besoins spécifiques du responsable de traitement, disposant de la liberté d'action et de l'autorité indispensables pour recommander des solutions organisationnelles ou technologiques. Il doit ainsi être à l'abri des conflits d'intérêt. Le responsable de traitement, ainsi que par extension toutes les personnes exerçant par délégation de fait ou de droit les fonctions du responsable de traitement, ne peuvent être désignés comme correspondant.

Une personne dotée de qualifications adaptées

Il devra nécessairement disposer des qualifications adaptées à la taille et à l'activité du responsable de traitement. Aucun agrément n'est prévu et aucune exigence de diplôme n'est fixée. Ces compétences et qualifications doivent porter tant sur la législation relative à la protection des données à caractère personnel que sur l'informatique et les nouvelles technologies, sans oublier le domaine d'activité propre du responsable des traitements.

Une personne interne ou externe

Il peut aussi bien être choisi au sein de l'organisme qu'à l'extérieur. Toutefois, les possibilités de choix d'un correspondant externe ne sont pas les mêmes pour tous les organismes. Au-delà d'un certain nombre de salariés concernés, seuls peuvent être désignés comme correspondants des personnes se trouvant dans l'entourage économique de l'organisme qui le désigne.

Des moyens au service des correspondants

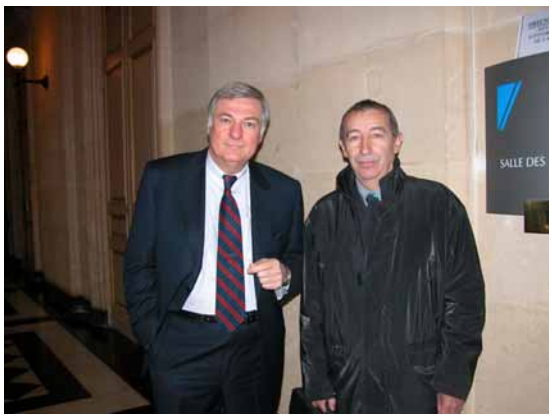
Pour aider les correspondants dans l'accomplissement de leurs missions, la CNIL a mis en place un service entièrement dédié avec pour objectif de les faire bénéficier, dans un délai très court, des conseils, de l'information et de l'orientation qui leur sont nécessaires pour développer leur action. Ceci signifie qu'ils feront l'objet d'un traitement prioritaire.

Ils seront invités à des échanges réguliers avec la CNIL qui, bien sûr, ne pourra prendre en charge l'ensemble de leur formation mais favorisera l'émergence d'enseignements adaptés, indispensables à l'exercice des missions du correspondant.

Les correspondants en chiffres

Au 31 décembre 2005, soixante-treize organismes avaient désigné un correspondant.

Certains correspondants ayant été désignés pour un groupe de sociétés ou un regroupement de responsables de traitement, le nombre de correspondants désigné est de vingt et concerne plusieurs milliers de salariés.



Alex Türk et Jacques Parent du port autonome de Marseille, premier correspondant en France.

Les correspondants en questions

La fonction de correspondant est-elle un emploi à plein temps ?

Très rarement. Dans la plupart des cas, les missions de correspondant seront intégrées à d'autres fonctions assurant la conformité aux règles internes ou légales : direction juridique, audit, déontologie, service qualité, sécurité des systèmes d'information, etc.

Un même correspondant peut-il être désigné par plusieurs organismes ?

Oui. On dit qu'il est « mutualisé ». Tel est le cas par exemple du correspondant salarié d'une des sociétés appartenant à un groupe et exerçant ses missions pour toutes les sociétés du groupe.

À propos du correspondant

Désigner un correspondant c'est :

- **disposer d'une personne compétente et qualifiée pour répondre aux questions que l'on se pose sur l'application de la loi ;**
- **organiser et structurer le traitement des informations à caractère personnel ;**
- **maîtriser le développement des nouvelles technologies de l'information et de la communication ;**
- **assurer le respect des droits des personnes.**

Désigner un correspondant n'est pas :

- **une nouvelle charge : les missions du correspondant relèvent de l'application des règles de bonne gestion des données à caractère personnel. Elles correspondent à un contrôle de conformité et de qualité ;**
- **un moyen pour le responsable de traitement de se défausser de toute responsabilité dans l'application de la loi. Sa responsabilité reste pleine et entière mais le correspondant est là pour le protéger ;**
- **la fin de la transparence pour les traitements dispensés de déclaration auprès de la CNIL du fait de la désignation du correspondant. Une des missions du correspondant consiste à tenir la liste des traitements dispensés et de la mettre à disposition de toute personne en faisant la demande.**

LES MESURES DE SIMPLIFICATION

La simplification des formalités préalables constitue l'un des principaux axes de la nouvelle loi et la CNIL en 2005 a pris à son compte cet objectif en utilisant toute la panoplie des instruments prévus par la nouvelle loi. Elle a défini un certain nombre de traitements, parmi les plus courants, qui ne sont pas susceptibles de porter atteinte aux droits des personnes. Ils bénéficient soit d'une dispense totale de déclaration, soit d'une procédure allégée : déclaration simplifiée ou engagement de conformité à une autorisation unique, qui s'effectuent toutes par téléprocédure sur le site de la CNIL.

Le lancement des exonérations de déclarations

La CNIL a fait application à trois reprises de la possibilité nouvelle offerte par la loi du 6 janvier 1978 modifiée de dispenser certaines catégories de traitements de toute formalité déclarative préalable :

– le 18 janvier 2005, les fichiers de fournisseurs qui étaient jusqu'alors soumis à la déclaration simplifiée en référence à la norme n° 14 ;

– toujours en janvier 2005, les traitements mis en œuvre par les organismes publics dans le cadre de la dématérialisation des marchés publics ;

– en décembre 2005, les sites web mis en œuvre par les particuliers.

La mise sur orbite des formalités allégées

Alors que de 1978 à 2004, quarante-cinq normes simplifiées avaient été émises, 2005 a vu la publication de cinq nouvelles normes, intervenant dans des secteurs d'activité jusqu'alors non concernés ou élargissant considérablement le champ d'application de normes existantes. Par ailleurs, en matière d'autorisation unique, trois décisions ont été prises dans le prolongement de celle intervenue en 2004.

Encore plus de normes simplifiées

La création de nouvelles normes

• Poursuivant son travail de simplification dans le secteur du travail qui reste source de très nombreuses déclarations, la Commission a adopté, le 13 janvier 2005, après consultation des partenaires sociaux et des pouvoirs publics, une nouvelle norme simplifiée couvrant les traitements courants de gestion des ressources humaines (norme simplifiée n° 46).

Bénéficiant aux secteurs public et privé, cette nouvelle norme concerne la gestion administrative des personnels (dossier professionnel, annuaires, élections professionnelles…), la mise à disposition d'outils informatiques (suivi et maintenance des matériels, annuaires informatiques, messagerie électronique, intranet…), l'organisation du travail (agendas professionnels, gestion des tâches), la gestion des carrières (évaluation, validation des acquis, mobilité…) et la formation des personnels. Elle prévoit des garde-fous en excluant notamment tous les fichiers permettant un contrôle de l'activité des employés (cybersurveillance, vidéosurveillance…). Elle ne concerne pas non plus des domaines sensibles tels que les fichiers médicaux gérés par la médecine du travail, les dossiers du service social ou encore le recours à des techniques biométriques.

• La norme simplifiée n° 47, adoptée le 3 février 2005, concerne l'utilisation des services de téléphonie fixe et mobile sur les lieux de travail.

La norme simplifiée n° 40 permettait de faire bénéficier de la procédure de la déclaration simplifiée les traitements mis en œuvre par les entreprises ou organismes privés et publics à l'aide d'autocommutateurs téléphoniques, c'est-à-dire ceux liés à l'utilisation de la téléphonie fixe. Elle n'incluait pas dans son champ d'application les traitements liés à l'utilisation de la téléphonie mobile par les employés.

Avec l'abrogation de la norme 40, les déclarations qui ont été effectuées en référence à cette norme restent valables mais, désormais, c'est la norme 47 qui devient la norme de référence en matière de déclaration simplifiée pour l'utilisation de services de téléphonie sur les lieux de travail.

• La CNIL a adopté le 7 juin 2005 une nouvelle norme simplifiée n° 48 relative à la gestion des fichiers de clients

et de prospects. Cette norme inclut désormais la collecte de données par le biais d'internet ainsi que la prospection par voie électronique.

Dès le début des années 1980, la CNIL avait prévu des procédures allégées en matière de déclaration de fichier clientèle avec l'adoption respectivement de la norme 11 relative à la gestion des clients actuels et potentiels, de la norme 17 pour la gestion des fichiers de clientèle des entreprises dont l'objet social inclut la vente par correspondance et de la norme 25 relative à la gestion des fichiers de destinataires d'une publication périodique de presse. Ces trois normes sont abrogées et remplacées par la nouvelle norme 48, qui intègre, compte tenu de la banalisation de l'utilisation de l'internet, la collecte des données par internet ainsi que la prospection commerciale opérée par voie électronique. Sont cependant exclus certains secteurs d'activité : les établissements bancaires ou assimilés, les entreprises d'assurances, de santé et d'éducation, qui disposent de normes particulières. La norme rappelle les principales préconisations dégagées par la CNIL, en concertation avec les professionnels du marketing direct, pour l'envoi de sollicitations par courrier électronique ou par SMS et pour la commercialisation des fichiers d'adresses de courrier électronique. Elle introduit des dispositions spécifiques dans le cadre de l'utilisation d'un service de communication au public en ligne en précisant les conditions de traitement des données de connexion et l'utilisation de « cookies ».

• Le secteur des collectivités locales a également bénéficié de cette politique de simplification puisque la CNIL a adopté le 18 octobre 2005 la norme simplifiée n° 49 à laquelle les collectivités pourront se référer pour déclarer l'utilisation du fichier des logements vacants de leur territoire qu'elles peuvent obtenir de l'administration fiscale depuis l'adoption de la loi de programmation pour la cohésion sociale. La norme n° 49 restreint l'utilisation des données aux objectifs de politique d'aide au logement pris en compte par le législateur.

• La multiplication du nombre des déclarations émanant des professions libérales et para-médicales de santé utilisant pour la gestion de leurs cabinets des logiciels bien connus de la CNIL a conduit celle-ci à décider de simplifier ces déclarations. Les professionnels peuvent désormais déclarer la gestion des dossiers médicaux par référence à la nouvelle norme n° 50 adoptée le 22 novembre 2005. Ils s'engagent en contrepartie à informer leurs patients et à assurer un haut niveau de confidentialité aux données de santé. Sont concernés les médecins, les dentistes et les professions paramédicales exerçant à titre libéral. En revanche, n'entrent pas dans son champ d'application les pharmacies et les laboratoires d'analyses de biologie médicale pour lesquels des normes simplifiées particulières devraient prochainement être adoptées. La norme rappelle que toute exploitation à des fins commerciales des données de santé ainsi collectées est prohibée.

L'extension du champ d'application de normes existantes

Par deux délibérations du 17 novembre 2005, la CNIL a simplifié les démarches des entreprises en matière de transferts de données à l'étranger : elle a en effet élargi le champ d'application des deux normes simplifiées les plus utilisées par les entreprises, relatives à la gestion des salariés et des clients, à certains transferts internationaux de données vers des pays n'assurant pas un niveau de protection adéquat (normes simplifiées 46 et 48).

Les transferts concernés sont relatifs :
– à la gestion de fichiers de clients et de prospects, qui a vocation à s'appliquer à toutes les opérations courantes auxquelles ont recours les entreprises dans le cadre de leurs activités s'agissant de la gestion de la facturation, des commandes et des livraisons ainsi que les actions de sollicitations commerciales ;
– à la gestion administrative des personnels mais uniquement pour les traitements permettant la réalisation d'états statistiques ou de listes d'employés pour répondre à des besoins de gestion administrative, la gestion des annuaires internes et des organigrammes et la mise à disposition des personnels d'outils informatiques. La CNIL a voulu limiter l'autorisation de transfert en excluant les traitements permettant le contrôle individuel de l'activité des employés.

Les nouvelles normes modifiées définissent le cadre dans lequel les transferts de données vers l'étranger pourront être autorisés.

Premières autorisations uniques pour les entreprises

Les traitements soumis à autorisation de la CNIL peuvent faire l'objet d'une autorisation unique, quand ils ont la même finalité et concernent les mêmes catégories de données et de destinataires.

• La CNIL a adopté le 1er décembre 2005 une autorisation unique pour les traitements de données à caractère personnel mis en œuvre dans certains organismes financiers au titre de la lutte contre le blanchiment de capitaux et le financement du terrorisme.

De tels traitements visent à détecter des transactions financières réalisées par les clients des établissements de crédit qui sont susceptibles d'être qualifiées d'infraction de blanchiment ou de financement du terrorisme par les autorités compétentes et qui, de ce fait, doivent, le cas échéant après la collecte de renseignements complémentaires ou un travail d'analyse non automatisé, donner lieu à l'envoi d'une déclaration à la cellule TRACFIN du ministère de l'Économie, des Finances et de l'Industrie. Ces traitements visent également à permettre l'application du dispositif légal de gel des avoirs dans le cadre de la lutte contre le financement du terrorisme.

L'identification de tels faits, pour une large part sur la base de critères intégrés dans les traitements automatisés des organismes financiers, peut conduire ces derniers, pour des raisons de prudence, à rompre toute relation contractuelle avec certains des clients qui en font l'objet. Ces traitements sont ainsi susceptibles de conduire à l'exclusion de personnes du bénéfice d'un contrat en l'absence de toute disposition légale prévoyant la mise en œuvre d'une telle exclusion et doivent donc être autorisés par la Commission.

Après avoir consulté tant les autorités publiques que les professionnels concernés, la Commission a défini le cadre juridique auquel les établissements doivent satisfaire pour bénéficier de la procédure allégée. Ce texte fera l'objet d'aménagements ultérieurs, afin d'en étendre le champ d'application aux autres secteurs d'activité concernés, notamment l'assurance.

• La CNIL a adopté, le 8 décembre 2005, une décision d'autorisation unique concernant les dispositifs d'alerte professionnelle (*whistleblowing*), à la suite du document d'orientation définissant les conditions que doivent remplir ces dispositifs pour être conformes à la loi « informatique et libertés ».

Seuls peuvent faire l'objet d'un engagement de conformité par référence à cette décision unique les traitements mis en œuvre par les organismes publics ou privés dans le cadre d'un dispositif d'alerte professionnelle répondant à une obligation de droit français visant à l'établissement de procédures de contrôle interne dans les domaines : financier, comptable, bancaire et de la lutte contre la corruption. Les traitements mis en œuvre dans les domaines comptable et d'audit par les entreprises concernées par la section 301(4) de la loi américaine dite Sarbanes-Oxley de juillet 2002 entrent également dans le champ de la décision. De plus, cette décision vaut, sous certaines conditions, autorisation de transfert des données vers des pays n'appartenant pas à l'Union européenne.

• La CNIL a adopté le 18 octobre 2005 une autorisation unique pour les traitements de gestion des aides ponctuelles allouées aux étudiants dans le cadre de l'action sociale et le suivi statistique de l'activité de services sociaux des centres régionaux des œuvres universitaires et scolaires.

LE CONSEIL

La loi donne à la CNIL mission de conseiller les pouvoirs publics et les responsables de traitement.

Les recommandations 2005 de la CNIL

La recommandation du 11 octobre 2005 sur les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel (délibération n° 2005-213)

Toute entreprise est aujourd'hui conduite, notamment afin d'assurer sa propre sécurité juridique ou d'améliorer sa capacité décisionnelle, à conserver nombre d'informations ou documents sur ses activités passées, s'agissant notamment des relations qu'elle entretient avec ses clients, ses fournisseurs ou ses salariés. Ceci implique généralement le recours à des systèmes d'archivage électronique (numérisation de documents papier ou conservation d'informations nativement électroniques).

En 1988, la CNIL avait déjà souligné dans une recommandation pour les administrations et organismes du secteur public la nécessité de concilier les principes de la « loi informatique et libertés » avec ceux de la loi sur les archives, en application du devoir de mémoire. Il est apparu nécessaire à la CNIL de poursuivre, sur le fondement du droit à l'oubli, la réflexion engagée sur ce sujet en la transposant aux problématiques concernant les archives dites privées.

À l'issue d'une large concertation engagée auprès des professionnels concernés (notamment dans le cadre de la Commission de normalisation n° 43-400 de l'AFNOR ainsi que du groupe de travail constitué par le Forum des droits sur l'internet relatif à l'archivage électronique de documents), la CNIL a adopté une recommandation dont l'objectif est d'établir des règles relatives aux modalités pratiques de l'archivage (conditions d'accès, support de stockage des données, etc.).

La recommandation du 22 novembre 2005 sur la mise en œuvre par des particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle (délibération n° 2005-285)

La question du respect de la vie privée des internautes est devenue essentielle à l'heure où plus de 4 millions de blogs sont en ligne et où un blog se crée toutes les dix secondes. Ce développement a conduit la CNIL à préciser les règles qui sont applicables aux sites personnels en matière de protection des données à caractère personnel. En effet, la loi « informatique et libertés » s'applique dès lors qu'un site web diffuse ou recueille une donnée à caractère personnel (nom, image d'une personne, etc.).

Prenant la mesure du très grand nombre de sites web mis en œuvre par les particuliers, la Commission a décidé de les dispenser de déclaration. Pour autant, comme la recommandation le rappelle, ceux-ci ne sont pas dispensés de respecter la loi.

La validation des codes de déontologie de l'e-mailing

Depuis plusieurs années, la CNIL a engagé un travail de concertation avec les professionnels de la vente à distance et du marketing direct afin de dégager des règles de déontologie dans le secteur du marketing. Cependant, c'est dans un cadre juridique nouveau que le SNCD (Syndicat national de la communication directe) et l'UFMD (Union française du marketing direct) ont demandé l'avis de la CNIL sur des projets de code de déontologie visant à définir les modalités pratiques d'application du nouveau régime juridique applicable à la prospection par courrier électronique introduit par la loi sur l'économie numérique.

La CNIL a ainsi, pour la première fois, fait application de l'article 11 de la loi de 1978 modifiée qui lui reconnaît la possibilité de donner un avis sur la conformité aux dispositions de la loi « informatique et libertés » des projets de règles professionnelles tendant à la protection des données à caractère personnel. C'est dans ce cadre que la Commission a, par deux délibérations adoptées en mars 2005, estimé que les projets de code présentés respectivement par le SNCD et l'UFMD étaient conformes aux exigences légales et à ses préconisations.

Ces codes proposent notamment des exemples de mentions de recueil du consentement des personnes concernées pour recevoir de la prospection.

Questions à …

Emmanuel de GIVRY

Conseiller à la Cour de cassation

Commissaire en charge du secteur «Gestion des risques et des droits»

Pourquoi faire des recommandations ?

Dans des domaines où les évolutions techniques sont très rapides et où des intérêts économiques forts sont en jeu, le conseil, la persuasion et l'autorité morale sont privilégiés dans un premier temps. En outre les recommandations adoptées par la CNIL ne le sont jamais sans concertation. Il s'agit d'un préalable indispensable à l'adoption de nos recommandations puisque celles-ci doivent être en prise directe avec les préoccupations des professionnels concernés mais également des consommateurs ou des usagers.

Pour les entreprises, la valeur ajoutée des recommandations est importante : elles peuvent devenir un véritable guide de bonnes pratiques. Le pari est fait que les recommandations de la CNIL seront utilisées par les entreprises pour réguler leurs pratiques et s'engager dans une véritable politique de la conformité.

Pourquoi une recommandation sur l'archivage électronique ?

La CNIL a fait un constat simple : de nombreuses bases de données d'archives ne répondent à aucun critère spécifique d'accès ou d'utilisation. Bien souvent, les données enregistrées dans un traitement, à l'occasion par exemple de la conclusion d'un contrat, sont librement accessibles jusqu'à effacement sans qu'il soit distingué entre la période d'exécution du contrat et la période d'archivage. Dans de nombreux cas, tout est fait pour que les informations collectées par l'entreprise, dont la valeur patrimoniale est forte, soient le plus librement accessibles tant que les informations ne sont pas effacées.

Du fait de la mémoire informatique, les individus peuvent ainsi devenir tout à fait et à jamais transparents à l'égard de leur employeur, de leur banque, de leur compagnie d'assurances ou de leur opérateur de télécommunications pour des durées pouvant atteindre plusieurs dizaines d'années. Ce « tout-savoir » peut ainsi, si l'on n'y prend garde, devenir un véritable livret social virtuel et, pour les plus démunis, un passeport pour l'exclusion.

Pourquoi la CNIL se mêle-t-elle des blogs ?

Pour être à la mode ! Non, ne croyez pas cela. En fait le sujet est sérieux. Chacun veut raconter sa vie mais en même temps raconte celle des autres. Dès lors, le contenu de certains blogs est susceptible de porter atteinte à la vie privée des personnes dont les informations peuvent être diffusées par des tiers, sans qu'elles en aient été informées. Dès lors, la Commission se doit de rappeler les règles issues de la loi « informatique et libertés » applicables à la création de sites web personnels afin que leur développement se fasse dans le respect de la vie privée des internautes.

C'est **plus net**

Favoriser un accès restreint…

Les sites personnels créés dans le cadre du cercle de famille ou d'amis devraient être restreints aux seules personnes identifiées par le responsable du site. Par exemple, lorsqu'un particulier souhaite créer un site qui diffuse les photographies prises à l'occasion d'un événement (mariage, anniversaire), il est important, compte tenu des risques de captation des données et de réutilisation de celles-ci, que soient mis en place des dispositifs permettant de limiter cette diffusion aux seules personnes concernées.

Comment diffuser en toute légalité des informations sur mes proches ?

La diffusion par internet d'informations sur des personnes nécessite le consentement préalable de celles-ci. Les données dites sensibles (par exemple, sur la santé ou les orientations sexuelles) n'ont pas vocation à être diffusées à partir d'un site internet ouvert au public.

Une attention particulière au bénéfice des mineurs…

Au regard des risques de captation d'images (photographies, vidéo) des mineurs, la CNIL préconise, ici aussi, la mise en place d'un accès restreint pour les sites personnels qui souhaiteraient diffuser ce type de données. En tout état de cause, la diffusion d'images de mineurs ne peut s'effectuer qu'avec leur accord et l'autorisation expresse des parents ou du responsable légal.

Est-ce que je peux collecter des informations à partir de mon site personnel ?

Oui, à condition que les personnes auprès desquelles sont recueillies les informations aient été informées de la finalité de cette collecte, des destinataires des données et de l'existence d'un droit d'accès, de rectification et d'opposition. La transmission des données collectées à des tiers ne peut se faire que dans le cadre d'activités privées, après que la personne concernée en ait été informée et ait pu s'y opposer.

Puis-je m'opposer à la diffusion d'informations me concernant sur un site blog et comment ?

Oui, à tout moment. Chacun dispose d'un droit d'accès, de modification, de rectification et de suppression des données qui le concernent. Pour faire valoir ces droits, il suffit de s'adresser au responsable du site ou directement à la personne en charge de ce droit d'accès.

La consultation de la CNIL sur les projets de loi

AUDITIONS PARLEMENTAIRES		
	Objet	**Date**
Assemblée nationale	Projet de loi de lutte contre le terrorisme	Audition par le rapporteur de la commission des lois le 7 novembre 2005
Assemblée nationale	Projet de loi de transposition de la directive droit d'auteur	Audition par le rapporteur de la commission des lois le 8 décembre 2005
Sénat	Mission sur la fraude documentaire	Audition le 15 mars 2005
Sénat	Commission d'enquête sur l'immigration clandestine	Audition le 21 décembre 2005
Sénat	Proposition de loi sur la récidive (bracelet électronique)	Audition par le rapporteur de la commission des lois le 11 octobre 2005
Sénat	Projet de loi de lutte contre le terrorisme	Audition par le rapporteur de la commission des lois le 22 novembre 2005
Sénat	Projet de loi de transposition de la directive droit d'auteur	Audition par le rapporteur de la commission des lois le 22 décembre 2005
Office parlementaire des choix scientifiques et technologiques	Étude sur la gouvernance de l'internet	Audition publique le 12 décembre 2005
Parlementaire en mission	Bracelet électronique	Audition le 16 mars 2005
Parlementaire en mission	Sécurité des systèmes d'information	Audition le 7 novembre 2005

La CNIL est consultée par le gouvernement sur les projets de loi relatifs à la protection des données, de fait il n'est guère de grands fichiers créés par la loi sans qu'elle n'ait au préalable donné son avis.

On peut regretter cependant que la CNIL soit parfois court-circuitée. Ainsi en 2005 des fichiers SALVAC et ANACRIM, concernant le recueil d'informations sur les crimes et délits graves aux fins d'identifier les criminels «en série». La CNIL avait demandé à plusieurs reprises au ministère de l'Intérieur à être saisie d'une demande d'avis concernant le fichier SALVAC. Or c'est par amendement du gouvernement à la proposition de loi relative au traitement de la récidive des infractions pénales que la légalisation de ces fichiers déjà en fonctionnement a été effectuée.

Au final, l'article 30 de la loi du 12 décembre 2005 crée un régime dérogatoire à celui défini par l'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure. Ainsi, un certain nombre de garanties applicables aux fichiers de police judiciaire ont été écartées par le législateur. Les conditions d'entrée dans le fichier, la définition des personnes concernées, les règles d'effacement sont en effet moins protectrices. Par exemple, le procureur de la République peut prescrire le maintien d'informations relatives à une victime qui s'y serait opposée quand bien même l'auteur des faits aurait été condamné.

La CNIL aura cependant une autre occasion de donner un avis : la durée de conservation des données, les modalités d'habilitation des personnels de la police et de la gendarmerie, ainsi que les conditions d'exercice du droit d'accès indirect aux deux fichiers seront définies par décret en Conseil d'État pris après avis de la CNIL.

Questions à …

Alex TÜRK

Sénateur du Nord
Président de la CNIL

Comme le tableau des auditions parlementaires le montre, nous avons été présents sur chacun des grands textes qui, cette année, ont eu un impact sur l'équilibre sécurité/liberté : projet de loi sur le terrorisme dont l'essentiel des dispositions tournait autour des traitements de données, proposition de loi sur la récidive avec une mesure-phare, le bracelet électronique, et projet relatif au droit d'auteur qui pose la question des limites de la surveillance de l'internet. Chacun jugera du bilan de l'intervention de la CNIL ou de ses membres. Pour ma part je dirais que la CNIL est souvent entendue mais pas toujours écoutée.

Au sujet de la proposition de loi sur la récidive précisément, la CNIL ne s'est pas positionnée officiellement. Pourquoi ?

Comme il s'agissait d'une proposition de loi, nous n'avons pas été consultés officiellement. Mais ce n'est pas la raison déterminante car dans d'autres cas nous n'hésitons pas à faire connaître notre avis même s'il ne nous a pas été demandé. En l'espèce, la Commission a choisi une approche plus informelle pour ne pas prendre parti dans le débat qui opposait l'Assemblée nationale et le Sénat. Patrick Delnatte, député, membre de la CNIL et moi-même avons reçu de nos collègues mandat pour veiller à ce que les préoccupations exprimées au cours des séances que la CNIL a consacrées, à chaque étape de la procédure parlementaire, à ce texte, soient prises en compte par les deux assemblées.

N'est-il pas particulièrement délicat d'être à la fois parlementaire et membre de la CNIL ?

L'expérience montre au contraire que le choix du législateur en 1978 de faire figurer deux députés et deux sénateurs parmi les membres de la CNIL a été très judicieux. L'action parlementaire n'est pas la partie la plus visible de mes fonctions bien que je ne m'interdise pas de déposer moi-même, comme Francis Delattre, Patrick Delnatte, députés ou Philippe Nogrix, sénateur, des amendements fortement inspirés par les prises de position de la CNIL ou de siéger dans les commissions mixtes paritaires. Elle n'en est pas moins réelle, constante et je le crois, pas sans résultats. Les contacts directs que je peux avoir avec un président de commission ou un rapporteur sont un atout important pour la défense des principes de la protection des données. Il est également, bien entendu, très important pour nous d'assurer une communication permanente avec les membres des Assemblées, indépendamment du dépôt de textes relatifs aux questions «informatiques et libertés» sur leur bureau. Le fait d'être membre de ces assemblées nous facilite la tâche.

LES CONTRÔLES

L'objectif premier était d'augmenter de manière significative le nombre de vérifications sur place effectuées. Qu'en est-il en 2005 ?

Les principaux secteurs d'activité contrôlés ont été, conformément au programme de contrôles adopté par la CNIL en séance plénière le 21 avril 2005 :
– la grande distribution (modalités du contrôle des paiements par chèque, tenue de fichiers de personnes surprises en flagrant délit de vol à l'étalage) ;
– le marketing direct (prises en compte des droits d'opposition des clients ou prospects, notamment internautes) ;
– la biométrie (contrôles d'accès sur les lieux de travail, à des clubs de sport, des chambres d'hôtel, etc.) ;
– la vidéosurveillance implantée dans des lieux privés ;
– le courtage d'assurance sur internet.

En outre, un audit des services de « banque en ligne » proposés par dix établissements bancaires importants a été réalisé au cours du premier semestre 2005 sur la base d'un questionnaire-type et a permis à la Commission de formuler des recommandations destinées tant aux établissements bancaires qu'aux internautes et de les diffuser sur son site internet.

Les contrôles 2005 en chiffres

- **104 missions de contrôle décidées par le président de la CNIL :**
  ▲ *une augmentation de 235% par rapport à 2004.*
- **96 contrôles effectués :**
  ▲ *une progression de 113% en un an.*
- **22% des contrôles réalisés font suite à des plaintes de particuliers.**
- **18 mises en demeure et 3 avertissements résultent des contrôles.**

Compte tenu des nouvelles modalités de contrôle prévues par la loi du 6 août 2004 et précisées par le décret d'application du 20 octobre 2005 dans le secteur de la santé (présence nécessaire d'un médecin pour accéder à des données médicales individuelles), aucune vérification n'a pu être effectuée dans ce secteur en 2005.

Environ 15% des suites à donner aux missions de contrôles sont examinées par la formation restreinte, compte tenu des manquements à la loi relevés lors des vérifications sur place. Dans les autres cas, un courrier est adressé au responsable de l'organisme contrôlé lui demandant, le plus souvent, de procéder à des modifications des applications mises en œuvre.

S'agissant des procédures, la CNIL n'a pas eu à faire usage des moyens prévus par la loi pour exercer pleinement ses pouvoirs de contrôle, aucun des responsables des organismes contrôlés ne s'étant opposé à l'accès de la délégation sur les lieux de mise en œuvre des traitements de données à caractère personnel ou à la communication de documents en invoquant un secret professionnel.

La Commission a, par deux fois, mis en application les dispositions de l'article 44-III de la loi du 6 janvier 1978 modifiée qui lui permettent de convoquer une personne pour recueillir tout renseignement utile.

Bon point !

Un contrôle opéré dans un seul établissement a eu des répercussions au sein de l'ensemble d'un groupe hôtelier international qui a adopté un plan d'action général destiné à garantir le respect de la loi « informatique et libertés ».

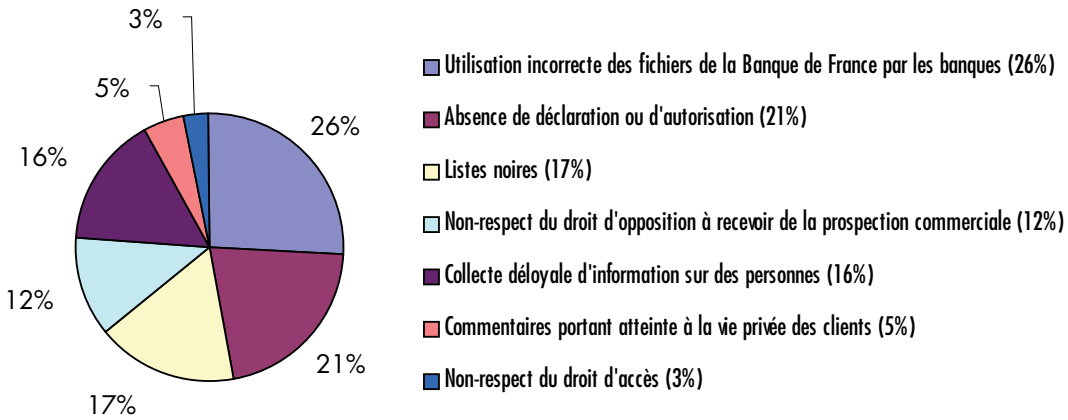
LES SANCTIONS

La loi du 6 août 2004 prévoit que la commission peut désormais, à l'issue d'une procédure contradictoire, décider de prononcer diverses mesures : un avertissement, une mise en demeure, une sanction pécuniaire, une injonction de cesser le traitement, etc. Il s'agit là d'un changement majeur dans les pouvoirs dont disposait jusqu'à présent la CNIL en la matière.

Autre nouveauté introduite par la nouvelle loi : certaines de ces mesures, parmi lesquelles la mise en demeure et la sanction pécuniaire, ne sont pas décidées par la formation plénière de la commission mais par une formation spécifique composée de six membres appelée «formation restreinte».

Cette formation se réunit au moins une fois par mois pour décider des mesures à prendre à l'égard des responsables de traitement qui ne respectent manifestement pas la loi «informatique et libertés». Les dossiers examinés font suite généralement à une mission de contrôle effectuée par la CNIL, à la réception de plaintes ou à toute situation dans laquelle la concertation n'a pas permis de rétablir une situation conforme sur le plan juridique.

Typologie des manquements à la loi relevés par la formation restreinte



MAUVAIS POINTS !

Secteur bancaire : un nombre record d'avertissements en 2005

Organismes concernés	Délibérations de la CNIL portant avertissement
Crédit Mutuel Sud-Est	Délibération 2005-043 du 9 mars 2005
Crédit Agricole Mutuel du Nord de la France	Délibération 2005-057 du 31 mars 2005
Credipar	Délibération 2005-059 du 31 mars 2005
Crédit Lyonnais	Délibération 2005-060 du 31 mars 2005
Crédit Agricole Mutuel du Gard	Délibération 2005-062 du 31 mars 2005
Caisse d'Épargne Ile-de-France Ouest	Délibération 2005-061 du 31 mars 2005
SOFINCO	Délibération 2005-075 du 10 mai 2005
Crédit Agricole de la Réunion	Délibération 2005-085 du 10 mai 2005
GE Money Bank	Délibération 2005-306 du 13 décembre 2005
Banque Populaire Val-de-France	Délibération 2005-307 du 13 décembre 2005

Gros plan sur ...

La formation restreinte et les sanctions

L'an I de la formation restreinte

Le nouveau pouvoir de sanction consacré par la loi du 6 août 2004 a nécessité de la part de la CNIL une adaptation de ses procédures afin d'assurer notamment le respect des droits de la défense. Cette adaptation s'est traduite par la modification à deux reprises des dispositions du règlement intérieur qui garantit aujourd'hui que toute décision de sanction est prise à la suite d'une procédure respectueuse des droits de la partie mise en cause. La première année de fonctionnement de la formation restreinte a été l'occasion, pour une large part, d'expérimenter les nouveaux mécanismes de sanction tant sur le plan des procédures que des dossiers à examiner. L'expérience acquise au cours de l'année 2005 et l'adoption du décret d'application devraient permettre d'engager la formation restreinte, au cours des prochains mois, dans une phase de montée en charge progressive de son activité.

Les types de dossiers présentés à la formation restreinte

En 2005, la formation restreinte s'est réunie huit fois et a examiné cinquante dossiers. Les dossiers examinés concernaient soit un manquement de fond à la loi (par exemple le non-respect des conditions d'inscription dans un fichier de la Banque de France, des difficultés pour exercer un droit d'accès ou d'opposition à recevoir de la prospection commerciale, l'existence de zones « bloc-notes » illicites, la mise en œuvre de fichiers d'infractions ou l'accès à des données par des tiers non autorisés), soit à un manquement de fond accompagné d'un manquement de procédure (absence de demande d'autorisation préalablement à la mise en œuvre de certains fichiers) soit encore à un manquement de procédure (non-réponse à des courriers de demande de compléments dans le cadre d'une procédure par exemple).

Les premières sanctions de la formation restreinte

Pour pouvoir infliger une sanction pécuniaire à un organisme, la loi fait obligation à la CNIL d'adresser au préalable une mise en demeure de faire cesser le manquement constaté. Ce n'est que lorsque la mise en demeure n'est pas suivie d'effets que la CNIL peut décider une sanction pécuniaire. En 2005, les trente-six mises en demeure adressées aux organismes mis en cause ont eu globalement un effet extrêmement dissuasif puisque plus de 85% d'entre elles ont permis de régulariser les manquements à la loi qui avaient été constatés. S'agissant des dossiers pour lesquels la mise en demeure n'a pas été efficace, et dont certains sont actuellement en cours d'instruction, la sanction pécuniaire n'est pas la réponse unique. En effet la formation restreinte a pu juger, en opportunité, que d'autres sanctions comme l'injonction de cesser la mise en œuvre d'un traitement ou l'avertissement rendu public étaient plus adaptées. On peut néanmoins supposer que l'augmentation mécanique du nombre des dossiers qui seront examinés par la formation restreinte en 2006 permettra d'utiliser l'ensemble des sanctions prévues dans la loi. Enfin, il convient de bien comprendre qu'une décision de sanction est le résultat d'une procédure complexe qui mobilise souvent l'ensemble des services de la CNIL (direction juridique, service des contrôles, expertise informatique) et qui nécessite donc des moyens humains très importants. Dans ce domaine, les résultats de la formation restreinte seront donc aussi conditionnés par les moyens qui seront donnés à la CNIL pour exercer pleinement ses nouvelles missions.

LES TRANSFERTS INTERNATIONAUX DE DONNÉES

La loi du 6 août 2004 donne à la CNIL un pouvoir d'autoriser les transferts internationaux de données vers des pays n'appartenant pas à l'Union européenne. La CNIL s'est tout d'abord attachée à élaborer une doctrine forte en la matière, s'appuyant sur celle élaborée antérieurement à la loi du 6 août 2004, et articulant de manière cohérente les différentes conditions auxquelles de tels transferts internationaux de données sont possibles.

Au titre des exemples marquants de travaux en la matière, la CNIL a accepté, le 30 juin 2005, que les « règles internes contraignantes » du groupe General Electric puissent être valablement utilisées pour encadrer les nombreux transferts internationaux de données que ce groupe opère en son sein, notamment pour des finalités de gestion des ressources humaines. De manière plus générale, elle a collaboré avec ses homologues européens pour faire avancer plusieurs dossiers de même nature, afin d'asseoir la légitimité des règles internes au plan européen et de les promouvoir auprès des entreprises concernées.

La CNIL a également joué un rôle essentiel dans l'adoption, en décembre 2005, d'un important document de travail du groupe de l'article 29 en la matière, donnant une interprétation commune de ce que l'on appelle les « dérogations de l'article 26-1 » de la directive 95/46/CE du 24 octobre 1995.

Elle a également travaillé sur les conditions de procédure et les formalités applicables aux transferts internationaux de données au niveau national. Elle a ainsi élaboré la procédure d'autorisation de transfert dont elle a été investie par la loi du 6 janvier 1978 modifiée. Elle a également tenu compte de ces questions de manière pragmatique en élargissant, le 17 novembre 2005, le champ d'application des deux normes simplifiées les plus utilisées par les entreprises, relatives à la gestion des salariés et des clients, pour y inclure, à certaines conditions, les transferts internationaux de données vers des pays n'assurant pas un niveau de protection adéquat.

Questions à …

Georges de LA LOYÈRE

Membre du Conseil économique et social
Commissaire en charge des « Affaires internationales »

Qu'est-ce qu'un transfert international de données ?

Les transferts internationaux de données sont une réalité incontournable de la vie des entreprises, notamment multinationales. Ils recouvrent des démarches très différentes : centralisation des bases de données de gestion des ressources humaines des groupes multinationaux ; mise en commun de services informatiques au sein de ces groupes ; recours à des prestataires étrangers pour des services de maintenance informatique à distance, pour la gestion de centres d'appel, l'externalisation de certaines fonctions, etc.

Pourquoi encadrer les transferts internationaux de données ?

Les données transférées seront traitées hors de France, voire hors de l'Union européenne, y compris dans des pays n'accordant pas nécessairement de protection similaire à celle accordée par les règles françaises et européennes de protection des données. Dans de tels cas, il faut s'assurer que le destinataire traitera ces données correctement, que leur sécurité sera assurée, que les personnes concernées pourront toujours exercer leurs droits, etc. L'entreprise qui est responsable de ce transfert doit s'assurer que les données transférées seront traitées dans des conditions similaires à celles qui s'appliqueraient en France.

Que prévoit la loi d'août 2004 sur les transferts ?

La loi « informatique et libertés » comporte des dispositions spécifiques encadrant les transferts vers de tels pays. Ces dispositions prévoient que de tels transferts sont possibles, mais les soumet à un certain nombre de conditions alternatives ou cumulatives :

– protection « adéquate » dans le pays destinataire ;
– transfert vers une entreprise américaine adhérente au *Safe Harbor* ;
– conclusion d'un contrat spécifique entre l'entreprise française et le destinataire ;
– autorisation par la CNIL, etc.

Un guide pratique élaboré sur ces questions est disponible sur le site de la CNIL.

L'HOMO INFORMATICUS EN 2005

entre servitude et liberté

L'HOMO INFORMATICUS TRACÉ

LES TRACES ACTIVES

Questions à …

Philippe LEMOINE

Président-directeur général de Laser et de COFINOGA

Commissaire en charge du secteur « Technologie »

Une situation nouvelle d'activation des traces est-elle en train d'apparaître ?

Oui et celle-ci se situe au carrefour de la sophistication des architectures de réseaux d'une part et d'autre part de la diversification des catégories d'objets tracés : outils communicants, objets passifs de consommation, titres d'identité et de service. Le corps humain lui-même peut, avec la biométrie, devenir un objet tracé.

Deux modèles d'architecture, toutes deux d'origine militaire, peuvent illustrer cette sophistication :
– une architecture provenant des années 1980 : les réseaux de télécommunications mobiles cellulaires de type GSM encore assez centralisés ;
– une architecture des années 2000 : les réseaux maillés de type *mesh networking* (réseaux *ad hoc*), appliquant les principes du P2P (*peer to peer*) à la gestion des infrastructures et pouvant gérer un nombre bien plus important de capteurs.

Ces architectures permettent un pistage permanent d'objets sinon de personnes en temps réel.

Parallèlement à la vulgarisation des terminaux de communication (voix, donnée) actifs par nature, de nombreux objets identifiants passifs sont apparus et continueront d'apparaître. On compte parmi ces objets qui prennent leur valeur identifiante dans un contexte particulier : les objets de consommation radio-identifiés par EPC (*Electronic Product Code*) mais aussi les titres de transport et d'accès d'entreprise et les titres personnels d'identité électronique. Ainsi, ces objets sont pris nécessairement dans un maillage fin et diffus d'un réseau de capteurs et de lecteurs. Les capacités techniques des supports comme leur coût ont évolué considérablement et continueront encore à le faire. Elles induisent un mode de gestion par archivage extensif et illimité.

Les développements techniques sont-ils seuls en cause ?

Le contexte politicojuridique s'est lui aussi métamorphosé particulièrement depuis septembre 2001. En raison notamment de la montée des enjeux de sécurité, les initiatives en matière de grands systèmes d'information se sont déplacées, passant de la technostructure à l'échelon politique proprement dit. Par exemple, les opérateurs se voient imposer des durées de conservation des données de connexion allant au-delà de leurs besoins propres.

Un élément venant encore compliquer l'analyse est que ce domaine est l'un des très rares, dans les technologies de l'information, où la France dispose d'atouts industriels. La France est pourtant le pays informatique et libertés, avant d'être le pays de l'électronique de sécurité.

De cette double évolution naît un risque : celui de voir la problématique informatique et libertés prise en tenaille entre une informatisation « par en bas » plus ou moins dérégulée et une informatisation « par en haut » décidée par des textes juridiques de rang équivalent à la loi de 1978 rénovée. L'ensemble formant le paysage des « traces actives ».

Selon vous, quelles sont les voies pour assurer l'équilibre informatique et libertés ?

D'abord des précautions en cas de sortie possible du régime d'État de droit : ainsi la CNIL pourrait recourir à certains pouvoirs qui lui sont reconnus par la loi, notamment celui d'ordonner la destruction d'un système d'information autorisé en temps normal.

Mais il ne faut pas perdre de vue que les mémoires des objets eux-mêmes passifs ou non peuvent contenir les éléments d'information permettant un contrôle excessif. On peut également limiter l'accès à ces données (ce qui est par exemple souhaitable pour la carte d'identité). Le principe du droit d'opposition devrait impliquer des dispositifs d'activation/désactivation simples à mettre à disposition des individus.

Une application très ferme du principe de finalité s'impose. Si des applications informatiques omniprésentes (on dit aussi *pervasives*) se développent, c'est dans des finalités bien déterminées et non pour recueillir des données qui seront utilisées dans des logiques de sécurité.

À l'inverse, si une préoccupation de sécurité fait l'objet d'une loi forte et cohérente, ceci devrait être suffisant et interdire l'emploi adjacent de « bretelles » informatiques diverses. Il faudrait faire également en sorte, notamment en matière biométrique que la CNIL intervienne sur les projets ou les propositions de loi.

LA GÉOLOCALISATION PERMANENTE DES ASSURÉS : LE COUP DE FREIN DE LA CNIL !

La CNIL a été saisie d'un projet concernant une nouvelle offre d'assurance automobile à destination des jeunes conducteurs qui y auraient volontairement souscrit. Cette nouvelle offre repose principalement sur l'engagement du jeune conducteur à respecter un certain nombre de règles parmi lesquelles figurent le respect des limitations de vitesse et un temps de conduite limité.

Afin de vérifier le respect de ces engagements pouvant conduire à une baisse de la surprime appliquée aux jeunes conducteurs, la compagnie d'assurance entendait demander aux assurés d'équiper leur véhicule d'un dispositif de géolocalisation de type GPS-GSM. Ce dispositif, en collectant les informations relatives aux déplacements du véhicule toutes les deux minutes, aurait permis à la compagnie d'assurance de déterminer la localisation du véhicule, les vitesses pratiquées, le type de route sur lequel roule le véhicule ainsi que les horaires et les durées de conduite. Pour bénéficier de la baisse de la surprime, le jeune conducteur s'engageait notamment à ne pas prendre le volant dans les nuits du samedi, dimanche et jours fériés entre 2 heures et 6 heures du matin.

Si la Commission ne peut évidemment qu'être favorable à la mise en œuvre d'actions visant à développer la prévention routière, il lui appartient de vérifier la conformité à la loi des traitements qui lui sont présentés. Au cas présent, la Commission a refusé la mise en œuvre du dispositif présenté au regard de ses caractéristiques (délibération n° 2005-278 du 17 novembre 2005).

En effet, la mise en œuvre d'un traitement permettant d'enregistrer l'intégralité des déplacements effectués par les assurés ne répond pas à l'exigence de proportionnalité posée par la loi et portait une atteinte excessive à la liberté d'aller et venir anonymement.

En outre, la Commission a estimé que le traitement, ayant notamment pour finalité de collecter de manière systématique les vitesses maximales et de détecter les éventuels dépassements des limitations de vitesse constituait un traitement portant sur des données relatives aux infractions. La Commission a, dès lors, rappelé les dispositions de l'article 9 de la loi du 6 janvier 1978 modifiée qui interdisent à des personnes privées la mise en œuvre de tels traitements.

Le fait que la compagnie d'assurance ne soit pas directement destinataire des informations issues du système de géolocalisation - celles-ci sont stockées chez un prestataire technique - n'influe pas sur la qualité de responsable de traitement de la compagnie d'assurance sur laquelle incombe l'obligation de respecter les dispositions de la loi du 6 janvier 1978 modifiée en août 2004.

Cette décision s'inscrit dans la réflexion globale menée par la Commission relative au développement des dispositifs de géolocalisation au regard du respect de la vie privée et des libertés des personnes.

Questions à …

Didier GASSE

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

En quoi la géolocalisation des véhicules pose-t-elle aujourd'hui un problème ?

De nombreux dispositifs de géolocalisation des véhicules sont aujourd'hui mis en œuvre, telles que la géolocalisation par l'intermédiaire du GPS permettant de fournir aux conducteurs une aide à la navigation, voire de recevoir une assistance en cas de panne ou d'accident, ou de retrouver un véhicule en cas de vol. Ces applications ne posent pas de problèmes particuliers en termes « informatique et libertés ». Mais, qui dit géolocalisation des véhicules dit géolocalisation des conducteurs et traitement éventuel de tous leurs déplacements. Or, dans le cas des salariés[1] ou des assurés, ce n'est pas le conducteur qui a recours à la géolocalisation, mais son employeur ou son assureur. Il ne s'agit plus d'une géolocalisation voulue mais d'une géolocalisation subie.

En quoi les données de géolocalisation sont-elles des données sensibles ?

Au-delà de la simple localisation d'une personne à un moment donné, les traitements de géolocalisation renseignent sur l'activité même de cette personne. Où va-t-elle ? Pour combien de temps ? À quelle fréquence ? Une des libertés que la CNIL s'attache à faire respecter est précisément la liberté d'aller et venir de façon anonyme dans tous les cas où cela est possible. C'est pourquoi, dans le cas d'une géolocalisation permanente de tous les déplacements de l'assuré par sa compagnie d'assurance, la CNIL a considéré que le seul contrôle du respect des engagements pris par l'assuré ne pouvait justifier une telle surveillance. C'est une question de proportionnalité.

Pourtant le système proposé n'était-il pas fondé sur le volontariat de l'assuré ?

C'est exact, mais vous remarquerez que, dans ce cas, l'assuré est volontaire avant tout pour obtenir des réductions de primes… On peut d'ailleurs facilement imaginer que l'ensemble des assurances propose un système équivalent, puis l'étendent ensuite progressivement des jeunes à l'ensemble des conducteurs. En l'espèce, la Commission a aussi retenu l'argument selon lequel la loi réserve à des personnes publiques la possibilité de tenir des fichiers d'infractions en ce qui concerne les excès de vitesse. Ce dossier pose clairement la question des possibilités infinies que vont donner les développements technologiques pour mieux contrôler nos comportements. Toute la question est de savoir où il faut s'arrêter.

1. Par ailleurs évoqué au chapitre 5 du présent rapport.

L'HOMO INFORMATICUS ADMINISTRÉ À DISTANCE

L'année 2005 a été marquée par la définition d'un cadre juridique nouveau pour les échanges électroniques entre administrations et administrés au travers de l'ordonnance du 8 décembre 2005 et par le lancement en grandeur réelle ou sous forme expérimentale de plusieurs téléservices.

Un nouveau cadre juridique : l'ordonnance « téléservices » du 8 décembre 2005

L'ordonnance du 8 décembre 2005[5] a donné un cadre juridique à la création des téléservices. Elle définit les conditions des échanges dématérialisés entre les « autorités administratives » (administrations de l'État, collectivités territoriales, organismes chargés de la gestion d'un service public administratif…) et les citoyens, ainsi qu'entre les administrations elles-mêmes.

Comme la CNIL l'a souligné, dans son avis du 22 novembre 2005[6], ce cadre est d'autant plus utile qu'il fait référence explicitement aux règles de la loi du 6 janvier 1978 modifiée. Toutefois une interrogation demeure sur la question du consentement de l'usager à la transmission des informations le concernant.

L'article 6 de l'ordonnance prévoit que lorsqu'une disposition législative ou réglementaire rend nécessaire qu'une administration demande à un usager une information émanant d'une autre administration, cette information, dès l'instant où elle contient des données à caractère personnel, pourra lui être transmise par voie électronique par une administration la détenant déjà à condition que l'usager l'ait expressément autorisé. La CNIL a considéré que cette disposition était protectrice, par principe, de l'usager même si ce consentement peut parfois paraître théorique quand il est lié à une demande de prestation. Mais le deuxième alinéa du même article 6 dispose que l'autorisation de l'usager « *n'est pas nécessaire lorsque l'autorité administrative est habilitée par une disposition législative ou réglementaire à obtenir, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, la transmission de l'information* ». Cette disposition peut concerner des échanges divers d'informations entre autorités administratives alors même que la loi du 9 décembre 2004 n'habilite le gouvernement à agir par ordonnance pour créer des échanges entre les autorités administratives que dans le cadre des « procédures de contrôle ». La CNIL avait demandé, sans succès, qu'il ne soit fait référence qu'aux procédures de contrôle pour les échanges entre administrations sans consentement de la personne.

Premiers téléservices de l'administration électronique

Dans son avis du 30 avril 2005[7], la CNIL a examiné le service en ligne de changement d'adresse développé par l'ADAE (Agence pour le développement de l'administration électronique). Il permet à toute personne qui le souhaite de transmettre sa nouvelle adresse aux organismes publics ou privés qu'elle désigne.

Un autre téléservice de l'ADAE, dont le lancement est imminent, a été examiné par la CNIL[8]. Il s'agit du portail national de demande d'extrait d'acte de naissance qui est

5. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
6. Délibération n° 2005-280 du 22 novembre 2005 portant avis sur le projet d'ordonnance relatif aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
7. Délibération n° 2005-54 du 30 mars 2005 portant avis sur le projet d'ordonnance relatif au service public du changement d'adresse, sur le projet de décret pris en application de l'ordonnance relative au service de changement d'adresse et sur le projet d'arrêté du Premier ministre créant un traitement de données à caractère personnel mettant en place le téléservice « mon changement d'adresse ».
8. Délibération n°2005-183 du 5 juillet 2005 portant avis sur le projet d'arrêté du Premier ministre créant un traitement de données à caractère personnel mettant en place le téléservice « demande d'acte de naissance ».

Isabelle FALQUE-PIERROTIN

Conseiller d'État
Commissaire en charge du secteur « Libertés publiques »
Présidente du groupe de travail sur l'administration électronique

Le changement d'adresse en ligne pose t-il des problèmes particuliers au regard de la loi « informatique et libertés » ?

Ce nouveau téléservice est une avancée majeure pour simplifier la vie des six millions de personnes qui déménagent chaque année. La CNIL a été associée à la conception de manière à éviter certains écueils. Ainsi il aurait pu servir à constituer progressivement un fichier national de domiciliation qui n'existe pas en France et qui est étranger à nos traditions, hors le cas de l'Alsace-Moselle. Ce n'est pas le cas et nous y avons veillé. Autre point fondamental qui est d'ailleurs lié au premier : l'inscription à ce service et la décision de transmettre à une autorité administrative ou un partenaire privé les informations relatives au changement d'adresse relèvent de la seule volonté de l'usager.

Ce principe de la liberté de l'usager non seulement d'avoir recours ou non au service mais surtout de l'utiliser « à la carte » se retrouve aussi dans le portail « monservice public ». Sur ce portail chacun pourra sélectionner les administrations avec lesquelles il souhaitera communiquer par téléprocédure. De même il est satisfaisant pour la CNIL que l'espace de stockage de dossiers et données personnels ne puisse être utilisé par les administrations pour échanger entre elles des documents qu'avec le consentement de l'usager.

À travers ces téléservices se pose la question de l'identification de l'usager ?

En ce qui concerne le changement d'adresse, opération ponctuelle qui ne nécessite qu'un compte temporaire mais qui peut, en cas d'accès non autorisé, avoir des conséquences fâcheuses, nous avons demandé que l'accès à ce service bénéficie à l'avenir d'une procédure d'authentification forte de l'usager quand il modifie son dossier. Cette authentification est, en effet, assurée actuellement par la saisie d'un numéro de dossier et d'un mot de passe. Un système de certificat électronique ou de signature électronique serait souhaitable lors de la prochaine évolution du dispositif.

La question de l'identifiant est d'une toute autre nature pour « monservicepublic » puisque le portail rassemble diverses administrations et pourrait conduire logiquement à un matricule administratif unique. La solution de « fédération d'identités » retenue par l'ADAE répond aux principes posés par la CNIL. L'usager qui s'authentifiera, par un identifiant sectoriel, sur un des sites partenaires du portail pourra demander à bénéficier d'une authentification unique pour accéder à d'autres téléprocédures en reliant entre elles, par le biais du compte « monservicepublic », ses différentes identifications sectorielles. La CNIL a pris acte que le numéro permettant de relier les sites partenaires choisis par l'usager ne conduira pas le portail « monservicepublic » à avoir accès aux identifiants sectoriels de l'usager. Ce numéro n'aboutira donc pas à un regroupement d'identifiants sectoriels autour d'un identifiant commun.

Pourquoi la CNIL a t-elle exprimé des réserves à l'égard du portail « demandes d'acte de naissance » ?

Il n'y a pas de question de principe en jeu puisqu'il s'agit d'un téléservice facultatif et qui n'a d'autre fonction que de simplifier les démarches administratives. Mais cette simplification a comme effet d'encourager une certaine forme de bureaucratie. Le décret du 26 décembre 2000 prévoit que la production du livret de famille ou de sa photocopie remplace la production d'un extrait d'acte de naissance. Malgré cette disposition claire, de nombreux organismes continuent de demander la production systématique d'un extrait d'acte de naissance. C'est pourquoi la CNIL a demandé à l'ADAE de diffuser sur le site internet du téléservice la liste des organismes seuls habilités à demander une copie intégrale ou un extrait d'acte de naissance.

un téléservice facultatif destiné à faciliter les démarches des usagers. Il est non exclusif de tout autre moyen de demander un acte de l'état civil directement aux communes ou aux autorités habilitées à délivrer les actes.

Le 8 décembre 2005[9], enfin, la CNIL s'est prononcée sur une première version du portail « monservicepublic » mis en place par l'ADAE. Ce portail, mis en œuvre à titre expérimental pour une durée d'un an, permettra aux usagers, à partir d'un point d'entrée unique et d'une seule authentification, d'accéder à ses comptes personnels dans différentes administrations. L'usager qui s'authentifiera, par un identifiant sectoriel, sur un des sites partenaires du portail pourra demander à bénéficier d'une authentification unique pour accéder à d'autres téléprocédures en reliant entre elles, par le biais du compte « monservicepublic », ses différentes identifications sectorielles.

Le portail assurera également le stockage sur un espace dédié de ses dossiers et données personnels qui aura pour fonctions, à la fois de permettre de stocker des données à caractère personnel qui serviront à compléter de façon automatique des formulaires en ligne et aussi, de comporter une partie contenant des pièces justificatives pouvant être envoyées par l'usager lorsque cela est nécessaire.

9. Délibération n° 2005-304 du 8 décembre 2005 portant avis sur le projet d'arrêté présenté par l'agence pour le développement de l'administration électronique, et créant le téléservice « monservicepublic.fr ».

Les télédéclarations de revenus

Pour la cinquième année consécutive, les contribuables ont eu la faculté de déclarer leurs revenus en ligne, via internet. Cette télédéclaration est désormais sécurisée grâce à la délivrance gratuite par l'administration, après identification et choix d'un mot de passe par le contribuable, d'un certificat électronique personnalisé et réutilisable, permettant le cryptage des informations transmises et la signature électronique de la télédéclaration. Tout contribuable, muni de son certificat électronique, qu'il ait ou non utilisé la télédéclaration, se voit en même temps proposer l'accès en ligne à son dossier fiscal, contenant ses déclarations et avis d'imposition, demain la mention de ses paiements, à terme celles de ses démarches. Une administration plus accessible et plus transparente, c'est un progrès, mais celui-ci ne saurait se payer d'un recul sur un autre plan, celui de la confidentialité, autrement dit du respect du à la vie privée des contribuables. Ainsi la CNIL a constaté que la procédure de télédéclaration pouvait conduire à ce que les noms des organismes bénéficiaires de dons, legs ou cotisations fassent l'objet d'un enregistrement informatique, alors qu'ils figurent seulement sur les justificatifs joints aux déclarations papier. Elle l'a admis parce que la non-transmission des pièces justificatives facilite la vie des contribuables. Mais elle a demandé et obtenu que ces informations soient effacées aussitôt après vérification et, au plus tard, à l'expiration d'un délai de six mois.

Les cartes de vie quotidienne

L'ADAE a décidé de financer, sous cette appellation de « carte de vie quotidienne », une quinzaine de projets en France. Les premières expériences ont commencé début 2004 même s'il faut noter que les cartes de ville existent depuis de nombreuses années déjà.

Questions à …

Jean-Marie COTTERET

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

En quoi la CNIL est-elle concernée par les cartes de vie quotidienne ?

Les questions « informatique et libertés » soulevées par ces projets sont nombreuses : la question de l'identifiant utilisé, de son caractère signifiant et de son stockage soit sur la carte soit dans une base de données (soit encore dans les deux) ; la centralisation de toutes les données d'une personne ou d'une famille en une base de données unique au sein d'une mairie ; la création par ce biais de fichiers de population là où jusqu'alors les fichiers étaient différents selon l'application (inscription scolaire, état civil, centres de loisirs…). Ces projets de cartes amènent aussi à s'interroger sur la coexistence de données d'informations de nature différentes (services municipaux et services privés) et sur la nécessité d'avoir des accès bien limités. La durée de conservation (traçage, notamment pour les cartes de transport), les sécurités des systèmes et diverses particularités (utilisation de la carte Vitale ; dispositif de vote électronique) sont autant de points que la CNIL doit examiner.

Pouvez-vous citer un exemple récent de carte de vie quotidienne examinée par la CNIL ?

Le 21 avril 2005, la CNIL a rendu un avis sur la carte de vie quotidienne du conseil général du Val-d'Oise[1]. Le dispositif concerne quelques classes dans différents établissements de quatre communes tests. Il est proposé aux parents des élèves concernés une carte à puce pour accéder à des bornes, des cartes sans contact pour les enfants déjeunant à la cantine et un ensemble de téléservices. Les parents peuvent effectuer une pré-inscription pour les enfants de maternelle et de primaire ou une demande d'inscription à la cantine ou aux activités péri-scolaires. Un espace personnel, accessible par internet, permet aux parents de consulter la liste les démarches effectuées, les données du foyer, de déposer et stocker des justificatifs nécessaires aux démarches administratives, de consulter les consommations de certains services et de les payer. Il s'agit d'un projet soucieux du respect des données personnelles auquel la CNIL a été associée très en amont ce qui a permis de prendre en compte ses remarques très tôt.

Quels sont les points sur lesquels la CNIL a insisté ?

La CNIL a insisté, compte tenu des nombreuses informations collectées, sur la nécessité qu'elles soient toujours pertinentes au regard des finalités poursuivies. Par exemple, là où le conseil général avait créé une rubrique « carnet de santé », la CNIL a demandé qu'elle soit remplacée par les seules informations effectivement recueillies à savoir les vaccinations et les allergies. Elle a aussi considéré que le recueil de la nationalité était excessif en l'espèce. La CNIL a été aussi vigilante sur la durée de conservation des données qui correspond donc à la période d'activité du dossier de la famille plus un an. Sur les mesures de sécurité, la CNIL a remarqué que le système développé conduisait à juxtaposer deux systèmes d'authentification (carte à puce d'une part et couple identifiant/mot de passe, d'autre part). Elle a, logiquement, recommandé au conseil général de rechercher une harmonisation de ses solutions d'accès tout en maintenant un haut niveau de sécurité.

1. Délibération n° 2005-074 du 21 avril 2005 portant avis sur le projet d'arrêté du conseil général du Val-d'Oise créant un traitement de données à caractère personnel mettant en place la carte de vie quotidienne « Cartevaloise ».

L'HOMO INFORMATICUS BIOMAÎTRISÉ

Consciente des risques potentiels d'atteinte aux libertés individuelles et des enjeux de société que comporte le développement de ces techniques, la CNIL considère que de telles données doivent faire l'objet d'une protection particulière. C'est cette même approche qui a conduit le législateur, lors de la refonte de la loi « informatique et libertés » en août 2004, à décider que les traitements de données biométriques devaient désormais être autorisés par la CNIL. Ceci ne s'applique cependant pas aux traitements mis en œuvre pour le compte de l'État, qui eux sont soumis à avis préalable de la CNIL. Par exemple, la CNIL devrait prochainement être saisie du projet de carte d'identité électronique susceptible de comporter la photographie et les empreintes digitales des personnes.

D'une manière générale, le nombre toujours croissant de demandes d'autorisation, présentées par les entreprises, les collectivités locales ou les établissements publics, amène à constater une réelle banalisation de la biométrie. Au fil des avis et des autorisations rendus sur les projets dont elle a été saisie, la CNIL a peu à peu dégagé une grille d'analyse reposant sur des critères permettant d'apprécier la conformité des dispositifs au regard des principes relatifs à la protection des données.

Le premier de ces critères est la prise en considération du type de biométrie. En effet, les diverses caractéristiques biométriques utilisables aujourd'hui peuvent être classées en deux groupes : les biométries portant sur des éléments traçables dites « à trace » et les biométries ne portant pas sur des éléments traçables dites « sans traces ». Cette distinction repose sur la possibilité ou non de récupérer une donnée biométrique à l'insu de la personne. Parmi les caractéristiques « à trace » figurent les empreintes digitales (chaque objet touché garde la trace de nos empreintes digitales, trace qui peut être collectée à notre insu). *A contrario*, il existe des biométries qui en l'état actuel de nos connaissances sont « sans traces », tels que la rétine ou le contour de la main.

Partant de ce constat, la CNIL considère que la reconnaissance du contour de la main est une biométrie qui ne soulève pas de difficultés au regard des règles de protection des données. Elle ne peut pas être utilisée à d'autres fins, à l'insu de la personne. Dès lors, la CNIL a adopté une position souple quant à ses modes d'usage. Elle a ainsi autorisé à plusieurs reprises des établissements scolaires à utiliser un dispositif de reconnaissance du contour de la main dans le cadre du contrôle de l'accès à la cantine.

Qu'est-ce que c'est ?

La biométrie

La biométrie est l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales…). Elles se rapprochent ainsi de ce qui pourrait être défini comme un « identificateur unique universel », permettant de fait le traçage des individus.

Le second critère consiste, dès lors que l'on est en présence d'une biométrie à trace, à mettre en relation le mode de stockage des données (dans un fichier ou un support individuel) avec l'existence ou non d'un impératif particulier de sécurité. À titre d'exemple, on peut citer une expérimentation présentée par les ministères de l'Intérieur et de la Défense et dont l'objet était notamment de mesurer les gains de temps que la biométrie est susceptible d'apporter en permettant l'automatisation du contrôle du passage aux frontières. Cette expérimentation, dénommée « PEGASE », se déroule pendant un an à l'aéroport Roissy-Charles-de-Gaulle et repose sur la reconnaissance des empreintes digitales des voyageurs volontaires.

Dans son avis du 10 février 2005, la CNIL a souligné le caractère facultatif et expérimental du dispositif mais a cependant rappelé que le traitement, sous une forme automatisée et centralisée des empreintes digitales, ne peut être admis, compte tenu à la fois des caractéristiques de l'élément d'identification physique retenu, des usages possibles de ces traitements et des risques d'atteintes graves à la vie privée et aux libertés individuelles en résultant, que dans la mesure où des exigences impérieuses en matière de sécurité ou d'ordre public le justifient.

À cette occasion la CNIL avait également alerté le Gouvernement sur la possibilité de stocker les données biométriques dans un support individuel. En effet, en présence d'un impératif de sécurité moindre, la mise en œuvre du dispositif reste acceptable dès lors que les données sont stockées sur un support individuel.

La CNIL a ainsi autorisé le 22 septembre 2005, la société Bloomberg à mettre en œuvre un dispositif biométrique dont l'objet est de garantir que les personnes se connectant à son service d'informations financières sont bien des utilisateurs légitimes. Ce dispositif, mis en œuvre à des fins de sécurité, repose sur l'enregistrement de l'empreinte digitale dans un support individuel exclusivement détenu par l'utilisateur, ce qui permet de garantir aux personnes concernées le contrôle sur leurs données biométriques et d'éviter qu'elles ne soient utilisées à d'autres fins.

Cette analyse a également été retenue dans le cadre du contrôle d'accès des salariés à des locaux sécurisés de la Poste, aux zones d'accès contrôlés des aéroports ainsi que pour la sécurisation des accès à des systèmes informatiques.

Enfin, dans l'hypothèse d'un recours à une biométrie à traces avec stockage sur un support individuel mais en l'absence d'un impératif de sécurité, un dernier critère est pris en considération : le caractère facultatif du dispositif. Outre l'existence d'un stockage sur un support individuel, c'est le fait que seules les données des personnes volontaires fassent l'objet d'un traitement qui a décidé la CNIL à autoriser la chambre de commerce de Nice-Côte d'Azur à utiliser depuis 2005 une carte de fidélité comprenant un système de reconnaissance de l'empreinte digitale des voyageurs.

La CNIL rappelle

Les dispositifs biométriques, parce qu'ils visent à identifier un individu non plus seulement par son état civil et le document qui en atteste, mais aussi et surtout par ses caractéristiques physiques, soulèvent des questions de société qui, avant tout choix politique quant à une utilisation généralisée, doivent être bien appréhendées à travers une évaluation des avantages et des risques qu'ils comportent.

Questions à …

Guy ROSIER

Conseiller maître honoraire à la Cour des comptes
Commissaire en charge du secteur « Affaires économiques »

En quoi l'autorisation de la CNIL portant sur la carte de fidélité biométrique de la chambre de commerce de Nice-Côte d'Azur est-elle novatrice ?

C'est la première fois que la CNIL autorise le recours à un dispositif biométrique reposant sur la reconnaissance des empreintes digitales à destination du grand public et en l'absence d'impératif de sécurité, ces données biométriques étant stockées sur une carte à puce individuelle, sans base centrale. Le dispositif en question a essentiellement pour objet de « faciliter la vie » des personnes. C'est ce que l'on pourrait appeler de la « biométrie de confort », on supprime la contrainte liée à la mémorisation d'un énième mot de passe.

En l'espèce, il s'agit d'identifier les voyageurs réguliers de l'aéroport de Nice détenteurs d'une carte de fidélité lorsqu'ils accèdent aux services spécifiques suivants :
– l'accès à des zones de stationnement réservées ;
– la possibilité de profiter d'un système de « coupe-file » afin de ne pas attendre pour accéder à la salle d'embarquement ;
– l'envoi par SMS d'informations sur les vols ;
– l'opportunité de bénéficier de réductions tarifaires sur des biens et des services.

Quelles sont les caractéristiques techniques du dispositif mis en œuvre ?

La particularité du dispositif réside dans le fait que l'accès aux services proposés au titre du programme de fidélité s'effectue grâce à une carte à puce comportant l'empreinte digitale du titulaire de la carte. Lorsqu'elles veulent accéder aux services précédemment listés, les personnes doivent introduire leur carte dans une des bornes prévues à cet effet dans l'enceinte de l'aéroport de Nice. Le traitement effectué à cette occasion consiste en une comparaison entre le doigt apposé sur le lecteur de la borne et l'empreinte digitale stockée dans la puce de la carte. Il s'agit de contrôler que la personne en possession de la carte en est bien le titulaire légitime.

Sur quels critères ce système a t-il été autorisé ?

La CNIL a autorisé la mise en œuvre de ce procédé dans la mesure où en l'espèce, seules les données à caractère personnel des personnes volontaires sont traitées et l'empreinte digitale est uniquement stockée dans un support individuel exclusivement détenu par la personne concernée (en l'espèce la carte de fidélité) et dont elle décide librement de l'utilisation.

Dans ces conditions, la CNIL a considéré que le dispositif soumis par la chambre de commerce et d'industrie de Nice-Côte d'Azur ne comportait pas de risques particuliers pour la protection des libertés et des droits fondamentaux de la personne.

TEMPS FORTS DE L'ANNÉE 2005

LA LUTTE CONTRE LE TERRORISME

L'avis sur le projet de loi antiterrorisme

Dans le contexte international actuel, la lutte contre le terrorisme constitue l'une des préoccupations majeures de l'État. Cette lutte fait de plus en plus appel à des traitements de données à caractère personnel afin non seulement d'identifier et de poursuivre les auteurs de faits en lien avec une entreprise terroriste mais aussi de prévenir les actes de terrorisme. La CNIL a ainsi été saisie par le ministère de l'Intérieur de l'avant-projet de loi relatif à la lutte contre le terrorisme, le 27 septembre 2005.

Ce texte prévoit la mise en place de nouveaux traitements de données personnelles dans divers domaines : vidéosurveillance, transmission aux services de police de données sur les passagers se rendant hors de l'Union européenne ou en provenance de ces pays, mise en place « en tous points appropriés » du réseau routier et autoroutier de dispositifs fixes ou mobiles de lecture des plaques minéralogiques et de prise des photographies des occupants des véhicules, accès aux données de connexion internet et téléphonie conservées par les opérateurs de communications électroniques et les cybercafés, consultation par les services antiterroristes de certains fichiers administratifs détenus par le ministère de l'Intérieur (fichiers des immatriculations, des cartes d'identité, des passeports, des permis de conduire, des titres de séjour et visas).

Dans son avis du 10 octobre 2005, la CNIL a rappelé que les objectifs poursuivis sont légitimes mais appellent des garanties particulières : les dispositifs de prévention du terrorisme, prévus par l'avant-projet de loi, devraient en effet être considérés comme des mesures exceptionnelles prises pour répondre à une menace d'une exceptionnelle gravité. La CNIL s'est ainsi attachée à définir les garanties qui lui paraissent essentielles pour le maintien d'un équilibre entre les impératifs de sécurité nationale et de protection des libertés.

Questions à ...

François GIQUEL

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

Comment la CNIL pourrait-elle s'opposer au renforcement des moyens de lutte contre le terrorisme ?

La lutte contre le terrorisme revêt un caractère nécessairement large et multiforme puisqu'il s'agit de recueillir et d'exploiter, selon des critères évolutifs par nature, des renseignements sur des personnes ayant un parcours particulier et pouvant avoir un lien avec une entreprise terroriste et de cibler ainsi des individus ayant un profil à risque, par exemple en se rendant de manière répétée ou prolongée vers des pays connus pour abriter des activités terroristes.

Mais il faut savoir que cet objectif conduit à mettre à la disposition des services de police et de gendarmerie, dans le cadre de leurs missions de police administrative, des fichiers et des enregistrements de vidéosurveillance susceptibles de « tracer » de façon systématique et permanente une très grande partie de la population, dans ses déplacements et dans certains actes de la vie quotidienne (le lieu où l'on se trouve à tel moment, l'heure d'une connexion internet, le lieu d'où l'on passe un appel d'un mobile, le passage à tel péage d'autoroute, la destination d'un voyage, etc.).

Comment seront obtenues, exploitées, rapprochées ces données ? Combien de temps seront-elles conservées ? Qui sera habilité à les consulter ? Y aura-t-il un contrôle des interrogations de fichiers effectuées par la police ? Comment le public sera-t-il informé de la mise en place de ces dispositifs (comme c'est déjà le cas pour la vidéosurveillance) ? Comment les informations traitées par la police seront-elle utilisées vis-à-vis des personnes concernées ?

Autant de questions que la CNIL se devait de soulever dans le cadre de l'adoption de la loi relative à la lutte contre le terrorisme.

La CNIL a-t-elle été entendue lors de la discussion de cette loi ?

Certaines demandes de la CNIL formulées dans son avis du 10 octobre ont été, pleinement ou en partie, prises en compte dans le cadre de l'adoption de la loi relative à la lutte contre le terrorisme : rappel du nécessaire respect de la loi « informatique et libertés » dans le cadre des dispositifs antiterroristes (hormis la vidéosurveillance), indication précise des services de police et de gendarmerie accédant aux données pour des finalités antiterroristes, définition des conditions d'habilitation et d'accès aux données, limitation dans le temps de certains dispositifs, remise d'un rapport d'évaluation annuel au Parlement.

En revanche, la CNIL a pu constater le maintien dans le texte adopté par le Parlement de la prise systématique de photographie des occupants de l'ensemble des véhicules empruntant certains axes de circulation, de la multiplicité des finalités attachées aux dispositifs (la lutte contre le terrorisme n'étant qu'un des motifs d'accès aux données parmi d'autres), de l'absence de définition des personnes offrant un accès à internet et chargées de conserver trace des données de l'ensemble des connexions ou encore de la constitution d'un fichier central de contrôle des déplacements en provenance ou à destination d'États situés en dehors de l'Union européenne aux contours mal définis.

Enfin, alors même que la CNIL venait de souligner, dans son avis du 10 octobre, la nécessité d'être en mesure d'exercer sans restriction les pouvoirs de contrôle prévus par la loi « informatique et libertés » sur l'ensemble des traitements de données prévus par la lutte antiterroriste, le texte de loi adopté par le Parlement le 22 décembre 2005 permet de limiter l'information communiquée à la CNIL lorsqu'elle devra rendre un avis sur les fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique.

Quels contrôles la CNIL pourra-t-elle exercer sur les dispositifs antiterroristes prévus par la loi ?

En amont et conformément à la loi « informatique et libertés », la CNIL sera saisie des textes d'application de la loi relative à la lutte contre le terrorisme organisant des traitements de données personnelles. Elle sera également saisie des déclarations de création ou de modification des fichiers utilisés. Cette phase de contrôle *a priori* devrait permettre de préciser les finalités poursuivies pour chacun des dispositifs antiterroristes, la nature des données traitées, leur durée de conservation, ainsi que les mesures destinées à assurer la sécurité des données et l'information du public.

En aval, le Gouvernement et les parlementaires ont souligné tout au long du processus d'élaboration de la loi que les traitements de données à finalité antiterroriste devaient être soumis au contrôle de la CNIL et qu'il s'agit là d'une garantie fondamentale. La CNIL veillera en effet à la bonne mise en œuvre de ces traitements, dans son champ de compétence.

La conservation des données de communications électroniques

Les données liées à l'utilisation des services de communications électroniques (c'est-à-dire la téléphonie fixe et mobile ainsi que l'accès à internet) sont de plus en plus fréquemment exploitées par les services de police dans le cadre de la lutte contre le terrorisme.

Plusieurs dispositions de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme visent ainsi à élargir l'exploitation de ces données dont la conservation est rendue obligatoire pour les opérateurs de communications électroniques depuis la loi du 15 novembre 2001 relative à la sécurité quotidienne.

En premier lieu, la loi élargit la définition d'un « opérateur de communication en ligne » afin de soumettre à l'obligation de conservation les opérateurs « classiques » bien sûr, mais aussi les cybercafés, les restaurants, les hôtels, les aéroports, etc., dès lors que ceux-ci proposent un accès au réseau internet. Tout en relevant que cette obligation n'imposait pas, notamment aux cybercafés, d'identifier les utilisateurs de services de communications électroniques, la CNIL a demandé, en vain, que les catégories de personnes physiques ou morales concernées soient précisées afin que les bibliothèques, les mairies, les universités, etc., offrant une connexion internet soient en mesure d'apprécier si elles sont, ou non, soumises à l'obligation de conservation.

En second lieu, la loi permet désormais, hors contrôle de l'autorité judiciaire, l'accès par des agents individuellement habilités des services de police et de gendarmerie nationales en charge de la lutte contre le terrorisme aux données techniques conservées par les opérateurs de communications électroniques. Cet accès est encadré par la loi : les demandes devront être motivées, centralisées et soumises à la décision d'une personne qualifiée, désignée par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'Intérieur. Sur ce point, la CNIL a préconisé une amélioration de la procédure de contrôle de l'accès aux données techniques, notamment par un renforcement de l'action de la CNIL aux côtés de l'intervention prévue par la loi de la Commission nationale de contrôle des interceptions de sécurité et a demandé à être saisie du projet de décret d'application.

Par ailleurs, la CNIL a été saisie d'une nouvelle version du projet de décret d'application de l'article L. 34-1 du Code des postes et des communications électroniques relatif à l'obligation de conservation des données qui vise, notamment, à fixer les catégories de données devant être conservées par les opérateurs. Dans son avis en date du 10 novembre 2005, la Commission a demandé à ce que le décret renvoie à un arrêté pris après avis de la CNIL la détermination exacte des données précitées. Elle a relevé que les nécessités des enquêtes concernant les infractions pénales les plus graves peuvent justifier un accès à des données de trafic remontant à une période supérieure à trois mois et que, dès lors, la durée de conservation d'un an prévue par le projet de décret n'appelait pas d'opposition de sa part.

Enfin, on doit noter que le Parlement européen s'est prononcé et a amendé le projet de directive présenté par la Commission européenne visant à harmoniser au sein de l'Union européenne les obligations de conservation des données relatives aux communications électroniques, notamment en prévoyant une durée minimale de conservation de six mois.

Dernière minute !

Décision du Conseil constitutionnel du 19 janvier 2006

Le Conseil constitutionnel estime que l'accès aux données de connexion par les services de police est assorti de limitations et précautions propres à assurer la conciliation entre le respect de la vie privée et la prévention des actes de terrorisme.

De même, il a validé la création des dispositifs de photographie automatique des véhicules et de leurs occupants, en considérant qu'au regard de l'ensemble des garanties prévues, la conciliation entre le respect de la vie privée et la sauvegarde de l'ordre public n'est pas manifestement déséquilibrée.

L'ÉCHANGE DE FICHIERS SUR INTERNET

À l'occasion de la modification de la loi « informatique et libertés » en août 2004, le législateur a introduit une nouvelle disposition permettant à certains organismes de mettre en œuvre des traitements afin de rechercher et constater des infractions aux droits d'auteur. Deux types d'organismes sont concernés :

– les sociétés de perception et de répartition des droits (SPRD) qui ont en charge la perception, la répartition et la protection des droits d'auteur, des droits des artistes-interprètes ou des producteurs d'œuvres. Il s'agit par exemple de la Société des auteurs, compositeurs et éditeurs de musique (SACEM) ou de la Société civile des producteurs phonographiques (SCPP) ;

– les organismes professionnels de défense qui ont en charge la protection et la défense des droits et intérêts collectifs et professionnels de leurs membres, notamment en luttant contre les atteintes à leurs droits de propriété intellectuelle. Il s'agit par exemple de l'Association de lutte contre la piraterie audiovisuelle (ALPA) ou du Syndicat des éditeurs de logiciels de loisirs (SELL).

Néanmoins, il a été prévu, à titre de garantie, que les traitements en cause soient soumis à l'autorisation préalable de la CNIL. Ainsi, au cours de l'année 2005, cinq organismes ont présenté à la CNIL des demandes d'autorisation afin de mettre en œuvre des dispositifs pour lutter contre la mise à disposition illicite de fichiers sur internet *via* les réseaux *peer to peer*.

Les dispositifs soumis à la CNIL comportaient à chaque fois deux volets :

– un volet préventif consistant en l'envoi d'un message d'avertissement informant les internautes utilisateurs des logiciels d'échanges de fichiers sur le caractère illégal de leurs agissements et sur les sanctions encourues ;

– un volet répressif à l'occasion duquel les agents assermentés des SPRD et des organismes de défense professionnels constatent les infractions et dressent des procès-verbaux en vue d'exercer des poursuites judiciaires.

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 internet. Aujourd'hui, ces échanges s'effectuent d'internaute à internaute, via un logiciel offrant la possibilité à deux ordinateurs reliés à internet de communiquer directement l'un avec l'autre sans passer par un serveur central. On parle d'architecture *peer to peer* décentralisée.

Pour chacun des dossiers qui lui ont été soumis, la Commission s'est attachée à examiner la conformité des traitements aux principes de la protection des données à caractère personnel ainsi qu'à déterminer s'ils assuraient un juste équilibre entre le respect de la vie privée et les droits de propriété intellectuelle.

M É M O

Parmi les 5 dispositifs présentés, la CNIL en a refusé 4 :
– les 4 dispositifs refusés étaient strictement identiques ;
– le responsable du dispositif autorisé a finalement décidé de l'interrompre.

	Dispositif autorisé	Dispositifs refusés
Organismes demandeurs	Syndicat des éditeurs de logiciels de loisirs (SELL)	Société des auteurs compositeurs et éditeurs de musique (SACEM) Société pour l'administration du droit de reproduction mécanique (SDRM) Société civile des producteurs phonographiques (SCPP) Société civile des producteurs de phonogrammes en France (SPPF)
Descriptif technique du dispositif de constatation d'infraction	Les agents assermentés du SELL déclenchaient des inspections grâce à un logiciel permettant d'effectuer des requêtes sur internet à partir du nom d'un logiciel figurant dans le catalogue du SELL. En réponse, ils obtenaient la liste des adresses IP des internautes mettant à disposition les logiciels correspondant aux requêtes effectuées. Seules étaient conservées, en vue d'effectuer des actions judiciaires, les adresses IP des internautes : – responsables de **la première** mise à disposition sur le réseau d'un logiciel ; – ayant mis à disposition un logiciel **non encore commercialisé**.	Les agents assermentés des SPRD devaient déclencher des inspections grâce à un logiciel permettant d'effectuer des requêtes sur internet à partir du titre ou du nom de l'auteur des œuvres figurant dans une base de données de référence. En réponse, ils devaient obtenir la liste des adresses IP des internautes mettant à disposition les fichiers musicaux correspondant aux requêtes effectuées. Ils devaient ensuite lancer une phase de constitution de preuves d'une durée de quinze jours pendant laquelle des requêtes devaient être effectuées sur l'adresse IP des internautes pour lesquels la phase d'inspection avait révélé qu'ils mettaient à disposition **un nombre d'œuvres supérieur à un seuil préétabli**. À échéance de ces quinze jours, deux nouveaux seuils devaient être appliqués afin de déterminer les internautes devant faire l'objet de poursuites civiles et ceux retenus pour des poursuites pénales.
Descriptif technique du dispositif d'envoi de messages	Les internautes mettant à disposition des logiciels de loisirs étaient repérés sur la base de leur adresse IP à la suite d'une phase d'inspection. Étaient visés les internautes ne répondant pas aux critères retenus pour les poursuites judiciaires. L'envoi du message se faisait via les fonctionnalités de communication des logiciels de *peer to peer*. **L'adresse IP était traitée instantanément et n'était pas conservée.**	Les internautes mettant à disposition illégalement des œuvres musicales étaient repérés sur la base de leur adresse IP à la suite d'une phase d'inspection. Devaient être visés les internautes en dessous des seuils prévus pour les poursuites judiciaires. L'envoi de message devait s'effectuer **par le fournisseur d'accès internet de l'internaute concerné. Il devait faire le lien entre l'adresse IP et l'identité de l'abonné et envoyer le message par courrier électronique.**
Motifs de la décision de la CNIL	Autorisation de la CNIL *Sur le volet préventif :* l'envoi de message ne nécessite pas l'identification des internautes concernés par leur fournisseur d'accès à internet. *Sur le volet répressif :* il est proportionné à la finalité poursuivie notamment, car les poursuites qu'il permet d'engager sont limitées à des cas particulièrement graves : seuls les internautes responsables de la première mise à disposition sur le réseau d'une œuvre et/ou ayant mis à disposition une œuvre non encore commercialisée sont concernés.	Refus d'autorisation de la CNIL *Sur le volet préventif :* – en l'état actuel de la législation, les fournisseurs d'accès à internet ne sont pas autorisés à conserver les données de connexions des internautes pour envoyer des messages pédagogiques pour le compte de tiers ; – dans sa décision du 29 juillet 2004 le Conseil constitutionnel indique que seule l'autorité judiciaire peut autoriser le rapprochement entre une adresse IP et l'identité d'un internaute lors des traitements relatifs aux infractions. *Sur le volet répressif :* – il n'avait pas pour objet la réalisation d'actions ponctuelles strictement limitées au besoin de la lutte contre la contrefaçon, il permettait la surveillance exhaustive et continue des réseaux d'échanges de fichiers *peer to peer* ; – la sélection des internautes susceptibles de faire l'objet de poursuites pénales ou civiles s'effectuait sur la base de seuils que les sociétés d'auteurs se réservaient la possibilité de réviser unilatéralement à tout moment.

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

Les origines du dossier : les refus d'autorisation du 26 mai 2005

Par deux décisions du 26 mai 2005, la CNIL a refusé d'autoriser des dispositifs d'alerte professionnelle, dont la finalité était de permettre à des salariés de signaler des comportements supposés fautifs imputables à leurs collègues de travail. La Commission a refusé leur mise en œuvre en considérant que ces dispositifs, au regard de leurs caractéristiques, risqueraient de conduire à un « système organisé de délation professionnelle ».

L'impact de ces deux refus d'autorisation a été important, tant en France qu'à l'étranger.

À la lecture de ces décisions, les entreprises ont craint que ces deux refus d'autorisation ne soient de principe et qu'il en résulte, pour elles, une incapacité d'être en conformité avec la loi « informatique et libertés » d'une part, et la loi américaine Sarbanes-Oxley qui prévoit la mise en place de telles procédures de traitement des alertes dans les domaines financier, comptable et de contrôle des comptes, d'autre part. En application de cette loi, les entreprises françaises présentes sur les bourses américaines doivent en effet certifier qu'elles sont en règle, sous peine d'être retirées de la cotation. Consciente de ces difficultés, et ne souhaitant pas laisser les entreprises dans cette incertitude juridique, la CNIL a entrepris diverses démarches afin d'assurer le suivi de ses décisions du 26 mai 2005.

Les démarches effectuées par la CNIL en France et à l'international

La CNIL a immédiatement informé de ses décisions l'autorité américaine chargée de veiller à la bonne application de la loi *Sarbanes-Oxley*, la *Securities and Exchange Commission* (SEC), le *New York Stock Exchange* (NYSE), et le Nasdaq. Elle a également pris attache avec les directions générales compétentes de la Commission

européenne (DG MARKT et JLS) et les autres autorités européennes de protection des données.

Parallèlement ont eu lieu des échanges avec les ministères concernés (Travail, Économie et Finances, Justice), les représentants des entreprises (le MEDEF et l'Association française des entreprises privées-AFEP, mais aussi directement avec quelques grands groupes), les syndicats et des organisations non gouvernementales d'éthique des affaires.

Par une lettre du 10 août 2005, la SEC, soulignant la flexibilité de la loi américaine en la matière, a informé la CNIL de sa volonté de travailler avec elle pour discuter des conditions dans lesquelles de tels dispositifs pourraient devenir acceptables au regard des règles françaises et américaines. Plusieurs échanges constructifs ont ainsi eu lieu entre la CNIL et la SEC.

Adoption par la CNIL d'un document d'orientation et d'une autorisation unique

Dès le début du mois de septembre, la CNIL avait annoncé sur son site web qu'après une phase de concertation, elle comptait rendre publique son analyse de la mise en place par les entreprises de dispositifs d'alerte respectueux à la fois de la loi Sarbanes-Oxley et de la loi « informatique et libertés ». La consultation sur le projet de lignes directrices émis en octobre 2005 a suscité de

nombreuses réponses, tant de France que d'autres pays d'Europe ou des États-Unis.

Sur la base des observations recueillies, un projet modifié a été soumis le 10 novembre 2005 à la CNIL qui l'a adopté sous la forme d'un document d'orientation. Ce document définit officiellement et publiquement la position de la CNIL.

Dans une seconde étape, la CNIL a adopté, le 8 décembre, une décision d'autorisation unique des dispositifs conformes aux orientations retenues par elle afin de simplifier les obligations déclaratives des entreprises. Cette autorisation unique (AU-004) permet aux entreprises de mettre en œuvre leur dispositif d'alerte après une simple télédéclaration sur www.cnil.fr et la réception du récépissé afférent.

Les travaux européens sur les alertes professionnelles

Dès le mois de juin 2005, la CNIL a rapporté à ses homologues européens la teneur de ses travaux et évoqué la nécessité que le groupe de l'article 29, qui rassemble les vingt-cinq autorités européennes de protection des données, se saisisse également de ce dossier.

Ce thème a été officiellement porté au programme de travail du groupe pour l'année 2006, et les travaux ont commencé début janvier. Les documents élaborés par la CNIL constituent la base de ces travaux européens.

Les grandes lignes du document d'orientation adopté par la CNIL

La CNIL recommande

La CNIL recommande de :
– restreindre le dispositif d'alerte au domaine comptable, au contrôle des comptes, au domaine bancaire et à la lutte contre la corruption ;
– ne pas encourager les dénonciations anonymes ;
– mettre en place une organisation spécifique pour recueillir et traiter les alertes ;
– informer la personne concernée dès que les preuves ont été préservées.

Questions à …

Hubert BOUCHET

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

Quels étaient les objectifs de la CNIL dans ce dossier ?

L'objectif premier de la CNIL a été d'éviter la constitution, sur les lieux de travail, de dispositifs d'alerte professionnelle susceptibles de dériver en systèmes organisés de délation. Cela s'est traduit par les deux refus d'autorisation du 26 mai 2005.

Une fois ce nécessaire coup d'arrêt donné, son objectif a ensuite été de définir, en concertation, un ensemble de recommandations à destination des entreprises pour une mise en œuvre de dispositifs d'alerte conforme aux exigences de la loi « informatique et libertés » et en prise avec les réalités économiques internationales (loi Sarbanes-Oxley notamment). Cette concertation a abouti au document d'orientation du 10 novembre 2005.

Dans un troisième temps, l'objectif a été de simplifier les obligations déclaratives des entreprises se conformant aux orientations retenues le 10 novembre. Une sorte de prime à la légalité et aussi à la modération. Ceci s'est traduit par la décision unique d'autorisation du 8 décembre 2005. La CNIL souhaite désormais alimenter la réflexion de ses homologues européens sur ces questions.

La CNIL est-elle finalement revenue sur ses refus d'autorisation du 26 mai 2005 ?

Non, les décisions de refus d'autorisation du 26 mai 2005 reposaient sur les principes de proportionnalité et de loyauté de la collecte des données, et soulignaient le risque lié à la réception d'alertes anonymes.

Cette analyse a ensuite été reprise dans le document d'orientation du 10 novembre. Le cadre défini par ce document rappelle ainsi que le champ du dispositif d'alerte professionnelle devrait être limité à certains domaines nécessitant, d'après la loi, un contrôle interne particulier, qu'une information claire et rapide de la personne mise en cause devrait être prévue, et que les alertes anonymes devraient demeurer l'exception. D'autres points ont également été précisés à cette occasion tels que la confidentialité des données, la durée de conservation, l'information des employés, les droits d'accès et de rectification, la transmission des données hors Union européenne.

LE RISQUE FINANCIER

Le nouveau régime de formalités applicable aux traitements de credit scoring et les mesures de simplification envisagées

En 2005, la Commission a examiné plusieurs traitements de score de crédit ou *credit scoring*. La multiplication de dossiers similaires a conduit la CNIL à envisager l'adoption de mesures de simplification.

Le credit scoring soumis à autorisation de la CNIL

Les applications de score de crédit sont non seulement susceptibles d'exclure des personnes du bénéfice d'un contrat mais ont aussi pour objet de sélectionner, selon certains profils, les personnes auxquels l'établissement de crédit ne souhaite pas ou ne peut pas distribuer de crédit. Bien souvent, en complément du score de crédit, le système expert analyse des éléments disqualifiants à eux seuls, tels que l'âge (plus de 65 ans ; moins de 25 ans), la profession (vendeur ambulant), le type d'habitation (caravane) etc., et rendant impossible toute issue favorable de la demande de crédit présentée.

Dès lors, la CNIL a décidé de faire application des dispositions de l'article 25-I-4° de la loi du 6 janvier 1978 modifiée en 2004 faisant relever les traitements susceptibles d'exclure une personne du bénéfice d'un contrat de crédit d'un régime d'autorisation.

Le principe d'une autorisation unique pour les traitements de score de crédit

Les établissements de crédit disposent tous d'un, voire plusieurs traitements de score de crédit. Bien que les grilles et tables de score diffèrent d'un type de crédit à l'autre et d'un établissement à l'autre, les fonctionnalités des applications sont identiques et les variables utilisées dans les systèmes classiques sont connues. Si de tels traitements doivent relever d'une procédure d'autorisation en raison de leur sensibilité, il est aussi du devoir de la CNIL d'utiliser les instruments prévus par la loi pour alléger les formalités pour les cas de traitements les plus courants.

Ces considérations ont conduit la CNIL à élaborer un projet d'autorisation unique relative à la mise en œuvre d'outils de score de crédit, projet qu'elle a soumis à la consultation des instances représentatives de la profession bancaire et à la Commission bancaire, et qui devrait être adopté définitivement au cours de l'année 2006.

Les systèmes de score de crédit ou de notation d'une nature particulière (comportant des variables non énumérées dans l'autorisation unique, par exemple) resteront soumis à une appréciation au cas par cas de la CNIL.

Qu'est-ce que c'est ?

Le *credit scoring* ou score de crédit

Les logiciels de score de crédit associent à des informations personnelles relatives aux demandeurs de crédit (niveau de ressources financières, nombre de personnes à charge, stabilité de résidence ou dans l'emploi) des pondérations particulières issues de données statistiques se traduisant par des probabilités de défaut, de sorte qu'au-dessus d'un montant de points, le crédit est accordé. En pratique, le score de crédit est surtout utilisé pour les crédits à la consommation et trouve sa consécration dans les systèmes experts permettant aux apporteurs d'affaire de « vendre » le crédit sur le lieu de vente du bien financé. Dans ce cas, le client n'obtient du logiciel qu'une réponse binaire : acceptation du financement ou rejet, les commerçants n'ayant aucune compétence pour décider l'octroi d'un crédit lorsque le système expert (souvent associé à une interrogation des fichiers de la Banque de France) donne une réponse négative.

Questions à …

Philippe NOGRIX

Sénateur de l'Ille-et-Villaine

Commissaire en charge du secteur « Monnaie et Crédit »

Cette autorisation unique est-elle destinée à créer un référentiel pour les traitements de* credit scoring *?

En aucun cas. Il s'agit d'une mesure de simplification des formalités. Par cette délibération, la CNIL détermine quels sont les traitements pouvant bénéficier de la simplification. Pour les autres, il y a maintien du régime de droit commun : c'est-à-dire dépôt d'une demande d'autorisation.

Dans quelles conditions un banquier peut-il communiquer des données à caractère personnel à d'autres établissements de crédit ?

Ni la loi bancaire ni la loi « informatique et libertés » ne permettent que le banquier puisse céder ou partager une information confidentielle sans que le client en soit informé. Le secret bancaire impose que le client ait donné son consentement éclairé. Doivent être définis contractuellement au moment où le client délie le banquier de son obligation de secret les éléments suivants : l'usage ou la finalité de l'information partagée, les conditions du partage (base centralisée, échange…) et les destinataires, qui doivent avoir une légitimité à partager l'information et être eux-mêmes tenus au secret bancaire.

Cela signifie-t-il que le client peut autoriser la levée totale du secret bancaire au bénéfice de tous les établissements de crédit?

La CNIL a toujours soutenu que seule une intervention législative était de nature à permettre une dérogation aussi large au principe du secret bancaire notamment pour des conventions ayant le caractère de contrats d'adhésion où par définition le pouvoir de négociation du particulier est extrêmement faible, où le droit d'opposition ne peut être réellement exercé et où la souscription d'une clause particulière ne permet pas d'assurer que la personne a indubitablement donné son consentement, de façon libre et éclairée. Il est difficilement admissible que le secret bancaire puisse être levé de façon générale et qu'il soit permis par exemple d'effectuer des diffusions publiques…. Le législateur devra notamment préciser les objectifs recherchés par la centralisation, définir les destinataires, la nature des données centralisées et déterminer les garanties permettant d'assurer que le fichier ne sera pas utilisé pour un autre usage…

La problématique de l'échange et la centralisation d'informations couvertes par le secret bancaire à des fins de lutte contre la fraude et les impayés

La CNIL a eu à se prononcer de nouveau [10] sur le partage d'informations couvertes par le secret bancaire. Elle a en effet été saisie par plusieurs établissements financiers spécialisés dans le crédit à la consommation de traitements répondant à des finalités de prévention de la fraude et du surendettement basés sur le partage d'informations couvertes par le secret bancaire.

10. *Cf.* le rapport sur la prévention de la fraude et des impayés dans le secteur du crédit de 2000, *Rapport sur les listes noires*, La Documentation française, novembre 2003.

Le partage ponctuel et limité d'informations entre filiales spécialisées d'un même groupe bancaire

La CNIL a été saisie conjointement par les sociétés FINAREF et SOFINCO [11] d'une demande d'autorisation relative à la mise en œuvre d'un traitement ayant pour finalité la prévention du surendettement par les filiales de crédit à la consommation du groupe Crédit Agricole. Le traitement envisagé repose sur un échange ponctuel d'informations entre les sociétés FINAREF et SOFINCO destiné à évaluer le niveau d'endettement d'un demandeur de crédit au regard des crédits à la consommation précédemment souscrits auprès de l'une des deux sociétés ou d'une société ayant confié la gestion de ses crédits à la société SOFINCO.

La CNIL a autorisé la mise en œuvre du traitement au motif principal que l'échange d'informations ponctuel et limité intervient uniquement entre deux sociétés appartenant au même groupe financier, qu'elles sont toutes

11. Délibération n° 2005-196 du 8 septembre 2005.

deux spécialisées dans le crédit à la consommation et qu'il existe une communauté de risque financier entre les sociétés bénéficiaires de l'échange de données.

Par ailleurs, la CNIL a estimé que le consentement des clients était recueilli dans des conditions satisfaisantes, une clause particulière de la demande de crédit précisant la finalité et les destinataires des échanges d'information et l'autorisation explicite du client de partager des informations couvertes par le secret bancaire étant prévues.

La mutualisation au sein d'une centrale d'information accessible à l'ensemble des établissements de crédit

La CNIL a examiné deux demandes d'autorisation présentées par les sociétés Banque Accord et Volkswagen finance relatives à l'utilisation d'un traitement de mutualisation des informations relatives aux demandeurs de crédit, dénommé « detect », mis en œuvre par la société Experian. La CNIL a estimé que les mentions d'information devaient explicitement prévoir que les éléments présentés par les demandeurs de crédit seront rapprochés des éléments qui avaient pu être antérieurement déclarés auprès d'un autre établissement de crédit également adhérent du service « detect » à des fins de contrôle de cohérence et que le client devait également être informé que la liste des adhérents du service « detect » peut lui être communiquée sur simple demande.

La CNIL a considéré de surcroît que la centralisation d'informations couvertes par le secret bancaire accessibles à un nombre indéterminé d'établissements de crédit, non liés entre eux par une communauté de risques, rendait nécessaire un recueil exprès du consentement, par le biais d'une case à cocher ou tout autre moyen permettant d'établir le caractère exprès du consentement [12]. La CNIL a aussi précisé [13] que la clause d'information devait aussi expressément désigner le fichier central d'Experian comme destinataire des données.

Dans la perspective de la multiplication de demandes d'autorisation portant sur la centralisation ou l'échange d'informations couvertes par le secret bancaire, la CNIL a saisi le Comité consultatif de la législation et de la réglementation financière (CCLRF) de la problématique liée à la mise en œuvre des traitements destinés à la prévention de la fraude et la mesure du risque de crédit et de surendettement au regard des dispositions du Code monétaire et financier relatives au secret bancaire.

---

12. Délibération n° 2005-198 du 8 septembre 2005.
13. Délibération n° 2005-199 du 22 septembre 2005.

LA MESURE DE LA DIVERSITÉ DES ORIGINES

La lutte contre les discriminations dans le secteur de l'emploi, notamment celles liées aux origines ethniques, nationales ou raciales, a fait l'objet au cours des derniers mois de nombreux rapports et initiatives. Dans le même temps, les pouvoirs publics, par la mise en place de la Haute autorité de lutte contre les discriminations (HALDE) ainsi que par la désignation d'un ministre délégué à la promotion de l'Égalité des chances, ont montré leur volonté de faire de cette lutte l'une des priorités des politiques publiques.

Les outils de mesure de la diversité, qui ont pour but de permettre aux employeurs de connaître les origines ethniques et sociales de leurs salariés ou des candidats à l'emploi, peuvent reposer sur la collecte et le traitement de données permettant l'identification, même momentanée, des personnes concernées. Or, la loi « informatique et libertés » considère toute donnée sur l'origine raciale ou ethnique d'une personne comme une donnée sensible dont le recueil et l'utilisation sont soumis à des précautions particulières.

La volonté affichée par certains employeurs publics et privés de se doter de tels outils pour mesurer la diversité des origines de leurs salariés a conduit la CNIL à mettre en place, au début de l'année 2005, un groupe de travail afin de recenser les projets en cours, de s'informer auprès des responsables desdits projets et de la statistique publique, et d'élaborer des recommandations.

Ces recommandations ont été adoptées par la CNIL le 5 juillet 2005.

Questions à ...

Anne DEBET

Professeur des universités

Commissaire en charge du secteur « Affaires sociales »

Quelles sont les principales recommandations élaborées par la CNIL à l'attention des employeurs désireux de mesurer la diversité des origines de leurs salariés ?

La CNIL estime que la mise en œuvre d'outils statistiques de mesure de la diversité pour lutter contre les discriminations en matière d'emploi est tout à fait légitime. Elle considère toutefois qu'en l'absence d'un référentiel national de typologies « ethno-raciales » constitué par la statistique publique et dont la création devrait être approuvée par le législateur, il n'existe pas de bases de comparaisons fiables. En conséquence, la CNIL recommande aux employeurs de ne pas recueillir de données relatives à l'origine raciale ou ethnique, réelle ou supposée de leurs employés ou de candidats à l'embauche.

Elle privilégie le traitement d'informations sur l'origine nationale des personnes telles qu'elles existent déjà dans la statistique publique (nationalité, nationalité d'origine le cas échéant, lieu de naissance, nationalité ou lieu de naissance des parents) et recommande que l'exploitation de ces données s'effectue dans le respect de l'anonymat. Elle conseille aux employeurs d'engager, en concertation avec les instances représentatives du personnel, une réflexion préalable pour clarifier les objectifs de la politique de diversité.

Peut-on cependant utiliser les fichiers du personnel tels qu'ils sont ?

La CNIL considère que l'utilisation, à des fins de mesure statistique de la diversité, des données enregistrées dans les fichiers de gestion des ressources humaines et en particulier de la nationalité des salariés et de leur lieu de naissance est possible à plusieurs conditions.

L'employeur doit bien sûr en faire la déclaration à la CNIL et les employés doivent être clairement informés des traitements opérés sur les données les concernant. Les statistiques produites ne doivent pas porter sur des groupes de moins de dix personnes afin de garantir l'anonymat, et les fichiers de données individuelles constitués pour la réalisation de l'étude (échantillons, réponses) doivent être détruits à l'issue de la production des résultats statistiques. Enfin, la CNIL rappelle que la mesure de la diversité ne permet pas à un employeur d'enrichir ses fichiers de gestion des ressources humaines de données non pertinentes ou disproportionnées au regard des finalités traditionnelles de tels fichiers. Ainsi, des données telles que la nationalité d'origine d'un employé ou d'un candidat à un emploi, de même que la nationalité ou le lieu de naissance de ses parents doivent être exclues.

Y a-t-il d'autres voies pour les employeurs ?

La réalisation d'enquêtes par questionnaires anonymes est admise. L'anonymat d'un questionnaire est garanti, non seulement par la suppression du nom mais aussi par l'absence de données permettant d'identifier indirectement la personne qui y répond (un numéro, désignation d'un poste particulier, descriptif de fonctions précises). Si le questionnaire comporte des données indirectement identifiantes, leur traitement doit s'effectuer dans des conditions de confidentialité vis-à-vis de l'employeur. En outre, les statistiques produites ne doivent pas concerner de groupes de moins de dix personnes et la destruction des questionnaires doit intervenir à l'issue de la phase d'exploitation des réponses.

Des questionnaires peuvent toutefois comporter des données d'identification lorsque l'objet de l'étude nécessite le suivi des réponses données par une même personne à des moments différents (suivi de trajectoires individuelles). Dans ce cas, la nécessité du suivi doit être justifiée et toutes mesures prises pour garantir la confidentialité des données. Bien entendu, ces enquêtes doivent être déclarées auprès de la CNIL.

OÙ EN EST-ON SUR…?

LE BRACELET ÉLECTRONIQUE

Le placement sous surveillance électronique mobile (PSEM) constitue une des dispositions « phare » de la loi du 12 décembre 2005 sur le traitement de la récidive des infractions pénales. Présenté sous forme d'une proposition de loi, le texte a suscité un vif débat parlementaire. Concrètement, le PSEM permet de connaître de façon continue la localisation de la personne porteuse du bracelet émetteur par recours à la technique du GPS ou du GSM alors que le placement sous surveillance électronique fixe, assimilé à une « assignation à résidence électronique », empêche la personne porteuse du bracelet émetteur de s'éloigner du lieu fixé par le juge (généralement son domicile), en dehors de plages horaires fixées à l'avance. Outre l'État de Floride, l'Espagne et la Grande-Bretagne, mènent des expérimentations de surveillance électronique par GPS.

Le PSEM peut être utilisé dans trois cadres juridiques distincts :

– le suivi socio-judiciaire : ordonné par la juridiction de jugement, le PSEM ne s'applique qu'aux personnes majeures condamnées à une peine privative de liberté d'au moins sept ans et dont la dangerosité doit avoir été constatée par une expertise médicale ; la durée du PSEM est de deux ans renouvelable avec un maximum de quatre ans pour les délits et de six ans pour les crimes. Le consentement de l'intéressé est indispensable. Il s'agit alors d'une peine complémentaire. Dans certains cas si la juridiction de jugement ne l'a pas prévu, le juge d'application des peines peut aussi proposer le PSEM ;

– la libération conditionnelle : modalité d'exécution de la peine, le PSEM, dans ce cadre est décidé par le juge d'application des peines, sous réserve du consentement de l'intéressé ;

Questions à …

Patrick DELNATTE

Député du Nord

Commissaire en charge du secteur « Justice »

En quoi ces dispositifs concernent-ils la CNIL ?

Dans la mesure où ils reposent notamment sur l'utilisation de systèmes de télécommunications permettant de géolocaliser les individus et sur la constitution d'un fichier nominatif permettant d'assurer le suivi des personnes ainsi géolocalisées à distance, ces dispositifs constituent des traitements de données personnelles qui doivent être soumis à la CNIL ainsi que le rappelle d'ailleurs la loi de décembre 2005 : le contrôle à distance de la localisation du condamné fait l'objet d'un traitement automatisé de données à caractère personnel, mis en œuvre conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (article 763-13 du nouveau Code pénal). Il est également prévu que les dispositions du décret d'application de la loi concernant ce traitement et qui devront préciser, notamment, la durée de conservation des données enregistrées, soient prises après avis de la CNIL.

Quelle réflexion appelle sur le plan des principes informatique et libertés le développement de ces dispositifs ?

Au seul regard des principes de protection des données personnelles, le recours à de tels dispositifs de géolocalisation pour suivre et contrôler les déplacements de personnes certes condamnées et jugées *a priori* dangereuses mais cependant libérées suscite des interrogations de fond relatives au respect de la vie privée et des libertés individuelles de ces personnes, en particulier leur liberté d'aller et venir et amène à réfléchir sur le nécessaire respect du principe de proportionnalité en la matière. À l'heure du développement des dispositifs de géolocalisation et des multiples possibilités d'utilisation de cette technique, il importe d'être vigilant sur le risque de banalisation de ce type de dispositifs et sur la nécessité d'en encadrer étroitement l'usage.

La loi du 12 décembre 2005 répond-elle à ces interrogations ?

Le principal acquis de la discussion parlementaire est d'avoir retenu le principe du consentement quel que soit le cadre juridique de l'utilisation du bracelet électronique. Sur ce point le pragmatisme rejoint les principes « informatique et libertés ». L'étude des expériences étrangères à laquelle s'était livré Georges Fenech, parlementaire en mission, a bien montré qu'un système aussi contraignant dans la vie quotidienne requiert une coopération de l'intéressé. On l'avait d'ailleurs déjà constaté avec la surveillance électronique fixe dont j'ai suivi la mise en œuvre pour la CNIL. Le PSEM va lui aussi demander des mois ou des années de mise au point et d'expérimentation.

– la surveillance judiciaire : il s'agit d'un cadre nouveau dans lequel le PSEM peut être ordonné par le juge d'application des peines à l'encontre de personnes condamnées à une peine privative de liberté d'une durée égale ou supérieure à dix ans pour certaines catégories de crimes ou de délits particulièrement graves (exemple : meurtre accompagné d'un viol, d'actes de tortures, délits d'agression sexuelles aggravées commis en récidive…) ; considérée comme une mesure d'exécution de la peine, sa durée ne peut excéder celle correspondant aux réductions de peine dont le condamné a bénéficié. Ces dispositions sont d'application immédiate y compris pour des personnes condamnées pour des faits commis avant leur entrée en vigueur, comme le Conseil constitutionnel l'a admis dans sa décision du 8 décembre 2005.

Toutefois, là encore, le bracelet électronique ne peut être imposé au condamné.

LA SURVEILLANCE DES SALARIÉS

Le contrôle par empreinte digitale des horaires

Le tribunal de grande instance de Paris, par une décision du 19 avril 2005, a jugé que la mise en place d'un contrôle par empreinte digitale des horaires des salariés est disproportionnée. Pourtant l'employeur avait respecté ses obligations en matière d'information individuelle des salariés et de consultation préalable des salariés. Il avait en outre déclaré le dispositif auprès de la CNIL.

En se fondant expressément sur l'exigence de la proportionnalité (posée notamment par l'article L. 120-2 du Code du travail) des moyens de contrôle mis en place par l'employeur au regard des objectifs poursuivis, le tribunal fait néanmoins interdiction à la société de mettre en place un système de « badgeage » biométrique par empreinte digitale. Le juge considère ainsi qu'un employeur n'est pas fondé à mettre en œuvre un système de contrôle des horaires par empreinte digitale lorsqu'il n'est pas démontré que l'utilisation d'un système de badgeage classique ne permettrait pas un contrôle aussi efficace.

Le tribunal s'inscrit ainsi dans la ligne des décisions prises par la CNIL en la matière. Il convient à cet égard de rappeler que, depuis la modification de la loi « informatique et libertés » par la loi du 6 août 2004, la mise en œuvre de tout système biométrique de contrôle des accès ou des horaires des salariés est soumise à une procédure d'autorisation préalable de la Commission.

L'accès au disque dur du salarié, sous certaines conditions

La chambre sociale de la Cour de cassation avait affirmé, en octobre 2001, le droit absolu des salariés au respect de l'intimité de leur vie privée dans le cadre de l'utilisation de leur messagerie électronique professionnelle.

Par son arrêt du 17 mai 2005, elle reconnaît le droit de l'employeur d'accéder sous certaines conditions aux fichiers personnels de ses salariés contenus dans le disque dur de leur ordinateur en décidant que *« sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé »*.

Un tel cas d'accès à l'espace réservé à l'employé devrait, par principe, être prévu par le règlement intérieur, ainsi que les modalités d'information préalable du salarié (qui doit être présent ou au moins être prévenu). Par exception, le contrôle de l'espace réservé est possible sans inscription au règlement intérieur et sans information préalable en cas de « risque ou d'événement particulier ». Cette exception doit nécessairement être d'interprétation stricte : la Cour de cassation a ainsi retenu en 2001 que la fouille de l'armoire individuelle ayant permis la découverte de boissons alcoolisées n'était justifiée par aucun risque ou événement particulier.

En fin de compte l'arrêt du 17 mai 2005 ne paraît pas remettre en cause l'application du principe de proportionnalité aux contrôles exercés sur les fichiers « personnels » des salariés, l'employeur demeurant obligé, dans tous les cas, de fournir une justification précise pour tout accès envisagé à des fichiers de nature personnelle, conformément à l'article L. 120-2 du Code du travail et aux textes relatifs à la protection de la vie privée.

Le pilotage de l'activité des travailleurs sociaux

La CNIL a eu, en 2005, l'occasion de préciser les conditions dans lesquelles un traitement informatisé permettant le contrôle de l'activité des travailleurs sociaux pouvait être mis en œuvre.

La CNIL ne conteste pas la légitimité d'un dispositif de pilotage de l'activité des services sociaux qui s'inscrit dans un contexte d'efficacité des services publics et du bon usage des fonds publics ; toutefois, la CNIL a refusé d'autoriser le recueil de données relatives à l'activité des travailleurs sociaux parce que le dispositif envisagé reposait sur la définition d'objectifs chiffrés d'accompagnement social et sur l'enregistrement de données pertinentes sur les difficultés sociales des usagers[14].

La CNIL a également refusé un traitement permettant l'exploitation aux niveaux régional et national de données individualisées relatives à l'activité des travailleurs sociaux, dans la mesure où le mode de recueil retenu, à savoir la collecte de données recueillies pour partie sur la base d'une *« déclaration de l'agent relative aux comportements de ses collègues qui lui posent problème »* n'apparaissait pas adéquat, dans le cadre d'un traitement à finalité statistique, en raison notamment du caractère subjectif de l'appréciation portée et donc de l'absence de fiabilité de cette information[15].

14. Délibération n° 2005-038 du 10 mars 2005 relative à la modification du traitement ANAISS, présentée par la Caisse nationale d'assurance maladie des travailleurs salariés.
15. Délibération n°2005-086 du 12 mai 2005 relative au traitement OSAME du ministère de l'Équipement.

LE SPAM

La condamnation d'un spammeur

Par un arrêt du 18 mai 2005, la cour d'appel de Paris a condamné à une amende de 3 000 euros un expéditeur de courriers électroniques non sollicités dont la CNIL avait dénoncé les agissements et qui avait été relaxé en première instance le 7 décembre 2004 par le tribunal correctionnel de Paris. Cette décision confirme ainsi l'analyse de la CNIL selon laquelle le fait de collecter, à l'insu des personnes concernées, dans le domaine public de l'internet, des adresses de courriers électroniques permettant d'identifier directement ou indirectement une personne physique, est contraire à la législation sur la protection des données. Un pourvoi en cassation a été formé contre cette décision.

La prospection par courrier électronique dans le cadre professionnel

Depuis 2004, l'utilisation du courrier électronique dans les opérations de prospection commerciale est subordonnée au recueil du consentement préalable des personnes physiques *(opt in)*. La question de savoir si le consentement préalable était également exigé dans le cadre de la prospection commerciale entre professionnels *(B to B)* a finalement été tranchée par la CNIL lors de sa séance du 17 février 2005 qui a estimé que le principe dit de *l'opt in* vise uniquement le cas d'une prospection électronique entre professionnels et particuliers *(B to C)*. S'agissant de la prospection en *B to B*, le principe est celui d'une information préalable et d'un droit d'opposition, ce qui signifie que le professionnel doit, au moment de la collecte de son adresse, avoir été informé que son adresse électronique sera utilisée à des fins de prospection et, avoir été mis en mesure de s'opposer à cette utilisation de manière simple et gratuite. L'objet de la sollicitation doit également être en rapport avec la profession de la personne démarchée (exemple : message présentant les mérites d'un logiciel à paul.toto@société.fr, directeur informatique.)

Questions à ...

Bernard PEYRAT

Conseiller à la Cour de cassation

Commissaire en charge du secteur «Commerce»

A-t-on avancé dans l'organisation de la lutte contre le spam ?

En juillet 2003, le Gouvernement français a mis en place, une plate-forme de concertation public-privé, dont les travaux ont permis le développement d'un projet de centre national de signalement des spams appelé Signal-spam. Ce projet est destiné à reprendre et pérenniser les missions de l'opération «boîte à spam» que la CNIL avait menée avec succès en 2002. Ce dispositif qui devrait en principe être opérationnel dans le courant 2006 permettra ainsi aux usagers de transférer vers une adresse dédiée les spams dont ils sont victimes.

Le spam a donc engendré une nouvelle administration ?

Ce piège a été évité. Signal-spam est une association de droit privé dont les statuts ont été signés le 8 novembre 2005 en présence des pouvoirs publics. Elle réunit les utilisateurs et les professionnels spécialistes des réseaux et du commerce en ligne et elle est financée par les professionnels.

Qu'apportera le dispositif Signal-spam en matière de lutte contre le spam ?

Avec ce dispositif auquel la CNIL est étroitement associée, il sera désormais possible d'apporter des réponses concrètes pour lutter contre le spam. Un véritable centre de ressources et de lutte contre le spam va ainsi voir le jour en France et des actions de coopération à l'échelle internationale vont être menées. Les autorités compétentes seront ainsi plus facilement à même de réprimer et sanctionner, dans le cadre de leurs compétences respectives, les spammeurs.

LE VOTE ÉLECTRONIQUE

En 2005, la CNIL a été saisie uniquement de dossiers de vote électronique portant sur des élections d'ordres professionnels. Elle a considéré que ces traitements constituaient des téléservices de l'administration électronique dans la mesure où ils sont à la disposition d'usagers d'un service public géré par un organisme privé.

Dans ses différents avis[16], la CNIL a souligné que les applications de vote électronique connaissent, depuis quelques années, une amélioration notable de leurs conditions de sécurité. Mais elle a, dans le même temps, relevé que le système technique qui lui était soumis (identique dans les différents dossiers) comportait plusieurs lacunes, en particulier au regard de la recommandation de la CNIL du 1er juillet 2003 sur les sécurités des systèmes de vote électronique.

Dans aucun des projets présentés, une expertise indépendante n'a été réalisée alors que c'était un des points forts de la recommandation de la CNIL pour garantir la sécurité et la fiabilité des dispositifs utilisés. Il est vrai que ces systèmes ne comportaient de toute façon pas de véritable scellement du dispositif de vote, c'est-à-dire un procédé permettant de déceler toute modification du dispositif utilisé lors de l'élection par rapport à celui analysé par l'expert.

En ce qui concerne l'anonymat du vote, la CNIL a toujours recommandé la mise en œuvre de procédés rendant impossible l'établissement d'un lien entre le nom de l'électeur et l'expression de son vote. Il en résulte que la gestion du fichier des votes et celle de la liste d'émargement doit être faite sur des systèmes informatiques distincts, dédiés et isolés avec des chiffrements de haut niveau. La CNIL a constaté, sur les derniers dossiers, que les données figuraient sur des bases distinctes mais sur un même serveur utilisé, parfois pour plusieurs élections en même temps. La CNIL a donc rappelé qu'il convient d'opter pour une séparation tant logique que physique de la liste des électeurs et de leurs votes.

Au-delà du contrôle de la CNIL en amont lors de l'accomplissement des formalités préalables prévues par la loi du 6 janvier 1978, la CNIL a aussi rappelé, toujours dans un souci de transparence, la nécessité que les opérations électorales soient placées sous le contrôle d'une commission en mesure de veiller à la confidentialité du vote et à la sincérité du scrutin. En particulier, il paraît indispensable à la CNIL qu'elle comprenne des experts indépendants et des représentants des candidats et du corps électoral, ayant reçu toute l'information nécessaire sur le dispositif technique mis en place. La CNIL dispose, enfin, d'un pouvoir de contrôle et de sanction qu'elle peut mettre en œuvre si nécessaire.

La CNIL a fait le choix d'un haut niveau d'exigence en matière de vote électronique. Ce choix est aujourd'hui unanimement reconnu comme ayant conduit à faire progresser les dispositifs techniques et à améliorer la confidentialité des données à caractère personnel. Il appartient à chaque organisateur d'élections de se positionner par rapport aux recommandations de la CNIL et d'assumer la responsabilité d'un système qui ne s'y conformerait pas pleinement. On peut signaler que l'élection au conseil de l'ordre du barreau de Paris a donné lieu à un contentieux qui n'est pas encore épuisé. Il y a fort à parier que d'autres scrutins électroniques connaîtront le même sort.

16. Délibération n° 2005-067 du 21 avril 2005 sur les élections aux conseils de l'ordre des pharmaciens ; délibérations 2005-272 à 274 du 17 novembre 2005 sur les élections aux barreaux de Paris, Nanterre et Lyon ; délibération n° 2005-275 du 17 novembre 2005 sur les élections aux conseils de quartier d'Issy-les-Moulineaux.

LE PARTAGE DES DONNÉES MÉDICALES PERSONNELLES

Le point sur le dossier médical personnel

Il y a maintenant un an et demi, le Parlement adoptait la loi du 13 août 2004 portant réforme de l'assurance maladie dont une des dispositions centrales est la mise en place du dossier médical personnel. Institué par l'article L. 161-36-1 du Code de la Sécurité sociale afin de favoriser la coordination, la qualité et la continuité des soins, le dossier médical personnel (DMP) dont disposera chaque bénéficiaire de l'assurance maladie, dans les conditions et sous les garanties prévues à l'article L. 1111-8 du Code de la santé publique et dans le respect du secret médical, sera constitué des données mentionnées à l'article précité, notamment des informations qui permettent le suivi des actes et prestations de soins. Le législateur a fixé au 1er juillet 2007 la date à laquelle tout bénéficiaire de l'assurance maladie doit pouvoir disposer d'un dossier médical personnel.

La création en avril 2005 du groupement d'intérêt public de préfiguration du dossier médical personnel - le GIP DMP - a donné une nouvelle impulsion au projet. Une phase de préfiguration du DMP doit être lancée au cours du premier semestre 2006 auprès d'un certain nombre de sites retenus qui feront appel à des hébergeurs de données de santé à caractère personnel. Six candidats hébergeurs pour cette phase de préfiguration ont été retenus à l'issue d'un appel d'offres lancé par le GIP DMP en juillet 2005. Ils devront toutefois préalablement être agréés par le ministre de la Santé après avis de la CNIL et d'un comité d'agrément selon la procédure prévue par la loi. Il est prévu que chaque hébergeur exploite 5 000 dossiers médicaux chacun. La CNIL devra être saisie par le GIP DMP d'une demande d'autorisation pour le lancement des phases de préfiguration.

Le cadre juridique exigé pour le lancement des phases de préfiguration

Dans la mesure où le législateur a rappelé dans la loi du 13 août 2004 sa volonté que le DMP se développe dans des conditions permettant de garantir tant sur le plan juridique que technique la confidentialité des données de santé et où la CNIL, dans sa délibération du 10 juin 2004 sur le projet de loi portant réforme de l'assurance maladie, a également insisté sur ces garanties, il est essentiel que les modalités d'agrément des hébergeurs et les règles de conservation et de transmission par voie électronique entre les professionnels de santé des informations médicales soient définies dès le lancement de la phase de préfiguration.

Le décret relatif à l'hébergement de données de santé à caractère personnel, sur le projet duquel la CNIL s'est à nouveau prononcée le 15 mars 2005, a été publié au *Journal officiel* du 5 janvier 2006 et prévoit donc un agrément par le ministre de la Santé après avis de la CNIL et d'un comité d'agrément placé auprès de lui. La CNIL devrait donc prochainement être saisie par le ministre de la Santé des dossiers des six hébergeurs.

Le projet de décret pris en application de l'article L. 1110-4 du Code de la santé publique et de l'article L. 161-36-1 A du Code de la Sécurité sociale qui doit déterminer les règles de conservation et de transmission par voie électronique entre les professionnels de santé des informations médicales a été examiné par la CNIL le 11 octobre 2005. Ce texte détermine en particulier les cas dans lesquels l'utilisation de la carte de professionnel de santé (CPS) est obligatoire. La CNIL a souhaité que soient plus précisément énumérées les mesures de sécurité qui devront figurer dans le protocole de confidentialité et destinées à garantir la confidentialité des données.

Il restera en tout état de cause à la CNIL à examiner les autres textes prévus par la loi, notamment celui concernant les conditions d'accès aux différentes catégories d'informations qui figureront au DMP et le texte pris en application de l'article 5 de la loi du 13 août 2004 qui détermine les conditions dans lesquelles un identifiant peut 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.

La transmission de données à l'assurance maladie complémentaire

Questions à ...

Jean-Pierre de LONGEVIALLE

Conseiller d'État honoraire

Commissaire en charge du secteur « Santé »

La CNIL a-t-elle poursuivi l'examen des expérimentations ?

Dans la ligne des conclusions du rapport de Christian Babusiaux et en se fondant sur la disposition du III de l'article 8 de la loi du 6 janvier 1978 modifiée en 2004 relative au traitement des données sensibles (dont les données de santé) « appelées à faire l'objet à bref délai d'un procédé d'anonymisation » reconnu conforme par la Commission, celle-ci avait autorisé en 2004 la Fédération nationale de la mutualité française à expérimenter, pendant une durée limitée à un an, un traitement comportant l'exploitation dans une base statistique de codes détaillés d'actes et de médicaments après transformation des données d'identification de l'assuré en un numéro d'anonymat irréversible. Sur le même fondement de l'anonymisation à bref délai et par une délibération en date du 3 février 2005 la Commission a également autorisé la société Axa à accéder, à titre expérimental et pendant la même durée d'un an, à certaines données de santé figurant sur les feuilles de soin électroniques de ses assurés.

Le dispositif concerne des pharmacies volontaires qui émettent, en utilisant leurs logiciels SESAM Vitale, des demandes de remboursement contenant des détails à destination du système informatique de la société Axa France. Ces flux seraient sécurisés par les dispositifs standards prévus dans les logiciels de télétransmission.

La Commission a demandé que le système d'information de la société Axa France qui comporte à la fois le dispositif d'accueil SESAM Vitale et le module de chiffrement de la société Axa soit scellé et que le logiciel d'anonymisation fasse l'objet d'une expertise indépendante dont les résultats seront communiqués à la Commission.

La CNIL a-t-elle été saisie d'autres dispositifs mis en œuvre par des sociétés d'assurance maladie complémentaire ?

Oui, elle a été saisie par la société Swisslife d'un traitement de données à caractère personnel mis en œuvre à titre expérimental, dont l'objet est de permettre à son sous-traitant, la société Almerys, d'accéder, pour son compte et avec le consentement des intéressés, aux données de santé contenues dans les feuilles de soin électroniques nécessaires à la liquidation rapide des prestations prévues dans les contrats d'assurance maladie complémentaire souscrits par ses assurés. Le consentement de l'assuré s'exprimera par la remise au professionnel de santé d'une carte à puce spécifique qui sera lue sur le poste de travail de ce dernier.

Le message transmis à Almerys comportera la double signature électronique de l'assuré et du professionnel de santé. Un numéro chiffré, différent à chaque utilisation de la carte, sera produit à partir du numéro d'anonymat contenu dans la puce, aucune donnée identifiante ne circulant ainsi entre le poste du professionnel de santé et la plate-forme de la société Almerys.

Quelle suite sera donnée à ces expérimentations ?

La Commission devra procéder, ainsi qu'elle l'a indiqué à l'occasion de l'examen de chacun de ces projets, à une nouvelle appréciation de ces applications, en particulier au regard des bilans qui doivent lui être adressés. Il faudra évaluer la nécessité pour ces organismes d'assurance complémentaires de disposer de données identifiantes associées à des données de santé détaillées pour la liquidation des prestations complémentaires.

LES ANNUAIRES ET SERVICES DE RENSEIGNEMENTS UNIVERSELS

Prévue dès 1996 par la loi de réglementation des télécommunications, la mise en œuvre de l'annuaire universel a connu de nombreux retards, notamment du fait de l'évolution du cadre législatif et réglementaire qui s'y applique.

La publication du décret du 27 mai 2005 vient définitivement compléter le cadre juridique applicable aux annuaires et services de renseignement universels qui ont vocation à regrouper les coordonnées de tous les abonnés à la téléphonie, quel que soit leur opérateur. Les opérations de communication auprès des clients des opérateurs se sont mises en place à la fin de l'année 2005 afin de permettre la constitution des listes d'abonnés ou d'utilisateurs en y intégrant les diverses options relatives à la protection des données à caractère personnel. Les opérateurs devront transmettre ces listes à toute personne souhaitant éditer, au niveau national ou local, un annuaire universel ou fournir un service universel de renseignements.

Les conditions d'inscription des utilisateurs dans les annuaires universels

Les abonnés à la téléphonie fixe peuvent s'opposer gratuitement à l'inscription de leurs coordonnées dans les listes constituées par les opérateurs (inscription en « liste rouge »).

Les utilisateurs de téléphonie mobile (abonnement ou formule prépayée) peuvent demander à figurer dans ces listes. À défaut, ils bénéficient de la protection de la « liste rouge ».

Tout utilisateur peut demander :
– que son adresse postale n'apparaisse pas ou que ces listes ne comportent pas de référence à son sexe (prénom masqué), ces deux possibilités pouvant être restreintes en cas d'homonymie ;
– que les données à caractère personnel le concernant ne soient pas utilisées à des fins de prospection directe, sauf en ce qui concerne les services de l'opérateur lui-même. Les utilisateurs qui auront effectué ce choix seront directement identifiables dans les annuaires par un signe distinctif ;
– à ne pas pouvoir être identifié à partir de son seul numéro de téléphone ;
– sous sa responsabilité, à ce que sa profession soit précisée ;
– l'inscription de son adresse électronique qui apparaîtra dans les annuaires mis en ligne ;
– et, sous réserve de leur accord, l'inscription des autres utilisateurs de sa ligne.

On doit noter que ces différents droits ne s'appliquent pas qu'aux annuaires et services de renseignements universels, mais aussi aux annuaires internes que les opérateurs peuvent mettre en œuvre. Ainsi, par exemple, une inscription en liste rouge garantit à la personne de ne pas figurer sur l'annuaire universel mais aussi sur les annuaires éventuellement mis en œuvre par les opérateurs.

Par ailleurs, et conformément au souhait exprimé par la CNIL, le décret prévoit que l'inscription d'une personne en raison de son activité professionnelle ne pourra s'effectuer qu'avec son accord.

LES DONNÉES DES PASSAGERS AÉRIENS

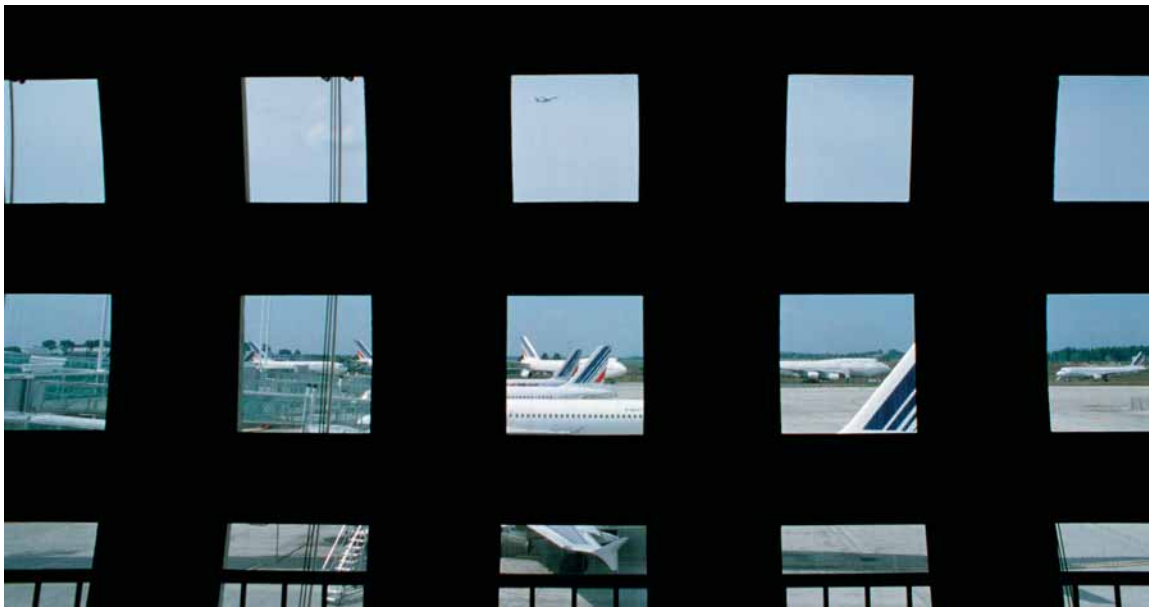
Premier bilan de l'accord Europe/États-Unis

L'accord du 28 mai 2004 entre l'Union européenne et les États-Unis qui permet aux autorités américaines d'accéder aux données détenues par les compagnies aériennes sur les passagers se rendant aux États-Unis, prévoit une évaluation annuelle. La CNIL a participé à cette première révision commune *(Joint Review)* à Washington du 19 au 22 septembre 2005 au sein de la délégation européenne, menée auprès des autorités de protection des frontières (CBP) du ministère américain de la Sécurité intérieure (DHS).

Cette première révision commune organisée sur les sites de l'aéroport international de Dulles-Washington et du Centre de traitement des données (NTC) et du CBP, poursuivait deux objectifs : vérifier, d'une part, le niveau de protection « adéquat » des données à caractère personnelles des passagers aériens, auprès du CBP autorisé, depuis l'accord, à consulter ces bases de données pour les vols entre l'Europe et les États-Unis, s'assurer, d'autre part, du respect des engagements stricts liés à cet accord.

Il en ressort un constat de mise en conformité globalement positif sur les engagements pris par le CBP mais qui n'est effectif que depuis mai 2005 : la mise en place d'un système informatique dédié pour traiter les données en provenance de 117 compagnies aériennes, un filtrage automatique des 34 champs autorisés avec blocage des données sensibles, la suppression de toutes les données collectées non conformes à l'accord de mai 2004 et la mise en place effective du système de filtrage, un tri à finalité limitative des champs ouverts, une limitation d'accès des personnes aux données. À la demande de la CNIL, le CBP s'est engagé à supprimer, dès janvier 2006, toutes les données stockées avant l'entrée en vigueur de l'accord, soit de février 2003 à mai 2004.

En revanche, les principaux points de préoccupation restent l'information aux passagers sur le traitement de leurs données comme sur leurs droits ainsi que la mise en place de façon plus active, du système *push* (envoi par les compagnies aériennes des informations sélectionnées vers les autorités américaines) afin de remplacer, en principe à fin 2005, l'accès par le *pull* (extraction par les autorités américaines de toutes les données des vols détenues par les compagnies) à toutes les données PNR concédées temporairement par l'accord. Or, ce dernier objectif reste prioritaire à court terme.



Contestation de la légalité de l'accord devant la Cour européenne

Le Parlement européen a saisi la Cour de justice des Communautés européennes et engagé deux actions en annulation, l'une contre la décision du Conseil du 17 mai 2004 et l'autre contre la décision d'adéquation de la Commission européenne.

Il conteste, d'une part, la légalité de l'accord international relatif au transfert des données passagers aux autorités américaines et sa compatibilité avec la protection du droit à la vie privée, soulignant qu'il n'existe pas aux États-Unis de protection légale des données des passagers non américains, en particulier européens, ni de droit de recours à un juge contre d'éventuelles mesures restreignant leur liberté de voyager. Il estime, d'autre part, que dans sa décision constatant le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés aux autorités américaines, la Commission européenne a excédé ses compétences d'exécution.

À ce jour, les conclusions de l'avocat général qui ne lient pas la cour ont été rendues proposant à la cour d'annuler ces deux décisions.

L'avocat général considère que la base légale de la décision du Conseil (article 95 CE - établissement du marché intérieur) est inappropriée pour permettre l'adoption de mesures de lutte contre le terrorisme et autres crimes graves (but et contenu de l'accord avec les États-Unis). L'examen, à titre subsidiaire, du moyen relatif à la violation du droit au respect de la vie privée, a été considéré comme non fondé.

En ce qui concerne la décision d'adéquation, l'avocat général estime qu'elle ne pouvait être prise par la Commission européenne car elle ne relève pas du droit communautaire puisqu'elle porte sur des activités étatiques relatives à des domaines du droit pénal. L'arrêt sera rendu en 2006.

Bons points !

L'accord international CE/Canada constitue un exemple «d'équilibre acceptable» entre le besoin de sécurité des vols et la protection des données à caractère personnel.
Signé en octobre 2005, il présente un cadre juridique bien meilleur du point de vue de son contenu. Les points d'amélioration suivants ont été reconnus tant par le groupe de l'article 29 que par le Parlement européen :
– le Canada dispose, à l'inverse des États-Unis, d'un système législatif de protection des données ;
– les «engagements» du Canada créent des droits d'accès, de rectification et d'opposition pour les passagers (citoyens de l'Union européenne) en liant également l'administration canadienne ;
– les données PNR demandées sont plus limitées (vingt-cinq éléments) et sans «catégories ouvertes» ;
– des délais de conservation limités à 72 heures avec accès à un nombre restreint d'agents et un contrôle des flux de données par l'autorité de protection canadienne ;
– un système *push* en fonctionnement avec les compagnies aériennes dès le début de l'accord.
Cet accord CE/Canada entrera en vigueur à l'issue d'une transposition des engagements par une loi canadienne début 2006.

LA DIFFUSION ET LA RÉUTILISATION DES DONNÉES PUBLIQUES

Un régime protecteur des données à caractère personnel institué par l'ordonnance du 6 juin 2005

De nombreux documents produits par les administrations d'État, les collectivités locales ou les organismes privés gérant des services publics contiennent des données à caractère personnel (listes électorales, fichier de gestion des bénéficiaires de prestations, cadastre, fichiers fiscaux…). Au sens de l'ordonnance du 6 juin 2005 [17], il s'agit de documents administratifs qui, par principe, bénéficient désormais des nouvelles dispositions de la loi du 17 juillet 1978 modifiée sur l'accès, la diffusion et la réutilisation de tels documents. Cette ordonnance a, non seulement, étendu la compétence de la CADA et lui a donné un pouvoir de sanction en matière de réutilisation de ces documents, mais a aussi permis de clarifier la situation, souvent confuse, de la diffusion et de la réutilisation par des tiers de documents administratifs.

L'article 7 de la loi du 17 juillet 1978 modifiée précise désormais que, sauf dispositions législatives contraires, les documents administratifs qui comportent des mentions entrant dans le champ d'application de l'article 6 de cette loi (secret de la vie privée et des dossiers personnels) ne peuvent être diffusés publiquement qu'après avoir fait l'objet d'un traitement afin d'occulter lesdites mentions ou de rendre impossible l'identification des personnes qui y sont nommées et, d'une manière générale, la consultation de données à caractère personnel. La CNIL a souligné, dans l'avis qu'elle a rendu le 19 mai 2005 sur le projet d'ordonnance du gouvernement, l'intérêt de procéder à ces effacements pour assurer, en particulier, le secret de la vie privée des personnes dont les données seraient appelées à faire l'objet d'une diffusion publique, notamment par voie électronique.

En second lieu, l'article 13 de la loi du 17 juillet 1978 dispose désormais que toute réutilisation d'informations publiques contenant des données à caractère personnel est soumise aux dispositions de la loi du 6 janvier 1978.

Cette disposition conduira, notamment, à soumettre à l'accomplissement de formalités préalables auprès de la CNIL tout traitement, du fournisseur ou du demandeur des données, visant à réutiliser de telles données.

En troisième lieu, l'article 13 de la loi du 17 juillet 1978 restreint la réutilisation des informations publiques comportant des données personnelles à trois cas. Le premier est celui où la personne intéressée a donné son consentement à cette réutilisation. La CNIL a estimé que le recueil préalable du consentement de l'intéressé à la réutilisation de ses informations ne saurait être envisagé que dans la mesure où ce consentement serait réellement libre et éclairé. À cet effet, la personne devra être précisément informée de l'objet de la réutilisation envisagée et des conséquences de son acceptation. Le consentement à la réutilisation des informations personnelles ne devrait pas être lié à l'attribution d'un droit ou d'une prestation.

L'article 13 prévoit également que la réutilisation des informations publiques contenant des données à caractère personnel est possible si l'autorité détentrice est en mesure de les rendre anonymes. Le décret du 30 décembre 2005 [18] a utilement ajouté que si l'anonymisation des données à caractère personnel entraînait « des efforts disproportionnés », l'autorité détentrice devait refuser de les communiquer.

Le troisième cas est celui où un texte législatif ou réglementaire autorise spécifiquement une telle réutilisation.

La CNIL désormais présente au sein de la CADA

La loi du 17 juillet 1978 confie au président de la CNIL le soin de proposer une personnalité qualifiée dans le domaine de l'informatique ou de la protection des données pour siéger au sein de la CADA. Alex Türk, président, a proposé comme membre titulaire, Jean Massot et comme membre suppléant Emmanuel de Givry, tous deux membres de la CNIL.

17. Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.

18. Décret n° 2005-1755 du 30 décembre 2005 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, pris pour l'application de la loi n° 78-753 du 17 juillet 1978 et qui a été soumis pour avis à la CNIL (délibération n° 2005-312 du 20 décembre 2005).

RÉFLEXIONS EN COURS

L'IDENTITÉ ÉLECTRONIQUE

La lutte menée par les pouvoirs publics contre la falsification des titres d'identité s'appuie sur les récents développements des technologies de l'information et de la communication. Les cartes à puce lisibles sans contact et la biométrie vont ainsi profondément modifier les modalités de délivrance et le contenu de la carte nationale d'identité et du passeport.

Les enjeux informatique et libertés du passeport électronique

La CNIL a rendu un avis, le 22 novembre 2005, sur le projet de décret instituant le passeport électronique et sur ses modalités de production sécurisée.

Photographie numérisée et biométrie

La photographie faisait déjà partie des données à caractère personnel traitées dans le cadre de l'émission du passeport. Le décret du 30 décembre 2005 relatif aux passeports électroniques prévoit qu'elle doit désormais être intégrée sous une forme numérisée, d'une part, dans le titre (à la place de l'actuelle photographie collée) comme c'est déjà le cas pour la carte nationale d'identité et, d'autre part, dans son composant électronique (puce sans contact). Cette modification du contenu du passeport a pour but, d'après le règlement européen du 13 décembre 2004 qui la rend obligatoire, de *« mieux sécuriser le passeport, par l'établissement d'un lien plus fiable entre ce titre et son titulaire grâce à l'introduction d'éléments de sécurité communs et à l'intégration d'identificateurs biométriques interopérables »*.

Le ministère de l'Intérieur n'envisage pas aujourd'hui que la photographie numérisée du détenteur du passeport soit utilisée, en France, dans le cadre de dispositifs automatisés de reconnaissance faciale. Le dispositif étant interopérable, la mise en place de tels traitements biométriques est en revanche susceptible d'intervenir à l'étranger, sur décision des seules autorités du pays concerné.

C'est nouveau

Le passeport électronique

Le passeport électronique a pour objectif premier la prévention et la lutte contre la fraude documentaire grâce à de nouvelles modalités de production, à l'insertion dans ce passeport de la photographie numérisée de son détenteur et d'un composant électronique (puce sans contact) contenant des données relatives à son détenteur et à sa délivrance, ainsi qu'à la mise en place de transmissions de données relatives aux passeports volés ou perdus vers le système d'information Schengen et vers Interpol.
Le passeport électronique doit également permettre, à terme, la simplification de la vie quotidienne des Français en devenant un véritable titre d'identité qui pourra être utilisé pour l'accomplissement de certaines formalités administratives ou commerciales.
Il est enfin prévu que les services de la police et de la gendarmerie nationales spécialement chargés de la prévention et de la répression du terrorisme puissent accéder au système d'information (fichier national des passeports) dans le cadre de leurs missions.

Éviter la captation frauduleuse des données enregistrées dans la puce sans contact

Conformément au règlement européen du 13 décembre 2004, le composant électronique du passeport est une puce sans contact, c'est-à-dire notamment un processeur et un lieu de stockage de données numériques accessibles à faible distance par un lecteur répondant à des spécifications techniques particulières. C'est la première fois que cette technologie sans contact est utilisée en France dans le cadre de documents d'identité.

Le passeport électronique permettra bientôt de certifier l'identité de son titulaire. Ainsi, le nouveau passeport sera, à terme, communément utilisé dans la sphère publique (lors des démarches auprès des services de l'État, des collectivités territoriales ou des organismes de sécurité sociale) et dans la sphère privée (par exemple, pour l'ouverture d'un compte bancaire). Compte tenu des risques de captation frauduleuse des données liées à la technologie sans contact, la CNIL considère que le recours à une telle technologie nécessite, de façon générale, la mise en place de sécurités appropriées.

Les mesures techniques et les garde-fous juridiques présentés par le ministère de l'Intérieur sont de nature à garantir l'authentification, la confidentialité et l'intégrité des données enregistrées sur le composant électronique du passeport. À titre d'illustration, les données ne pourront être lues que si le passeport est présenté ouvert ; les échanges de données entre la puce et le lecteur seront cryptés ; le contenu de la puce sera limité aux informations figurant déjà sur le passeport.

Mieux contrôler les accès au fichier national des passeports

Afin de renforcer la sécurisation de la production des passeports, ces derniers ne seront plus produits localement mais de façon centralisée. Un centre de personnalisation du passeport sera ainsi mis en place.

La CNIL a pris acte des précautions particulières qui seraient prises en cas d'externalisation de la production : engagement contractuel du prestataire de préserver la sécurité des données traitées et de ne pas les utiliser à des fins détournées, conservation des données de production limitée à trois mois, contrôle du respect des mesures de sécurité exigées par le ministère. Elle a souligné l'importance du contrôle des accès au fichier national des passeports et a demandé à être informée, dans un délai de trois mois, du renforcement des mesures prises à cet effet.

La CNIL a également demandé que l'accès prochainement ouvert au bénéfice des services de police et de gendarmerie chargés de la lutte antiterroriste s'accompagne de la désignation d'une personne chargée d'assurer le contrôle effectif de ces consultations et de la remise d'un bilan annuel des contrôles opérés sur ces accès.

À l'horizon

Le projet identité nationale électronique sécurisée (INES)

En synergie avec le passeport électronique, le projet INES de carte d'identité électronique et biométrique devrait voir le jour en 2008. Conçu selon des normes d'interopérabilité, la carte d'identité électronique sera lisible dans tous les pays équipés de lecteurs de cartes à puce sans contact, en particulier en Europe. Elle devrait également pouvoir être utilisée pour accéder à des téléservices en certifiant l'identité électronique de son détenteur. La détention de ce titre d'identité devrait demeurer facultative. Les données stockées dans la puce de la carte comporteront notamment les empreintes digitales et la photographie de son détenteur.

Le projet de carte d'identité nationale électronique sécurisée (INES)

La CNIL suit depuis plusieurs années le développement du projet INES. Il s'agit en effet d'une question de société majeure autour de l'identification, par des moyens biométriques, de l'ensemble de la population française. On peut en effet légitimement se poser un certain nombre de questions :
– Une base de données centralisée d'empreintes digitales est-elle nécessaire pour la délivrance sécurisée des cartes d'identité ?
– Qui pourrait accéder à cette base de données et à quelles fins ?
– Qui en contrôlerait les usages ?
– Quelles seraient les solutions alternatives ?

C'est pourquoi la CNIL a demandé au ministère de l'Intérieur un argumentaire précis sur le projet de carte d'identité électronique. Elle a également obtenu que les autorités européennes de protection des données prennent une position commune sur les projets européens en matière de biométrie. Elle a par ailleurs recueilli le point de vue de personnalités, d'historiens, de sociologues, de philosophes, de responsables d'associations des droits de l'Homme et d'organisations syndicales sur ce projet. Elle a enfin pris l'attache des industriels du secteur et des chercheurs afin de disposer d'un éclairage technologique complet.

Pour nourrir le débat, la CNIL a lancé, au début de l'année 2005, des premières pistes de réflexion et publie sur son site web un dossier d'information (la carte d'identité aujourd'hui, le projet du ministère de l'Intérieur, la carte d'identité à l'étranger, les avis précédemment rendus par la CNIL et les instances de protection des données sur le sujet …), ainsi que le compte rendu des auditions auxquelles elle avait procédé.

La CNIL devrait être saisie du projet de loi portant création de la carte d'identité INES au cours du premier semestre 2006.

LA GÉOLOCALISATION DES VÉHICULES DES SALARIÉS

La CNIL est saisie d'un nombre important de demandes de conseil ou de plaintes tant de la part des employeurs que des employés qui s'interrogent sur le cadre juridique applicable à la mise en œuvre de dispositifs permettant de géolocaliser les véhicules. Ces dispositifs sont principalement basés sur l'utilisation de la technologie GSM/GPS qui permet, par exemple, d'afficher sur une carte à un instant donné la position d'un véhicule équipé d'un système de géolocalisation. Ce faisant, ils permettent un contrôle étroit de l'activité de l'employé qui utilise le véhicule.

La mise en place d'un outil de géolocalisation présente des risques certains tant au regard des droits collectifs (droit syndical, droit de grève) que des libertés individuelles (liberté d'aller et venir anonymement, droit à la vie privée). Ces traitements soulèvent donc deux questions : celle de la frontière entre travail et vie privée et celle du niveau de contrôle permanent qu'il est admissible de faire peser sur un employé.

La Commission a, dès à présent, identifié les problématiques relatives à l'utilisation d'outils de géolocalisation dans le contexte professionnel et compte préciser dans une recommandation les conditions dans lesquelles ces dispositifs peuvent être utilisés dans ce cadre.

En premier lieu, l'utilisation d'un outil de géolocalisation doit répondre à un besoin spécifique lié à la nature même de l'activité exercée par l'employeur. Le respect de ce principe de finalité est de nature à éviter une surveillance disproportionnée des employés qui ne serait pas justifiée par la nature des tâches qu'ils ont à accomplir. La CNIL souhaite donc définir de manière la plus précise possible les cas dans lesquels la mise en œuvre d'un outil de géolocalisation peut être admise.

En second lieu, les conditions de mise en œuvre des outils de géolocalisation doivent être précisément déterminées. La CNIL abordera dans sa recommandation la question de la désactivation par l'employé lui-même de la fonction de géolocalisation, du traitement par l'employeur de la vitesse du véhicule et des données qui y sont associées, de la durée de conservation de ces données ou encore des conditions d'accès et de sécurité applicables à ce traitement.

La CNIL a lancé sur ce sujet au cours de l'année 2005 une consultation très large des acteurs concernés, à savoir les ministères compétents (du travail, de la fonction publique et des transports), les organisations professionnelles et syndicales et les intégrateurs de services de géolocalisation, c'est-à-dire les entreprises proposant la mise en place de ce type d'outils.

L'ensemble de ces éléments devrait permettre à la CNIL de définir précisément dans quel cadre peuvent être mis en œuvre des outils de géolocalisation au sein du contexte professionnel en prenant en compte, d'un côté, les intérêts légitimes des entreprises et, de l'autre, le nécessaire respect des droits des employés.

VERS UNE DÉFINITION EUROPÉENNE DE LA NOTION DE DONNÉE À CARACTÈRE PERSONNEL

Qu'est-ce qu'une « donnée à caractère personnel » ? Cette interrogation est fondamentale, puisqu'elle conditionne l'applicabilité des règles françaises et européennes de protection des données et définit ainsi l'étendue de la protection accordée aux personnes dont les données font l'objet d'un traitement.

Une interprétation traditionnellement large

La CNIL a toujours interprété la notion de données à caractère personnel de manière large. La loi française, les lignes directrices de l'OCDE, la convention 108 et la directive européenne 95/46 autorisent d'ailleurs une telle interprétation. Le législateur français avait ainsi, dès 1978 retenu la notion d'« informations directement ou indirectement nominatives » ; la loi d'août 2004 définit désormais la donnée personnelle comme « *toute information relative à une personne physique qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* » (article 2 alinéa 2 de la loi du 6 janvier 1978 modifiée en août 2004).

C'est en maniant les notions d'« informations indirectement nominatives » ou d'« informations relatives à une personne physique identifiable », que la CNIL et ses homologues européens ont progressivement appliqué les règles de protection des données personnelles à des cas de figure extrêmement divers (plaque d'immatriculation d'un véhicule, numéro de téléphone, adresse IP, empreintes digitales, tests psychotechniques ou psychologiques, mais aussi statistiques qui, agrégées à un niveau insuffisant, permettent indirectement l'identification des personnes auxquelles elles s'appliquent, etc.).

Apport du document de travail du groupe de l'article 29 sur la technologie RFID

Le groupe de l'article 29 a adopté, le 19 janvier 2005, un document de travail WP105 sur les questions de protection des données liées à la technologie RFID. Ce document marque une nouvelle évolution de la définition de la notion de donnée à caractère personnel. Il pose en effet le principe que les données traitées dans ces circonstances sont bien des données personnelles, même s'il s'agit de données ne portant que sur des objets, dès lors que la technologie RFID permet de constituer un maillage dense d'analyse des milliers d'objets qui entourent une personne. Il consacre ainsi une extension de la notion de données à caractère personnel, préconisée par ailleurs par la CNIL dont les travaux ont inspiré ceux du groupe sur ce sujet. Soucieux de mesurer l'impact de cette évolution, le groupe a décidé d'aller plus loin dans cette analyse et a officiellement porté au programme de l'année 2006 une réflexion approfondie sur la notion de données à caractère personnel au sens de la directive 95/46.

La position britannique : la jurisprudence « Durant »

La décision rendue par la Cour d'appel britannique dans l'affaire « Durant » ne manquera pas d'être évoquée durant ces travaux européens. Cette décision de 2003 a pour effet de restreindre de manière substantielle la notion de données à caractère personnel au Royaume-Uni, en retenant une interprétation restrictive du terme « *relatives à* », utilisé par la loi britannique de protection des données personnelles pour définir la notion de données à caractère personnel (« *données relatives à une personne physique identifiée ou identifiable* »).

Selon la Cour d'appel, ne peuvent être considérées comme des « données relatives à une personne », au sens de la loi et de la directive, que des données de nature « biographique » ou véritablement « centrées » sur la personne concernée. Autrement dit, la cour réfute une interprétation plus large qui aurait recouvert toutes les données « ayant un quelconque lien avec », ou « portant sur » la personne concernée. Sur cette base, ainsi que sur une interprétation restrictive de la notion de « fichier », la Cour conclut à la non-application, en l'espèce, des règles relatives au droit d'accès aux fichiers de l'autorité de contrôle financière britannique.

L'impact de cette décision, que l'autorité britannique de protection des données a par ailleurs repris à son compte, revenant sur sa doctrine antérieure, contraste fortement avec le mouvement européen tendant à l'extension de la notion.

GÉNÉALOGIE ET PROTECTION DES DONNÉES PERSONNELLES

La démocratisation de l'accès au réseau internet et la diffusion des outils facilitant la diffusion ou la recherche d'informations généalogiques ont contribué à soutenir l'engouement français pour la généalogie. Si ces outils facilitent les recherches généalogiques et leur diffusion, ils sont également porteurs de certains risques, notamment de captation à des fins commerciales de l'identité des personnes recensées dans des arbres généalogiques mis en ligne. Ces dérives sont d'autant plus dangereuses que ces compilations d'informations peuvent concerner des personnes vivantes, majeures comme mineures.

Une application modulée de la loi « informatique et libertés »

Dans certains cas, la loi ne s'applique pas

Certains fichiers généalogiques échappent totalement à l'application de la loi du 6 janvier 1978. Il s'agit, en application de l'article 2 de la loi, des fichiers « *mis en œuvre pour l'exercice d'activités exclusivement personnelles* » (par exemple, l'arbre généalogique familial qui ne fait l'objet d'aucune diffusion).

Dans d'autres cas, la loi s'applique partiellement

La CNIL a toujours considéré que certains fichiers échappaient à l'obligation de déclaration. Ainsi, en est-il des fichiers constitués à partir d'informations issues de documents d'archives librement communicables (par exemple, arbre généalogique constitué à partir du dépouillement de registres paroissiaux ou de registres d'actes d'état civil de plus de cent ans) ou des sites internet servant à collecter ou à diffuser des données à caractère personnel mis en œuvre par des particuliers [19].

Le responsable d'un tel site doit toutefois respecter les dispositions de fond de la loi (respect des droits des personnes vivantes qui y sont recensées et respect des obligations s'imposant au maître du fichier : obligation d'information des intéressés, obligation de mise à jour, obligation de sécurité…).

Parfois, la loi s'applique totalement

Sont ainsi soumis à l'ensemble des dispositions de la loi les fichiers et sites internet qui n'entrent dans aucune des catégories ci-dessus, c'est-à-dire les plus nombreux : les sites internet « associatifs » regroupant plusieurs arbres généalogiques.

Des difficultés pratiques liées à l'exercice des droits des personnes

Les personnes dont l'identité figure dans les fichiers ou sur les sites internet soumis à la loi disposent évidemment de l'intégralité des droits reconnus par la loi (droit d'opposition, droit d'accès, droit de rectification et droit de suppression). Les droits des mineurs éventuellement recensés doivent être exercés par leurs représentants légaux.

S'agissant des personnes décédées, l'article 40 de la loi permet à leurs héritiers d'exiger que les fichiers dans lesquels figurent des informations les concernant soient mis à jour afin de prendre en compte ce décès. La Cour de cassation a, dans un arrêt du 14 décembre 1999 interprétant les dispositions de l'article 9 du Code civil, posé le principe selon lequel le droit d'agir pour le respect de la vie privée s'éteint au décès de la personne concernée, seule titulaire de ce droit. La CNIL a toutefois admis dans le passé que certaines dispositions de la loi « informatique et libertés » pouvaient trouver à s'appliquer à des fichiers recensant uniquement des personnes décédées (par exemple, dans le cas de la diffusion sur internet, par les Mormons, des registres d'état civil français anciens).

Dès lors, et à la lumière des modifications apportées par la loi en août 2004, la CNIL a décidé de procéder en 2006 à une étude générale et approfondie des enjeux et des conséquences de l'application de la loi aux fichiers constitués par des généalogistes et, plus généralement, aux fichiers de personnes décédées.

19. Cette exonération, décidée par la Commission dans une délibération du 22 novembre 2005, ne concerne pas les sites internet d'associations.

AU PROGRAMME 2006

L'EUROPE DE LA SÉCURITÉ

Les domaines de la coopération policière

Depuis les événements du 11 septembre 2001 et les attentats à la bombe de Madrid et en 2005 de Londres, l'agenda européen est fortement marqué par les mesures de lutte contre le terrorisme. Plus précisément l'échange d'information est actuellement au cœur de la coopération policière. Suite à l'adoption en juin 2005 du plan d'action de la Commission et du Conseil mettant en œuvre le programme de La Haye, visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne, nombre de propositions en matière de coopération policière ont émergé et devraient être adoptées en 2006 :
– trois nouveaux instruments juridiques venant remplacer la base actuelle de la convention d'application des accords de Schengen : une proposition de décision sur la base du troisième pilier (fonctionnement du SIS II) et deux règlements sur la base du premier pilier (SIS II et transport) ;
– l'amélioration de la coopération policière entre les États membres aux frontières intérieures et modifiant la convention d'application de Schengen (projet de décision du Conseil - 18 juillet 2005) ;
– la simplification de l'échange d'informations et de renseignements entre les services répressifs de l'ensemble de l'Union européenne (projet de décision cadre) ;
– la consultation des systèmes d'informations sur les visas (VIS) par les autorités compétentes en matière de sécurité intérieure et par l'Office européen de police Europol (proposition de décision du Conseil - 30 novembre 2005) ;
– le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergie entre ces bases (communication de la Commission - 24 novembre 2005) ;
– l'échange d'information en vertu du principe de disponibilité (projet décision cadre - 12 octobre 2005).

En outre un traité conclu à Prüm le 27 mai 2005 entre sept États, dont la France, relatif à l'approfondissement de la coopération transfrontalière, en matière de lutte contre le terrorisme, la criminalité et la migration illégale, prévoit la réalisation d'actions poussées destinées à améliorer l'échange d'information (fichiers d'analyse ADN, notamment).

Compte tenu du renforcement des mesures législatives dans le troisième pilier, il est devenu de plus en plus évident pour l'ensemble des acteurs, que le domaine de la coopération policière nécessite un corps clair et spécifique de règles sur la protection des données.

C'est précisément l'objet du projet de décision-cadre du Conseil relatif à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale présenté en octobre 2005 par la Commission. Ce texte fondamental est inscrit au calendrier d'adoption 2006, sur lequel s'appuiera le principe d'échange d'informations entre États membres. Les autorités de contrôle ont pour objectif de peser de tout leur poids dans l'équilibre échange de données/respect des droits des personnes.

Les outils biométriques au service de la coopération policière

L'Union européenne a pris la décision d'introduire des données biométriques dans les passeports, les visas et les permis de séjours à partir de 2006, en vue de fiabiliser les documents d'identification (lutte contre la fraude documentaire). Le groupe de l'article 29 a adopté, le 30 septembre 2005, un nouvel avis sur la biométrie dans les passeports et documents de voyage qui s'inscrit dans le prolongement de son avis d'août 2004 sur la biométrie dans les visas en excluant la constitution de toute base centrale contenant des données biométriques.

LES JEUNES À L'ÈRE NUMÉRIQUE (ESPACES DE TRAVAIL, BLOGS…)

Comme en témoigne, si besoin était, une étude réalisée en juillet 2005 par Médiamétrie pour la Délégation aux usages de l'internet, les nouvelles technologies de l'information occupent une place de plus en plus importante auprès des jeunes.

L'école est également devenue un vecteur de formation des jeunes aux NTIC avec notamment la mise en place progressive des espaces numériques de travail au sein des établissements scolaires.

BON À SAVOIR

96 % des jeunes interrogés déclarent utiliser régulièrement internet *.

Cependant, l'utilisation d'internet par les enfants constitue une source de préoccupation importante pour les parents et les éducateurs, conscients des dangers auxquels les enfants peuvent être confrontés sur le réseau du fait des contenus qui peuvent être illégaux ou de nature à les troubler (pornographie, racisme, violence physique et psychologique), de l'existence de messageries (avec la possibilité de contacts directs avec des tiers) ou de la collecte d'informations à des fins de prospection commerciale. L'inquiétude des parents et éducateurs se trouve d'ailleurs souvent renforcée par leur manque de maîtrise des techniques et leur sentiment de ne pas être en mesure d'apporter aux enfants qui, eux, surfent sur la toile avec aisance, les conseils de prudence et d'assistance dont ils pourraient avoir besoin. Les enfants sont par ailleurs des acteurs à part entière sur internet et peuvent porter atteinte aux droits d'autrui (exemple : les blogs aux contenus diffamatoires).

Pour toutes ces raisons, la CNIL estime essentielle la mise en place d'opérations de sensibilisation des jeunes, des parents et des éducateurs, pour une utilisation plus sûre d'internet. À cet effet, la CNIL est régulièrement sollicitée pour participer à des programmes dont l'objet est de conduire des actions de sensibilisation des enfants et de leurs parents aux enjeux et risques d'internet. La CNIL veille à chacune de ces occasions à rappeler que les garanties offertes à tous par la loi « informatique et libertés » doivent s'imposer avec encore plus de force lorsqu'il s'agit de mineurs.

La CNIL a ainsi été associée à la rédaction du rapport sur la protection de l'enfant et les usages de l'internet mis en place par le ministère des Solidarités, de la Santé et de la Famille. Remis au ministre en septembre 2005 lors de la conférence de la famille, ce rapport reprend en grande partie les préconisations de la CNIL parmi lesquelles il est possible de citer la proposition n° 4 visant à « créer un programme pédagogique destiné à une appropriation familiale de l'internet ». À ce titre, la mise en place au sein des établissements secondaires de « commissions locales informatique et libertés » (CLIL) est envisagée. Ces commissions sont destinées à être un lieu d'échanges et de discussions pour tout ce qui concerne l'utilisation des technologies de l'information et de la communication : expliciter les enjeux, présenter les risques, informer sur les droits des personnes et la protection des données. À ce jour, le seul exemple de CLIL est celui du Lycée Charles-de-Gaulle à Muret (Haute-Garonne). La désignation de correspondants informatique et libertés chargés en particulier d'animer les CLIL au sein des établissements pourrait également être envisagée.

La CNIL participe également à deux projets développés en partenariat avec le ministère de l'Éducation nationale, à savoir le projet Serinette pour la sensibilisation des enfants de 7 à 11 ans et le projet Confiance, plan français d'action et de sensibilisation financé par la Commission européenne dans le cadre de son plan d'action pour un internet plus sûr.

* Ce sondage a été réalisé auprès de 1 500 individus représentatifs de la population âgés de 11 ans et plus.
Source : Médiamétrie - Baromètre DUI - juillet 2005.

LA VIOLENCE DANS LES STADES

La multiplication des événements sportifs d'envergure liés au football (finale de la Ligue des champions organisée à Paris au mois de mai 2006, Coupe du Monde 2006 organisée en Allemagne) et les débordements parfois constatés dans certains stades ont ravivé le thème de la sécurité dans les enceintes sportives. Les organisateurs de ces événements peuvent être légitimement tentés de recourir au fichage informatique pour sélectionner les spectateurs.

Ainsi l'attention de la Commission a été attirée sur les conditions dans lesquelles la Fédération française de football (FFF), à l'occasion du match France-Allemagne du 12 novembre 2005, avait procédé à l'enregistrement des données telles que le nom, prénom adresse et numéro de carte d'identité des spectateurs français. Telle qu'elle était organisée, cette opération, présentée comme répondant à des objectifs de sécurité, ne respectait pas les dispositions de la loi, notamment parce que l'utilisation de ces données n'était pas clairement définie et parce que cette collecte n'avait pas été déclarée auprès de la CNIL. À la suite de l'intervention de la Commission, la FFF a donc décidé de stopper cette opération et d'engager une concertation avec la CNIL afin que ces différentes pratiques soient mises en conformité avec la loi « informatique et libertés ».

À côté de la possibilité reconnue à la justice de prononcer une peine d'interdiction de pénétrer ou de se rendre aux abords d'une enceinte sportive, la loi du 23 janvier relative à la lutte contre le terrorisme permet au préfet de prononcer une telle mesure, accompagnée d'une obligation de répondre, au moment des manifestations sportives, aux convocations de toute autorité ou personne qualifiée qu'il désigne, par exemple les commissariats de police.

Dans la mesure où l'application concrète de ces mesures pourrait se traduire par l'enregistrement informatique des personnes ainsi frappées d'exclusion, la CNIL veillera au cours de l'année 2006 à ce que la mise en place de ces dispositifs se fasse en parfaite conformité avec la loi « informatique et libertés ».

Questions à …

Francis DELATTRE

Député du Val-d'Oise

Commissaire en charge du secteur « Affaires culturelles »

Pourquoi la CNIL s'intéresse-t-elle aux problèmes liés à la sécurité dans les stades ?

Il existe plusieurs façons de lutter contre la violence dans les stades. L'une consiste à identifier les fauteurs de trouble et les éloigner des enceintes sportives. La constitution de « fichiers de *hooligans* » ou d'une liste noire de « supporters indésirables » ne peut être envisagée que si sont respectées les dispositions de la loi « informatique et libertés ». J'ai quelques raisons de penser que certains clubs professionnels se sont engagés dans cette voie sans prendre toutes les précautions utiles et notamment sans faire de déclaration à la CNIL.

Quels seront les axes de l'action de la CNIL sur cette question ?

La CNIL engagera une concertation avec la Ligue de football professionnel (LFP) et de la Fédération française de football (FFF) sur les modalités de mise en œuvre des textes visant à exclure les fauteurs de trouble des stades, notamment afin de s'assurer du respect des dispositions de la loi du 6 janvier 1978 modifiée. De plus, la volonté de la CNIL est d'entamer, en partenariat avec les instances professionnelles compétentes et les pouvoirs publics, une réflexion sur le besoin, ou non, d'identifier les spectateurs lors de l'organisation d'organisations sportives, au premier desquelles, les matchs de football. Cette question est, pour l'instant, largement ouverte.

La vidéosurveillance dans les stades pose-t-elle des problèmes particuliers ?

Justifiée par des raisons de sécurité, opérée dans un lieu privé ouvert au public, elle relève de la loi de 1995 et échappe donc à la compétence de la CNIL. Toutefois, il n'en serait pas de même si les images de certains spectateurs venaient alimenter les fichiers mentionnés *supra*. Fondamentalement, le spectateur ne vient pas au stade pour être lui-même filmé.

LA PROSPECTION POLITIQUE

La CNIL a été saisie, au cours de l'année 2005, de plaintes d'internautes concernant la réception de courriers électroniques relatifs à un parti politique. En effet, la récente campagne de communication par courrier électronique de l'UMP a soulevé le mécontentement de nombreux internautes qui estiment ne jamais avoir autorisé l'UMP à utiliser leur adresse de courrier électronique et assimilent ces messages à du « spam ».

Au vu des premiers éléments portés à la connaissance de la Commission, il apparaît que les adresses de courriers électroniques des personnes démarchées proviennent de fichiers constitués par des sociétés spécialisées dans la location de fichiers. Les personnes figurant dans ce type de fichiers semblent avoir accepté, lors de la collecte de leurs données, que celles-ci soient mises à disposition de tiers afin qu'il leur soit adressé des offres commerciales ciblées, avec la possibilité de s'y opposer à tout moment. Il est important de souligner que les coordonnées utilisées n'ont jamais été portées à la connaissance de l'UMP.

Il existe cependant une différence entre une utilisation des données à des fins de prospection commerciale et une utilisation des données à des fins de communication politique. Sur ce point, il ressort des premiers éléments dont dispose la Commission que l'utilisation à des fins de communication politique n'était pas envisagée, c'est-à-dire que les personnes destinataires des courriers électroniques n'ont pas été informées de la possible utilisation de leurs coordonnées pour l'envoi de messages à caractère politique.

Or, la CNIL a, dans une recommandation du 3 décembre 1996 relative à l'utilisation de fichiers à des fins politique, rappelé que les personnes figurant dans un fichier du secteur privé doivent être informées de la possibilité que leurs données soient cédées, louées ou échangées à des fins de communication politique, et avoir été mises en mesure de s'y opposer. En revanche, il n'est pas nécessaire de recueillir leur consentement préalable à recevoir de tels messages par voie électronique car cette règle ne s'applique qu'aux messages de nature commerciale.

Pour faire suite aux plaintes reçues, la CNIL a entrepris, dans un premier temps, de vérifier auprès des entreprises ayant mis à disposition de l'UMP des fichiers d'adresses électroniques les conditions de collecte de ces données qui doivent satisfaire aux exigences de la loi « informatique et libertés ».

À l'issue de cette enquête, le président de la CNIL organisera une table-ronde pour dialoguer avec les partis politiques au sujet des conditions dans lesquelles des fichiers peuvent être utilisés pour des actions de communication et de prospection politiques, par mél ou SMS notamment.

Extrait de la résolution adoptée par la conférence internationale des commissaires à la protection des données

« […] *les données personnelles collectées initialement pour des activités de marketing sur la base du consentement éclairé de la personne concernée peuvent être utilisées à des fins de communication politique si ce but est spécifiquement mentionné dans la déclaration de consentement de la personne concernée* […] » Montreux 14 au 16 septembre 2005.

LES CASIERS JUDICIAIRES PARALLÈLES

En 2006, comme en 2005 les conséquences sociales de la consultation des fichiers de police judiciaire à des fins administratives resteront une préoccupation majeure pour la CNIL.

UN RISQUE RÉEL D'ATTEINTE AUX DROITS DES PERSONNES

La Commission a constaté à maintes reprises, lors des nombreux contrôles qu'elle assure au titre du droit d'accès indirect, que le recours aux fichiers de police judiciaire, dans le cadre des enquêtes administratives réalisées pour l'accès à certains emplois de sécurité ou l'assermentation à certaines fonctions, peut avoir des conséquences dramatiques pour les personnes, des refus d'embauche ou des licenciements étant décidés sur la seule consultation de ces fichiers et sur la base de signalements parfois injustifiés, erronés ou périmés.

Cette utilisation administrative des fichiers de police judiciaire leur fait jouer, de fait, aujourd'hui le rôle d'un casier judiciaire parallèle, sans les garanties rigoureuses prévues par le Code de procédure pénale pour le casier judiciaire national.

Ainsi, alors que le Code de procédure pénale, dans le souci de préserver le droit à l'oubli et de faciliter la réinsertion sociale des personnes condamnées, prévoit expressément l'exclusion de la mention de certaines condamnations sur les extraits de casier judiciaire transmis aux administrations en particulier dans le cadre d'enquêtes préalables à des recrutements, la seule connaissance, par l'autorité administrative, de l'existence d'un signalement dans le STIC sans rien connaître des suites judiciaires peut conduire sans autre forme d'examen, à l'exclusion d'un emploi ou d'une fonction.

Cette situation risque de s'aggraver d'une part avec l'élargissement considérable de la liste des enquêtes donnant lieu à consultation des fichiers de police judiciaire, que consacre le décret du 6 septembre 2005, et d'autre part, avec l'extension prévisible du champ d'application du fichier STIC à l'ensemble des contraventions de cinquième classe contre les biens, contre les personnes et contre la

Ça la **fiche** mal

◆ Madame X, âgée de 43 ans, postulant pour un emploi au sein de l'aéroport d'Orly, s'est vue refuser son assermentation, étant signalée dans le STIC. Elle saisit donc en août 2004 la CNIL qui entreprend aussitôt les démarches de vérification des fichiers auprès du ministère de l'Intérieur. Le 25 novembre 2004, la sécurité publique informe la CNIL que Madame X est connue de ses services, ce que fait aussi la police judiciaire le 13 janvier 2005 ce qui donne lieu en février 2005, à des investigations de la CNIL au ministère de l'Intérieur, au cours desquelles le magistrat de la CNIL découvre que Madame X est seulement signalée pour une affaire de non-représentation d'enfant datant de 1993… Ce signalement, compte tenu de l'ancienneté des faits, n'aurait jamais du figurer dans le STIC. Il a donc été supprimé. La CNIL a demandé que les services de police judiciaire, prennent attache avec le préfet qui avait refusé l'assermentation de Madame X afin que sa situation soit réexaminée.

◆ Monsieur L, agent de sécurité, âgé de 44 ans, a été licencié en août 2004, suite à un signalement dans le STIC pour un vol commis en 1994. Ce signalement a été supprimé car le délai de conservation de cinq ans était expiré. Mais ce dossier n'a pu être réglé qu'en mai 2005.

◆ Madame K, agent de sécurité, âgée de 24 ans, n'a pu être embauchée dans une société de sécurité et de gardiennage en septembre 2004. Elle était signalée dans le STIC pour une infraction à la législation relative aux animaux dangereux (elle promenait son chien dans la rue, non muselé et non tenu en laisse). Il y avait là une erreur d'enregistrement, cette infraction relevant d'une contravention de deuxième classe n'aurait en effet jamais du donner lieu à signalement dans le STIC. La CNIL l'a donc fait supprimer..

◆ Monsieur D, agent de sécurité, âgé de 24 ans, a été licencié à la suite d'une enquête de moralité défavorable. Il était signalé dans le STIC pour une affaire de détention de stupéfiants datant de 1999. Ce signalement a été supprimé en raison de l'expiration du délai de conservation de cinq ans pour cette catégorie d'infractions.

◆ Monsieur C, agent de sécurité depuis plus de dix ans, âgé de 33 ans, a été licencié en mai 2004. Il était signalé dans le STIC pour deux affaires : port illégal d'arme datant de 1988 - il était alors mineur ; conduite en état d'ivresse datant de 1994. Suite à l'intervention de la CNIL il a été radié du fichier, le délai de conservation des informations étant expiré.

nation, l'État ou la paix publique, extension qui n'apparaît, en l'état, aucunement justifiée.

Aujourd'hui, faute de moyens de transmission informatique, les mises à jour concernant notamment les personnes mises en cause ayant fait l'objet d'un classement sans suite ou les données relatives aux victimes ne sont pas transmises de façon régulière et rapide. La mise à jour immédiate, systématique, et rigoureuse des informations enregistrées constitue cependant une garantie essentielle pour les personnes.

Dans le contexte actuel de renforcement de la lutte contre le terrorisme, il ne s'agit aucunement pour la CNIL de contester la légitimité de l'objectif poursuivi en l'espèce par l'État qui souhaite ainsi assurer un contrôle plus étroit des activités dites sensibles mais de faire corriger les effets pervers d'un dispositif qui fondamentalement, n'a pas été conçu à l'origine pour cette fin. À cet effet la CNIL a fait part au Gouvernement d'un certain nombre de propositions pour remédier à cette situation (p.101).

Mais ainsi qu'elle l'avait souligné en 2002 lors de l'examen du projet de loi sur la sécurité intérieure la Commission estime que l'élargissement de l'accès à des informations sur les antécédents judiciaires des personnes à des fins d'enquête administrative appelle une réflexion nouvelle sur le rôle et les modalités de fonctionnement du casier judiciaire. C'est pourquoi elle a décidé de constituer en son sein un groupe de travail sur le sujet afin d'évaluer clairement les enjeux en ce domaine et de formuler des propositions auprès des pouvoirs publics.

LES LABELS

Aux termes de l'article 11 3° de la loi du 6 janvier 1978 modifiée en août 2004, la CNIL peut être saisie par des organisations professionnelles ou des institutions regroupant principalement des responsables de traitement d'une demande de délivrance d'un label à des produits ou à des procédures tendant à la protection des données, après que la Commission les a reconnus conformes aux dispositions de la loi « Informatique et libertés ».

Cette disposition est une réelle nouveauté pour la CNIL et même dans le paysage européen des autorités de la protection de données, dans la mesure où la CNIL est la seule autorité, à l'exception de l'autorité du *land* du Schleswig-Holstein (Allemagne), a disposer d'un pouvoir de labellisation.

La mise en œuvre de ce nouveau dispositif étant toutefois subordonnée à l'adoption d'un décret d'application, la CNIL n'a pas eu l'occasion, depuis la modification de la loi de 1978 introduite en août 2004, de le mettre en pratique. Elle a néanmoins entamé une réflexion sur le sujet qui fait apparaître les orientations suivantes.

Elle considère tout d'abord que la procédure de délivrance de label doit être subordonnée à une demande d'avis de conformité du produit ou de la procédure à la loi. Selon les termes mêmes de la loi, la délivrance d'un label ne peut être réalisée qu'après que la CNIL « *les* [produits ou procédures] *a reconnus conformes aux dispositions de la loi* ». Dès lors, toute demande de label équivaudra en pratique à une demande préalable de conformité.

S'agissant de la procédure permettant d'évaluer la conformité du dispositif à la législation sur la protection des données, il pourrait être envisagé, en fonction de la nature et de la complexité de la demande qui lui est soumise, soit que la Commission procède elle-même à l'évaluation du dispositif, soit qu'elle décide de faire appel à un organisme extérieur indépendant reconnu. Cette reconnaissance pourrait ainsi être fondée sur une accréditation délivrée par le Comité français d'accréditation (COFRAC) qui est le seul organisme en France à disposer des compétences, de l'expérience et de la structure nécessaires pour reconnaître l'aptitude d'un organisme à procéder à une évaluation.

Les critères décidant de la conformité ou non d'un produit ou d'une procédure à la loi de 1978 pourraient être contenus dans un document appelé « référentiel ». Celui-ci serait validé par la CNIL en concertation, le cas échéant, avec des représentants des diverses parties intéressées (professionnels, consommateurs ou utilisateurs, administrations).

Le développement des procédures de labellisation constitue un vecteur essentiel de diffusion des règles informatique et libertés permettant ainsi d'intégrer « en aval » dès la conception, les règles de protection des données et de sensibiliser de manière effective les éditeurs de logiciels et concepteurs de systèmes de sécurité à ces règles.

LES PRINCIPAUX DÉCRETS D'APPLICATION DEVANT ÊTRE SOUMIS POUR AVIS À LA CNIL EN 2006

Décrets d'application de la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

– Conditions de la communication par les opérateurs de communications électroniques des données techniques aux services de police chargés de la lutte antiterroriste.
– Conditions de la communication par les prestataires techniques internet des données d'identification aux services de police chargés de la lutte antiterroriste.
– Modalités de transmission aux services de police des données relatives aux passagers enregistrées dans les systèmes de réservation et de contrôle des transporteurs.
– Mise en œuvre de dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants.
– Liste des informations devant figurer obligatoirement dans les demandes d'avis concernant certains traitements intéressant la sûreté de l'État, la défense ou la sécurité publique.

Décrets d'application de la loi relative au traitement de la récidive des infractions pénales

– Traitement automatisé permettant le contrôle à distance de la localisation du condamné (« bracelet électronique »).
– Traitements automatisés de données à caractère personnel visant à faciliter la constatation et la répression des crimes et délits en série.

Décrets d'application de l'ordonnance relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

– Modalités de mise en œuvre et d'exploitation de l'espace de stockage en ligne mis à la disposition des usagers de l'administration.

Décrets d'application de l'ordonnance relative à des mesures de simplification en matière fiscale et à l'harmonisation et l'aménagement du régime des pénalités

– Conditions de la communication à l'administration fiscale par les organismes de Sécurité sociale d'informations relatives aux personnes déclarées par les particuliers employeurs.

Décrets d'application de la loi relative au développement des territoires ruraux

– Constitution d'un fichier central national des permis de chasser et lien avec le fichier national automatisé des personnes interdites d'acquisition et de détention d'armes.

Décrets d'application de la loi pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées

– Transmission par les maisons départementales des personnes handicapées à la Caisse nationale de solidarité pour l'autonomie de données relatives à leur activité et aux personnes concernées.

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

– Conditions de mise en œuvre du dossier médical personnel (DMP).
– Utilisation d'un identifiant pour l'ouverture et la tenue du dossier médical personnel.
– Conditions de mise en œuvre du volet d'urgence de la carte VITALE.
– Mise à disposition par le GIP « Institut des données de santé » d'informations dans des conditions garantissant l'anonymat.

Décrets d'application de la loi relative à la politique de santé publique

– Transmission par les médecins de données issues des consultations médicales périodiques de prévention et des examens de dépistage.

Décrets d'application de la loi relative à la bioéthique

– Modalités de recueil, de conservation et d'accès aux données relatives à l'information médicale à caractère familial.

Décrets d'application de la loi pour la confiance dans l'économie numérique

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

Décrets d'application de l'ordonnance portant diverses mesures de simplification dans le domaine agricole

– Communication par les caisses et organismes de mutualité sociale agricole d'informations nominatives aux services de l'inspection du travail, de l'emploi et de la politique sociale.

Décrets d'application de la loi portant adaptation de la justice aux évolutions de la criminalité

– Bureau d'ordre national automatisé des procédures judiciaires.

Décrets d'application de la loi relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité

– Collecte et conservation des empreintes digitales des ressortissants étrangers pris en situation irrégulière ou sollicitant un titre de séjour en France.
– Collecte et conservation des empreintes digitales des ressortissants étrangers sollicitant la délivrance d'un titre de séjour en dehors de l'espace Schengen.
– Numérisation et transmission aux autorités douanières par les entreprises de transport des documents de voyage et visas.

Décrets d'application de la loi portant réforme des retraites

– Utilisation du numéro de Sécurité sociale par les organismes de retraite pour une mutualisation des informations sur les droits des assurés.

Décrets d'application de la loi pour la sécurité intérieure

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

Décrets d'application de la loi relative aux droits des malades et à la qualité du système de santé

– Conditions d'inscription et d'accès au tableau professionnel du Conseil des professions d'infirmier, masseur-kinésithérapeute, pédicure-podologue, orthophoniste et orthoptiste.

Décrets d'application de la loi relative à la sécurité quotidienne

– 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

Dans son précédent rapport annuel, la CNIL s'était inquiétée des conditions de fonctionnement des fichiers de police judiciaire STIC et JUDEX et avait formulé des propositions afin d'une part de mieux encadrer l'utilisation de ces fichiers à des fins administratives et d'autre part de simplifier et d'accélérer les procédures de droit d'accès à ces fichiers.

Le ministère de l'Intérieur a mis en place des procédures d'apurement du fichier STIC qui ont ainsi permis en 2004 d'éliminer 1 241 742 fiches relatives à des personnes mises en cause. Mais ainsi que le montre ce rapport annuel la mise à jour des fichiers de police judiciaire ne s'est pas améliorée faute de liaisons informatiques entre les parquets et les gestionnaires des fichiers. En outre, l'exercice par le citoyen de son droit d'accès indirect aux fichiers de police reste une procédure lourde, complexe et lente (*cf.* p. 21).

C'est la raison pour laquelle la CNIL est revenue sur ces questions, à l'occasion de l'examen le 8 septembre 2005, de la modification du décret du 5 juillet 2001 relatif au STIC ainsi que du projet de décret concernant le système d'information judiciaire JUDEX mis en œuvre par la gendarmerie nationale. Ces textes ont pour objet de prendre en compte les dispositions de la loi du 21 mars 2003 pour la sécurité intérieure qui a étendu le champ d'application de ces fichiers à de nouvelles contraventions, a modifié les modalités d'alimentation et de mise à jour ainsi que les règles de contrôle et d'accès à ces fichiers et a étendu les possibilités de consultation des fichiers de police judiciaire à des fins administratives.

Dans son avis, la CNIL a exprimé sa préoccupation au sujet des conditions dans lesquelles ces fichiers sont actuellement utilisés dans le cadre des enquêtes administratives et a estimé nécessaire d'appeler à nouveau solennellement l'attention du Gouvernement sur les risques graves et réels d'exclusion ou d'injustice sociale qu'ils comportent du fait des nombreux dysfonctionnements constatés et sur la quasi-impossibilité pour les personnes de faire valoir, en pratique, leurs droits. Elle a en conséquence réitéré ses propositions d'amélioration du dispositif.

Mieux encadrer l'utilisation des fichiers de police à des fins administratives et leur mise à jour

Un fichier rigoureusement mis à jour

Il est nécessaire de mettre en place rapidement des liaisons informatiques sécurisées entre les parquets et le ministère de l'Intérieur afin d'assurer un contrôle effectif des parquets sur le fonctionnement des fichiers de police judiciaire et permettre ainsi une mise à jour sans délai de ce fichier. Il est en effet de la compétence du procureur de décider de l'effacement ou de la mise à jour des informations en cas de décision de relaxe, d'acquittement, de non-lieu ou en encore de classement sans suite pour insuffisance de charges. Cette garantie, inscrite dans la loi, doit être rendue effective.

En l'attente des développements informatiques indispensables, des mesures devraient être prises sans délai pour que le résultat de la consultation du STIC ne puisse être communiqué à l'autorité compétente qu'après que le responsable du fichier s'est assuré auprès du procureur de la République compétent qu'aucune décision judiciaire n'est intervenue qui appellerait la mise à jour de la fiche de l'intéressé ou encore qu'aucune requalification judiciaire n'est intervenue qui justifierait la rectification des informations figurant sur cette fiche.

Une utilisation administrative du fichier mieux encadrée

La Commission s'interroge sur le bien-fondé d'une consultation systématique à des fins administratives des fichiers de police judiciaire s'agissant des personnes mises en cause pour des faits relevant d'une contravention de cinquième classe ou de certains délits, qui à l'évidence ne mettent pas en cause « la protection de la sécurité des

personnes ou la défense des intérêts fondamentaux de la Nation », conditions exigées par le législateur pour justifier la consultation administrative de ces fichiers. Sur le modèle des mesures techniques prises pour exclure la consultation des fiches concernant les victimes, des dispositions pourraient être adoptées pour restreindre la consultation administrative des signalements concernant des personnes mises en cause dans des affaires relevant des contraventions de cinquième classe voire de certains délits.

Par ailleurs, des instructions précises devraient à nouveau être données aux services chargés de la réalisation des enquêtes administratives pour qu'en aucun cas la seule consultation du STIC fasse foi et constitue l'unique élément sur lequel se fonde l'autorité administrative pour émettre son avis.

Un fonctionnement plus transparent des fichiers de police judiciaire

L'information des personnes sur leurs droits

Alors que le législateur, en particulier par la loi du 18 mars 2003, a expressément reconnu aux personnes inscrites dans les fichiers de police judiciaire un certain nombre de droits, tels que la possibilité, sous certaines conditions, de demander la rectification des données en cas de requalification judiciaire et, s'agissant des victimes, l'effacement des données les concernant, ces droits ne sont, en pratique pas ou peu exercés, faute d'être connus. Aucune mesure d'information n'a en effet été prévue ni à l'égard des personnes mises en cause ni à l'égard des victimes faisant l'objet d'un signalement dans le STIC. Certes la loi « informatique et libertés » prévoit une dérogation à l'obligation générale d'information des personnes s'agissant des traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales. Toutefois, la CNIL estime que l'information des personnes sur l'existence et les conditions d'exercice de ces droits, ainsi que sur leur droit d'accès doit être reconnue et garantie par des mesures spécifiques telles que l'affichage dans les locaux des commissariats, des mentions sur les dépôts de plaintes…

Pour un aménagement du droit d'accès

Pour un droit d'accès direct des victimes

Dès lors que la loi du 18 mars 2003 ouvre au gestionnaire du fichier concerné une possibilité de communiquer directement aux requérants les informations dont la communication ne mettrait pas en cause la finalité du fichier considéré, la CNIL estime qu'il y a lieu de prévoir pour les personnes inscrites dans le fichier STIC en tant que victimes, la transmission directe par les soins du ministère de l'Intérieur du contenu de leur fiche. La saisine directe du responsable du traitement, même limitée aux victimes, permettra en outre de réduire la durée des procédures, ce qui va dans le sens d'une meilleure garantie des droits individuels.

Pour un allègement des modalités d'exercice du droit d'accès indirect

Pour tenir compte des dispositions de l'article 41 de la loi « informatique et libertés » du 6 janvier 1978 modifiée, et dans le souci de répondre plus rapidement et efficacement aux requérants, ce d'autant que le décret d'application de la loi « informatique et libertés » impose désormais des délais d'instruction stricts tant pour le ministère de l'Intérieur que pour la CNIL, la CNIL considère qu'il n'y a plus lieu de recueillir l'accord du procureur de la République et d'attendre que la procédure soit judiciairement close.

L'ACCÈS AUX DONNÉES DE SANTÉ PAR LES ORGANISMES D'ASSURANCE MALADIE COMPLÉMENTAIRES

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 souhaitent accéder aux données de santé figurant sur les feuilles de soins électroniques afin de mieux pouvoir identifier les soins remboursés et ainsi améliorer leur politique de tarification à l'égard de leurs assurés.

Actuellement, seule l'assurance maladie obligatoire est autorisée à accéder à la nature des actes médicaux effectués à travers la CCAM (classification commune des actes médicaux)[21]. S'agissant des médicaments, le code CIP qui identifie précisément chaque médicament et constitue donc un indicateur de la pathologie de la personne, n'est pas transmis à l'assurance maladie complémentaire. Seuls le montant global payé par l'assuré et le taux de remboursement sont communiqués.

Aucune disposition législative n'autorise en effet expressément la transmission des données de santé nominatives issues du codage des actes et prestations figurant sur les feuilles de soins électroniques vers l'assurance maladie complémentaire.

Une des propositions du rapport de Christian Babusiaux du 26 mai 2003 était de faire voter une loi permettant, à l'instar de ce qui est prévu par l'article L. 161-29 du Code de la Sécurité sociale, aux organismes d'assurance maladie complémentaire d'avoir accès aux données de santé figurant sur les feuilles de soins.

La CNIL considère que seule la loi en effet peut déterminer les cas dans lesquels il est possible de lever le secret médical, avec ou sans le consentement de la personne intéressée. Le vote d'une loi précisant le cadre juridique de la transmission des données de santé à l'assurance maladie complémentaire à l'instar de ce qui existe pour l'assurance maladie obligatoire[22] ou pour les unions régionales de médecins libéraux (URML)[23], apparaît être la solution la plus protectrice pour les assurés.

L'article 8-II de la loi du 6 janvier 1978 modifiée en août 2004 prévoit que, dans la mesure où la finalité du traitement l'exige et pour certaines catégories de données, certains traitements de données sensibles peuvent être admis. Ainsi, en est-il des traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée (article 8-II 1°).[24]

Il est donc nécessaire qu'une disposition législative écarte le consentement comme seul fondement et subordonne la transmission des données de santé aux organismes maladie complémentaires, à l'instar de l'assurance maladie complémentaire, à des garanties de confidentialité qu'il appartiendrait à la CNIL de vérifier dans le cadre d'une procédure d'autorisation.

---

21. La CCAM décrit l'activité médicale et permet l'allocation de ressources aux praticiens et aux établissements.
22. L. 161-29 du Code de la Sécurité sociale.
23. L'article L. 4134-4, 4e alinéa du Code de la santé publique (CSP) précitée.
24. Le législateur a ainsi interdit, dans la loi relative à l'assurance maladie du 13 août 2004 (L. 161-32-3 du Code de la Sécurité sociale), l'accès au dossier médical personnel lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de santé, même avec le consentement de la personne concernée.

LA NÉCESSAIRE DÉFINITION D'UN CADRE POUR MESURER LA DIVERSITÉ DES ORIGINES

Dès lors que les pouvoirs publics jugeraient opportun de permettre aux entreprises ou à tout organisme de mesurer la diversité des origines de leurs employés, la CNIL estime indispensable l'intervention du législateur pour définir le cadre dans lequel pourrait être effectuée cette mesure. Elle ne peut se faire sans la définition et l'utilisation préalables, par la statistique publique, d'un référentiel national de typologies « ethno-raciales » pour établir une base de comparaison fiable par origine, par bassin d'emploi ou encore par secteur d'activité.

En effet, en l'absence d'un tel référentiel et donc d'une base de comparaison pertinente, la CNIL recommande aux employeurs de ne pas recueillir de données relatives à l'origine raciale ou ethnique, réelle ou supposée, de leurs employés ou de candidats à l'embauche. Elle privilégie, en l'état, le traitement d'informations sur l'origine nationale des personnes telles qu'elles existent déjà dans la statistique publique (nationalité, nationalité d'origine le cas échéant, lieu de naissance, nationalité ou lieu de naissance des parents).

LES FICHIERS CENTRAUX DE CRÉDIT OU FICHIERS POSITIFS

La CNIL conclut à la nécessité d'une loi

S'il existe depuis 1989 un fichier national des incidents de paiement des crédits aux particuliers (le FICP géré par la Banque de France), la création d'un fichier regroupant les informations sur la situation financière des individus a toujours été écartée jusqu'à présent, à la différence de nombreux pays européens ou des États-Unis.

S'agissant de fichiers susceptibles de concerner plusieurs millions de personnes, les risques d'atteinte à la vie privée et à la protection des données personnelles sont réels, d'autant plus que ces projets correspondent à des objectifs multiples et ont des contours mal définis. La question, longtemps abordée en France sous le seul angle du surendettement, est désormais envisagée comme élément de stimulation de la croissance par le développement du crédit à la consommation.

Si le législateur en décidait la création, la CNIL estime qu'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 ainsi qu'une durée de conservation limitée.

Annexe

LISTE DES DÉLIBÉRATIONS ADOPTÉES PAR LA CNIL EN 2005

Numéro Date	Objet
2005-001 13 janvier 2005	Délibération portant autorisation d'un traitement automatisé de données à caractère personnel présenté par la société TF1 et concernant la mise en œuvre d'un système de contrôle des accès par biométrie
2005-002 13 janvier 2005	Délibération portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels
2005-003 13 janvier 2005	Délibération décidant de la dispense de déclaration des traitements mis en œuvre par les organismes publics dans le cadre de la dématérialisation des marchés publics
2005-004 18 janvier 2005	Délibération portant avis sur un projet de décret relatif aux conditions d'exploitation des réseaux et à la fourniture de services de communications électroniques
2005-005 18 janvier 2005	Délibération décidant de la dispense de déclaration des traitements relatifs à la gestion des fichiers de fournisseurs comportant des personnes physiques
2004-006 18 janvier 2005	Délibération portant autorisation de la mise en œuvre par la SNCF d'un traitement automatisé de données à caractère personnel ayant pour finalité de limiter le nombre de chèques impayés en paiement de prestations voyageurs
2005-007 18 janvier 2005	Délibération portant autorisation de la mise en œuvre par le groupe Distribution Casino France d'un traitement automatisé de données à caractère personnel ayant pour finalité de permettre d'éviter d'encaisser des chèques pour des comptes bancaires en incident non régularisé
2005-008 18 janvier 2005	Délibération portant autorisation de la mise en œuvre par FIAT-NET d'un traitement automatisé modificatif de données à caractère personnel ayant pour finalité la détermination d'un niveau d'assurance pour une transaction
2005-009 18 janvier 2005	Délibération portant autorisation de la mise en œuvre par Boursorama SA d'un traitement automatisé de données à caractère personnel ayant pour finalité d'alerter le contrôle interne de l'ouverture d'un compte par un ancien client ayant fait l'objet d'une clôture de compte à l'initiative de Boursorama
2005-010 18 janvier 2005	Délibération portant autorisation de la mise œuvre par la Banque Accord d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte antiblanchiment
2005-011 18 janvier 2005	Délibération portant autorisation de la mise en œuvre par l'Union de Banque Arabes et Françaises d'un traitement automatisé de données à caractère personnel ayant pour finalité de surveiller des mouvements comptables sur les comptes à vue dans le cadre de la lutte contre le blanchiment d'argent
2005-012 18 janvier 2005	Délibération portant autorisation de la mise en œuvre par la Fédération du Crédit Mutuel Océan d'un traitement automatisé de données à caractère personnel ayant pour finalité d'exécuter des obligations de consignation, de surveillance et de déclaration de lutte antiblanchiment
2005-013 18 janvier 2005	Délibération portant autorisation de la mise en œuvre par le CCF d'un traitement automatisé modificatif de données à caractère personnel ayant pour finalité de respecter des obligations légales et réglementaires en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme
2005-014 18 janvier 2005	Délibération portant autorisation de la mise en œuvre par l'Union de Banque à Paris d'un traitement automatisé modificatif de données à caractère personnel ayant pour finalité de respecter des obligations légales et réglementaires en matière de lutte contre le blanchiment des capitaux
2005-015 18 janvier 2005	Délibération relative aux projets de décret et d'arrêté pris pour la première phase de l'informatisation de la tenue du Livre foncier d'Alsace et de Moselle
2005-16 1er février 2005	Délibération portant mise en demeure
2005-017 1er février 2005	Délibération portant mise en demeure
2005-018 3 février 2005	Délibération portant autorisation d'une expérimentation présentée par la société Axa France ayant pour finalité d'accéder, sous forme anonymisée, aux données de santé figurant sur les feuilles de soins électroniques
2005-019 3 février 2005	Délibération portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de l'utilisation de services de téléphonie fixe et mobile sur les lieux de travail (norme simplifiée) et portant abrogation de la norme simplifiée n° 40

2005-020 10 février 2005	Délibération portant avis sur un projet de décret en Conseil d'État relatif à une expérimentation ayant pour objet d'améliorer, par comparaison d'empreintes digitales, les conditions et la fiabilité des contrôles effectués lors du passage de la frontière à l'aéroport de Roissy-Charles-de-Gaulle
2005-021 17 février 2005	Délibération relative à quatre projets de décret présentés par le ministère de l'Emploi, du Travail et de la Cohésion sociale dans le cadre des dispositifs de contrats aidés et de Maisons de l'emploi
2005-022 17 février 2005	Délibération portant avis sur un projet de décret du ministère des Affaires étrangères modifiant le décret du 31 décembre 2003 relatif à l'inscription au registre des Français établis hors de France et sur un projet d'arrêté relatif au système informatique de traitement des données relatives aux Français établis hors de France
2005-023 17 février 2005	Délibération portant autorisation de la mise en œuvre par la Banque de France d'un traitement automatisé de données à caractère personnel ayant pour finalité de contrôler l'accès aux locaux sensibles
2005-024 17 février 2005	Délibération portant autorisation de mise en œuvre par l'association réseau de soins sur l'hypertension artérielle en Guadeloupe d'un dossier médical partagé
2005-025 17 février 2005	Délibération portant autorisation de mise en œuvre par l'association Onco Pays-de-Loire d'un dossier médical partagé
2005-026 17 février 2005	Délibération portant autorisation de mise en œuvre par le GIE Télémédecine océan d'un dossier médical partagé en cancérologie
2005-027 17 février 2005	Délibération autorisant le service médical de la région Île-de-France à mettre en œuvre une étude sur les ententes préalables en matière de chirurgie plastique et reconstructrice et de vérifier les conditions techniques de réalisation de ces actes
2005-028 17 février 2005	Délibération portant autorisation de mise en œuvre par l'union régionale des caisses d'assurance maladie d'Alsace d'une expérimentation consistant à sensibiliser les assurés atteints de pathologies chroniques à l'existence de médicaments génériques pour le traitement de leur pathologie
2005-029 17 février 2005	Délibération portant autorisation de mise en œuvre par le service du contrôle médical de la caisse d'assurance maladie des artisans et commerçants d'Aquitaine d'une étude sur les prescriptions de psychotropes chez les personnes âgées en Aquitaine
2005-030 17 février 2005	Délibération portant autorisation de mise en œuvre d'un dossier médical partagé par le réseau de santé de gérontologie dénommé « Visage »
2005-031 17 février 2005	Délibération portant refus d'autorisation de la mise en œuvre par la société UTEL d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité de contrôle des horaires des employés
2005-032 3 mars 2005	Délibération portant avis sur le projet de décret présenté par la ministre de l'Emploi, du Travail et de la Cohésion sociale relatif au contrat initiative emploi (CIE) et au contrat d'accompagnement dans l'emploi (CAE) et autorisant la mise en œuvre du système d'information nécessaire à leur gestion
2005-033 3 mars 2005	Délibération portant avis sur le projet de décret présenté par le ministre de l'Emploi, du Travail et de la Cohésion sociale relatif au contrat d'avenir et au contrat insertion - revenu minimum d'activité et autorisant la mise en œuvre du système d'information nécessaire à leur gestion
2005-034 17 février 2005	Délibération portant refus d'autorisation de la mise en œuvre par la société UCOM d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2005-035 17 février 2005	Délibération portant refus d'autorisation de la mise en œuvre par la société MFG Éducation d'un traitement automatisé de donnée à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2005-036 17 février 2005	Délibération portant refus d'autorisation de la mise en œuvre par la société Paris Monitoring d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2005-037 17 février 2005	Délibération portant refus d'autorisation de la mise en œuvre par la mairie des Sables-d'Olonne d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2005-038 10 mars 2005	Délibération relative à la modification du traitement « ANAISS » destiné à la gestion des dossiers des usagers des services sociaux des caisses régionales d'assurance maladie et des caisses générales de Sécurité sociale
2005-039 10 mars 2005	Délibération portant avis sur un projet de décret en Conseil d'État relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles
2005-040 10 mars 2005	Délibération portant autorisation de la mise en œuvre par la Direction générale de l'aviation civile d'un traitement automatisé de données à caractère personnel relatif à la gestion de la taxe sur les nuisances sonores aériennes instaurée par la loi de finances rectificatives n° 2003-1312 du 30 décembre 2003

2005-041 10 mars 2005	Délibération portant autorisation d'intégration dans les systèmes d'information de la caisse de retraite et de prévoyance des clercs et employés de notaires de la nouvelle classification des actes médicaux et des prestations
2005-042 9 mars 2005	Délibération relative aux suites données à des contrôles
2005-043 9 mars 2005	Délibération portant avertissement à la caisse de Crédit Mutuel Saint-Étienne Gambetta
2005-044 15 mars 2005	Délibération portant autorisation de la mise en œuvre par la RTM d'un traitement automatisé de données à caractère personnel relatif aux infractions à la police des services publics de transports terrestres
2005-045 15 mars 2005	Délibération portant avis sur un projet de décret en Conseil d'État relatif aux conditions d'agrément des hébergeurs de données de santé à caractère personnel
2005-046 15 mars 2005	Délibération portant avis sur le projet de décret en Conseil d'État fixant les modalités selon lesquelles les médecins ont accès aux données relatives aux prestations servies aux bénéficiaires de l'assurance maladie et modifiant le Code de la Sécurité sociale
2005-047 22 mars 2005	Délibération portant avis sur un projet de code de déontologie présenté par le Syndicat national de la communication directe (SNCD) relatif à la communication directe électronique
2005-048 22 mars 2005	Délibération portant autorisation de mise en œuvre par l'association de gestion du réseau e-santé bas-normand d'une plate forme régionale d'information de santé
2005-049 24 mars 2005	Délibération portant avis sur un projet de décret en Conseil d'État pris pour l'application de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
2005-050 24 mars 2005	Délibération portant autorisation de la mise en œuvre par le Syndicat des éditeurs de logiciels de loisirs (SELL) d'un traitement de données à caractère personnel ayant pour finalités l'envoi aux internautes de messages pédagogiques et la constatation des infractions au Code de la propriété intellectuelle dans le cadre de l'utilisation des protocoles de communication peer to peer
2005-051 30 mars 2005	Délibération portant avis sur un projet de code de conduite présenté par l'Union française du marketing direct (UFMD) sur l'utilisation de coordonnées électroniques à des fins de prospection directe
2005-052 30 mars 2005	Délibération portant avis sur le projet de décret en Conseil d'État prévu par l'article L. 211-7 du Code de l'entrée et du séjour des étrangers et du droit d'asile et relatif aux modalités de mise en œuvre par les maires, agissant en leur qualité d'agents de l'État, d'un traitement automatisé de données à caractère personnel relatif aux demandes de validation des attestations d'accueil
2005-053 21 avril 2005	Délibération relative au projet de décret présenté par le ministre délégué à l'Industrie modifiant le décret n° 2004-325 du 8 avril 2004 relatif à la tarification spéciale de l'électricité comme produit de première nécessité
2005-054 30 mars 2005	Délibération portant avis sur le projet d'ordonnance relatif au service public du changement d'adresse, sur le projet de décret pris en application de l'ordonnance relative au service de changement d'adresse et sur le projet d'arrêté du Premier ministre créant un traitement de données à caractère personnel mettant en place le téléservice « monchangementdadresse »
2005-055 30 mars 2005	Délibération portant autorisation de la mise en œuvre par la Banque Martin-Maurel d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte antiblanchiment
2005-056 31 mars 2005	Délibération clôturant une procédure
2005-057 31 mars 2005	Délibération portant avertissement à la Caisse régionale du Crédit Agricole mutuel du Nord de France
2005-058 31 mars 2005	Délibération clôturant une procédure
2005-059 31 mars 2005	Délibération portant avertissement à l'organisme de crédit CREDIPAR
2005-060 31 mars 2005	Délibération portant avertissement au Crédit Lyonnais
2005-061 31 mars 2005	Délibération portant avertissement à la Caisse d'Épargne Île-de-France Ouest
2005-062 31 mars 2005	Délibération portant avertissement à la caisse régionale du Crédit Agricole mutuel du Gard
2005-063 21 avril 2005	Délibération relative au projet de décret présenté par le ministre délégué à l'Industrie relatif à la procédure applicable en cas d'impayés des factures d'électricité

2005-064 20 avril 2005	Délibération portant autorisation de la mise en œuvre par la direction des monnaies et médailles d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès aux locaux sensibles
2005-065 20 avril 2005	Délibération portant autorisation de la mise en œuvre par la société Daimler Chrysler services fleet management d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé des infractions au Code de la route
2005-066 20 avril 2005	Délibération portant autorisation de la mise en œuvre par la société Redbus Interhouse SA d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'iris et ayant pour finalité de contrôler l'accès aux locaux sensibles
2005-067 21 avril 2005	Délibération portant avis sur le projet d'acte réglementaire de Conseil national de l'ordre des pharmaciens créant un traitement de données à caractère personnel mettant en œuvre un dispositif de vote électronique pour les élections aux Conseils de l'ordre des pharmaciens de 2005
2005-068 20 avril 2005	Délibération portant autorisation du traitement ARCHIMED ayant pour objet la gestion des fiches médicales des services médicaux de chaque Caisse mutuelle régionale (CMR)
2005-069 20 avril 2005	Délibération portant autorisation de mise en œuvre par l'association Réseau ONCOLOR d'un système d'échange de données de santé dans le cadre de comités de concertation pluridisciplinaire
2005-070 20 avril 2005	Délibération portant autorisation de mise en œuvre par la direction de la santé de Polynésie française d'un réseau de santé
2005-071 20 avril 2005	Délibération portant autorisation de mise en œuvre par l'association Diabète 92 Nord d'un dossier médical partagé
2005-072 21 avril 2005	Délibération portant autorisation d'un transfert de données à caractère personnel vers le Japon à l'occasion d'un contrat de sous-traitance entre la succursale française Mitsubishi Electric Europe et la société Mitsubishi Electric Information Network Corporation
2005-073 20 avril 2005	Délibération portant autorisation de mise en œuvre par le conseil général des Hauts-de-Seine d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2005-074 21 avril 2005	Délibération portant avis sur le projet d'arrêté du conseil général du Val-d'Oise créant un traitement de données à caractère personnel mettant en place la carte de vie quotidienne « Cartevaloise »
2005-075 10 mai 2005	Délibération portant avertissement à la société SOFINCO
2005-076 10 mai 2005	Délibération clôturant une procédure
2005-077 10 mai 2005	Délibération clôturant une procédure
2005-078 10 mai 2005	Délibération portant mise en demeure
2005-079 10 mai 2005	Délibération portant mise en demeure
2005-080 10 mai 2005	Délibération portant mise en demeure
2005-081 10 mai 2005	Délibération portant mise en demeure
2005-082 10 mai 2005	Délibération portant mise en demeure
2005-083 10 mai 2005	Délibération portant mise en demeure
2005-084 10 mai 2005	Délibération portant mise en demeure
2005-085 10 mai 2005	Délibération portant avertissement à la caisse régionale du Crédit Agricole mutuel de la Réunion
2005-086 12 mai 2005	Délibération portant refus d'autorisation d'un traitement automatisé d'observation sociale statistique des agents du ministère de l'Équipement, des Transports, de l'Aménagement du territoire, du Tourisme et de la Mer
2005-087 12 mai 2005	Délibération portant autorisation de mise en œuvre par le ministère de l'Emploi, du Travail et de la Cohésion sociale d'un traitement automatisé de données à caractère personnel ayant pour finalité de permettre la gestion continue entre les ministères concernés des procédures d'acquisition ou de perte de la nationalité française et de participer à la preuve de la nationalité française

2005-088 12 mai 2005	Délibération portant autorisation d'un traitement automatisé de données à caractère personnel mis en œuvre par la préfecture de police de Paris pour assurer le suivi administratif des demandes de titre de séjour pour raisons médicales
2005-089 10 mai 2005	Délibération portant mise en demeure
2005-090 12 mai 2005	Délibération portant autorisation de la mise en œuvre par la fédération des chasseurs de Dordogne d'un traitement automatisé de données à caractère personnel comportant des informations relatives aux infractions
2005-091 12 mai 2005	Délibération portant désignation d'un membre de la Commission nationale de l'informatique et des libertés chargé d'exercer le droit d'accès indirect en application de l'article 41 de la loi du 6 janvier 1978 modifiée
2005-092 19 mai 2005	Délibération modifiant la délibération n° 2004-094 du 2 décembre 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)
2005-093 19 mai 2005	Délibération portant autorisation d'un traitement automatisé de données à caractère personnel mis en œuvre par l'Institut national de veille sanitaire ayant pour finalité la conduite d'une enquête sur les défenestrations d'enfants de moins de 16 ans survenues en Île-de-France entre mai et septembre 2005
2005-094 19 mai 2005	Délibération portant avis sur le projet d'ordonnance relatif à la réutilisation des informations publiques et modifiant la loi du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal
2005-095 19 mai 2005	Délibération portant autorisation de mise en œuvre par la Banque Populaire Loire et Lyonnais d'un traitement automatisé de données à caractère personnel ayant pour finalité la saisie et les contrôles des informations nécessaires à l'étude des demandes de prêts personnels effectués par la clientèle
2005-096 19 mai 2005	Délibération portant autorisation de mise en œuvre par la Banque Populaire Loire et Lyonnais d'un traitement automatisé de données à caractère personnel ayant pour finalité le calcul du score de crédit *revolving*
2005-097 19 mai 2005	Délibération portant autorisation de mise en œuvre par la Caisse régionale de crédit agricole de la Martinique d'un traitement automatisé de données à caractère personnel ayant pour finalité de mesurer le risque crédit des clients professionnels en analysant leur situation financière et en attribuant une note correspondant au niveau de risque
2005-098 19 mai 2005	Délibération portant autorisation de mise en œuvre par le Crédit agricole de Franche-Comté d'un traitement automatisé de données à caractère personnel ayant pour finalité le calcul d'une cotation bancaire du client pour faciliter l'instruction et la prise de décision d'un dossier de crédit
2005-099 19 mai 2005	Délibération portant autorisation de mise en œuvre par la Caisse régionale de crédit agricole mutuel Champagne-Bourgogne d'un traitement automatisé de données à caractère personnel ayant pour finalité le calcul d'un score pour les prêts personnels
2005-100 19 mai 2005	Délibération portant autorisation de mise en œuvre par la Caisse régionale de crédit agricole Loire Haute-Loire d'un traitement automatisé de données à caractère personnel ayant pour finalité scoring permanent de la clientèle des particuliers au regard du crédit à la consommation
2005-101 19 mai 2005	Délibération portant refus d'autorisation de mise en œuvre par la société COFINOGA d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-102 19 mai 2005	Délibération portant refus d'autorisation de mise en œuvre par la société SOFICARTE d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-103 19 mai 2005	Délibération portant refus d'autorisation de mise en œuvre par la société MEDIATIS d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-104 19 mai 2005	Délibération portant refus d'autorisation de mise en œuvre par la société SYGMA BANQUE d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-105 19 mai 2005	Délibération portant refus d'autorisation de mise en œuvre par la société Banque du Groupe Casino d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-106 19 mai 2005	Délibération portant refus d'autorisation de mise en œuvre par la société Compagnie de gestion et de prêts CDGP d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-107 19 mai 2005	Délibération portant autorisation de mise en œuvre par l'association Réseau 25 d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'un dossier médical partagé dans le domaine des conduites addictives

2005-108 19 mai 2005	Délibération portant autorisation de mise en œuvre par les services médicaux de chaque caisse mutuelle régionale (CMR) d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des prescriptions et les délivrances atypiques de médicaments de substitution aux opiacés
2005-109 26 mai 2005	Délibération relative aux projets de décrets présentés par le ministère des Solidarités, de la Santé et de la Famille visant à mettre en œuvre le droit à l'information des assurés sur leur retraite
2005-110 26 mai 2005	Délibération relative à une demande d'autorisation de McDonald's France pour la mise en œuvre d'un dispositif d'intégrité professionnelle
2005-111 26 mai 2005	Délibération relative à une demande d'autorisation de la Compagnie européenne d'accumulateurs pour la mise en œuvre d'un dispositif de « ligne éthique »
2005-112 7 juin 2005	Délibération portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion des fichiers de clients et de prospects et portant abrogation des normes simplifiées 11, 17 et 25 (norme simplifiée n° 48)
2005-113 7 juin 2005	Délibération portant autorisation de la mise en œuvre par le groupe Imprimerie nationale d'un traitement de données à caractère personnel ayant pour finalité le contrôle des accès par reconnaissance des empreintes digitales
2005-114 7 juin 2005	Délibération portant autorisation de la mise en œuvre par la Compagnie des transports strasbourgeois (CTS) d'un traitement automatisé de données à caractère personnel relatif aux infractions à la police des services publics de transports terrestres
2005-115 7 juin 2005	Délibération portant autorisation de la mise en œuvre par la chambre de commerce et d'industrie de Nice-Côte d'Azur d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion d'une carte de fidélité impliquant l'utilisation d'un dispositif biométrique de reconnaissance des empreintes digitales
2005-116 à 125 7 juin 2005	Délibérations portant autorisation d'un transfert de données à caractère personnel
2005-126 12 mai 2005	Délibération portant rectification de la délibération n° 04-067 du 24 juin 2004 concernant les traitements automatisés d'information nominatives mis en œuvre par les communes pour la gestion de l'état civil
2005-127 14 juin 2005	Délibération portant autorisation de mise en œuvre par le ministère des Solidarités, de la Santé et de la Famille au sein des services médicaux de l'assurance maladie obligatoire d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle de la facturation des établissements publics et privés de santé dans le cadre de la réforme de la tarification à l'activité
2005-128 14 juin 2005	Délibération portant autorisation de mise en œuvre par la caisse primaire d'assurance maladie de la Seine-Saint-Denis d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'un tableau de suivi des fraudes et anomalies
2005-129 14 juin 2005	Délibération portant autorisation de mise en œuvre par l'association Réseau Onco-Normand d'un système d'échange de données de santé destiné à l'organisation de réunions de concertations pluridisciplinaires
2005-130 14 juin 2005	Délibération portant mise en demeure
2005-131 14 juin 2005	Délibération portant mise en demeure
2005-132 et 133 22 septembre 2005	Délibérations portant autorisation d'un transfert de données à caractère personnel
2005-134	Numéro non utilisé
2005-135 14 juin 2005	Délibération autorisant la mise en œuvre par le centre hospitalier de Hyères d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de ses employés
2005-136 14 juin 2005	Délibération portant autorisation de mise en œuvre à titre expérimental par La Poste à Vigneux-sur-Seine d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès aux locaux
2005-137 14 juin 2005	Délibération portant autorisation de mise en œuvre à titre expérimental par La Poste à Palaiseau d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès aux locaux
2005-138 14 juin 2005	Délibération portant autorisation de mise en œuvre à titre expérimental par La Poste à Aubervilliers d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès aux locaux
2005-139 14 juin 2005	Délibération portant autorisation de mise en œuvre à titre expérimental par La Poste à Noisy-le-Sec d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès aux locaux
2005-140 14 juin 2005	Délibération portant autorisation de mise en œuvre par La Poste à Argenteuil d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès aux locaux

2005-141 14 juin 2005	Délibération portant mise en demeure
2005-142 14 juin 2005	Délibération portant autorisation de mise en œuvre par la Banque BCP d'un traitement automatisé de données à caractère personnel ayant pour finalité l'aide à l'analyse du comportement bancaire des clients dans le cadre de la lutte contre le blanchiment
2005-143 14 juin 2005	Délibération portant autorisation de mise en œuvre par la Société Marseillaise de Crédit d'un traitement automatisé de données à caractère personnel ayant pour finalité le recensement des dossiers ayant fait l'objet d'analyses et d'études par le département conformité, déontologie et lutte antiblanchiment
2005-144 14 juin 2005	Délibération portant autorisation de mise en œuvre par la société Fortis Banque France d'un traitement automatisé modifié de données à caractère personnel ayant pour finalité la gestion du fichier de lutte contre le blanchiment, fraude et antiterrorisme
2005-145 14 juin 2005	Délibération portant autorisation de mise en œuvre par le Crédit commercial de France (CCF) d'un traitement automatisé de données à caractère personnel ayant pour finalité la communication intra-groupe CCF des personnes physiques qui ont fait l'objet d'une déclaration de soupçon auprès de TRACFIN
2005-146 14 juin 2005	Délibération portant mise en demeure
2005-147 14 juin 2005	Délibération portant mise en demeure
2005-148 14 juin 2005	Délibération portant autorisation de la mise en œuvre par la Cité des sciences et de l'industrie d'un traitement automatisé de données à caractère personnel ayant pour finalité l'expérimentation de dispositifs de reconnaissance biométrique dans le cadre d'une exposition pédagogique
2005-149 14 juin 2005	Délibération portant autorisation de la mise en œuvre par l'Institut national des hautes études de sécurité (INHES) d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès par reconnaissance des empreintes digitales
2005-150 14 juin 2005	Délibération portant mise en demeure
2005-151 14 juin 2005	Délibération portant autorisation de mise en œuvre par l'association Réseau Onco-Bourgogne d'un système d'information du réseau de santé en cancérologie
2005-152 14 juin 2005	Délibération portant autorisation de mise en œuvre par la société Kappa Santé et le centre de mémoire de ressources et de recherche de la région Provence-Alpes-Côte d'Azur d'un réseau de données épidémiologiques standardisées sur la maladie d'Alzheimer
2005-153 21 juin 2005	Délibération portant autorisation de mise en œuvre par le ministère de la Justice d'un traitement automatisé de gestion des opérations d'interconnexions nécessaires à la mise en œuvre du fichier judiciaire national automatisé des auteurs d'infractions sexuelles
2005-154 14 juin 2005	Délibération portant mise en demeure
2005-155 14 juin 2005	Délibération portant mise en demeure
2005-156 14 juin 2005	Délibération portant mise en demeure
2005-157 14 juin 2005	Délibération portant mise en demeure
2005-158 14 juin 2005	Délibération portant autorisation de mise en œuvre par la communauté de communes du canton de Beuzeville d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales et des données relatives à l'assainissement non collectif
2005-159 14 juin 2005	Délibération portant autorisation de mise en œuvre par la communauté de communes de Val-de-l'Eyre d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique ayant pour finalité l'instruction du droit des sols et la gestion des installations individuelles d'assainissement non collectif
2005-160 14 juin 2005	Délibération portant autorisation de mise en œuvre par la mairie de Paris d'un traitement automatisé de données à caractère personnel relatif à la gestion des procès-verbaux en matière de salubrité publique, des procédures d'enlèvement d'office des déchets et de nettoiement des salissures, des procédures d'enlèvement d'office des affiches et des interventions des inspecteurs du centre d'action pour la propreté de Paris
2005-161 21 juin 2005	Délibération portant autorisation de la mise en œuvre par les services de la Commission nationale de l'informatique et des libertés d'un traitement de données à caractère personnel relatif à la gestion des déclarations, demandes d'avis et demandes d'autorisation de traitements de données personnelles et des saisines adressées à la Commission

2005-162 21 juin 2005	Délibération autorisant la mise en œuvre par la société Reichen et Robert & associés architectes urbanistes d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux locaux
2005-163 21 juin 2005	Délibération autorisant la mise en œuvre par la mairie de Gagny d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires de ses employés
2005-164 21 juin 2005	Délibération portant autorisation de mise en œuvre par la société FIA-NET d'un traitement automatisé de données à caractère personnel ayant pour finalité l'aide à la détermination d'un niveau d'assurance (incidents et impayés)
2005-165 21 juin 2005	Délibération portant autorisation de mise en œuvre par la Banque populaire du Massif central (BPMC) d'un traitement automatisé de données à caractère personnel ayant pour finalité l' « application lutte antiblanchiment permettant d'historiser les dossiers ayant fait l'objet d'une étude dans le cadre des procédures réglementaires » auprès de TRACFIN
2005-166 21 juin 2005	Délibération portant autorisation de mise en œuvre par l'hypermarché Record Saint-Avold d'un traitement automatisé de données à caractère personnel ayant pour finalité de réduire le nombre d'impayés en magasin
2005-167 30 juin 2005	Délibération portant avis sur la mise en œuvre par la direction générale des douanes et droits indirects du système d'information des douanes
2005-169 5 juillet 2005	Délibération portant autorisation de mise en œuvre par le collège « Les Mimosas » d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de l main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2005-170 5 juillet 2005	Délibération portant autorisation d'un transfert de données à caractère personnel par la société Domisanté vers la société Air Products ans Chemicals Inc., établie aux États-Unis
2005-171 à 182 5 juillet 2005	Délibérations portant autorisation d'un transfert de données à caractère personnel
2005-183 5 juillet 2005	Délibération portant avis sur le projet d'arrêté du Premier ministre créant un traitement automatisé de données à caractère personnel mettant en place le téléservice « demande d'acte de naissance »
2005-184 5 juillet 2005	Délibération portant autorisation de mise en œuvre par la mairie de Roubaix d'un traitement automatisé de données à caractère personnel relatif à la gestion des procès-verbaux en matière de salubrité publique, du non-respect des conditions d'octroi des occupations privatives du domaine public, et de la régulation des infractions en matière d'aménagement du territoire et du droit des sols
2005-185 5 juillet 2005	Délibération portant autorisation de mise en œuvre par la société Claranet d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès à la salle d'hébergement
2005-186 5 juillet 2005	Délibération portant autorisation de mise en œuvre par la société Carrefour hypermarché France d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès à certains locaux de l'établissement de la Valette du Var
2005-187 8 septembre 2005	Délibération portant avis sur le projet de décret en Conseil d'État pris pour l'application de l'article 21 de la loi n° 2003-239 du 18 mars 2003 et modifiant le décret n° 2001-583 du 5 juillet 2001 pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées « STIC »
2005-188 8 septembre 2005	Délibération portant avis sur le projet de décret en Conseil d'État pris pour l'application de l'article 26 II de la loi du 6 janvier 1978 modifiée et portant création du système d'information judiciaire « JUDEX »
2005-189 8 septembre 2005	Délibération portant autorisation de la mise en œuvre par la société Télé 2 d'un traitement automatisé de données à caractère personnel relatif à la prévention des impayés
2005-190 8 septembre 2005	Délibération portant autorisation de la mise en œuvre par la société Omer Télécom d'un traitement automatisé de données à caractère personnel relatif à la prévention des impayés
2005-191 8 septembre 2005	Délibération portant autorisation de mise en œuvre par la société COFINOGA d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédit (score)
2005-192 8 septembre 2005	Délibération portant autorisation de mise en œuvre par la société MEDIATIS d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-193 8 septembre 2005	Délibération portant autorisation de mise œuvre par la société Banque du Groupe Casino d'un traitement automatisé de données à caractère personnel ayant une finalité la pré-étude des demandes de crédits (score)
2005-194 8 septembre 2005	Délibération portant autorisation de mise en œuvre par la société Compagnie de gestion et de prêts (CDGP) d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)

2005-195 8 septembre 2005	Délibération portant autorisation de mise en œuvre par la société SYGMA banque d'un traitement automatisé de données à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-196 8 septembre 2005	Délibération portant autorisation de mise en œuvre par la société SOFINCO d'un traitement automatisé de données à caractère personnel ayant pour finalité la prévention de surendettement par les filiales de crédit à la consommation du Groupe Crédit Agricole
2005-197 8 septembre 2005	Délibération portant autorisation de mise en œuvre par la société FINAREF d'un traitement automatisé de données à caractère personnel ayant pour finalité la prévention du surendettement par les filiales de crédit à la consommation du Groupe Crédit Agricole
2005-198 8 septembre 2005	Délibération portant refus d'autorisation de mise en œuvre par la société Banque Accord d'un traitement automatisé de données à caractère personnel ayant pour finalité la mutualisation de la détection des incohérences dans les demandes de crédit par l'adhésion au service « detect » mis en œuvre par la société EXPERIAN
2005-199 22 septembre 2005	Délibération portant autorisation de mise en œuvre par la société Volkswagen finance d'un traitement automatisé de données à caractère personnel ayant pour finalité la mutualisation de la détection des incohérences dans les demandes de crédit par l'adhésion au service « detect » mis en œuvre par la société EXPERIAN
2005-200 8 septembre 2005	Délibération portant autorisation de mise en œuvre par la société SOFICARTE d'un traitement automatisé de donnés à caractère personnel ayant pour finalité la pré-étude des demandes de crédits (score)
2005-201 à 205 22 septembre 2005	Délibérations portant autorisation d'un transfert de données à caractère personnel
2005-206 22 septembre 2005	Délibération portant autorisation de mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès logique à un service d'informations financières de la société Bloomberg L.P.
2005-207 22 septembre 2005	Délibération portant autorisation de mise en œuvre, par le ministère de la Justice, d'un traitement automatisé de données à caractère personnel permettant le suivi et le contrôle de l'activité du secteur associatif en charge des mineurs en danger et l'établissement de statistiques anonymisées
2005-208 10 octobre 2005	Délibération portant avis sur le projet de loi relatif à la lutte contre le terrorisme
2005-209 11 octobre 2005	Délibération portant avis sur un projet de décret en Conseil d'État relatif à la confidentialité des données de santé à caractère personnel pris en application de l'article L. 1110-4 du Code de la santé publique
2005-210 11 octobre 2005	Délibération portant autorisation de mise en œuvre par la caisse autonome nationale de compensation d'assurance vieillesse des artisans, CANCAVA, d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'une base de données des arrêts de la cour nationale de l'incapacité et de la tarification de l'assurance des accidents du travail (CNITAAT)
2005-211 11 octobre 2005	Délibération portant autorisation de mise en œuvre par la caisse d'assurance vieillesse, invalidité et maladie des cultes (CAVIMAC) d'un traitement automatisé de données à caractère personnel au sein du service de contrôle médical ayant pour finalité la gestion du contrôle médical
2005-212 11 octobre 2005	Délibération portant autorisation de mise en œuvre par le groupement d'intérêt public carte de professionnel de santé d'un traitement automatisé de données à caractère personnel ayant pour finalité le rapprochement des répertoires des professionnels de santé détenus par l'État, la direction centrale du service de santé des armées, les ordres professionnels, la CNAMTS et le GIP-CPS afin de déterminer les règles de rapprochement des différents répertoires préalablement à la constitution d'un répertoire partagé des professionnels de santé (RPPS)
2005-213 11 octobre 2005	Délibération portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel
2005-214 11 octobre 2005	Délibération portant autorisation de mise en œuvre par l'association Carédiab d'un dossier médical partagé dans le cadre d'un réseau de santé en Champagne-Ardennes
2005-215 11 octobre 2005	Délibération portant autorisation de mise en œuvre par le centre hospitalier régional et universitaire de Lille d'un traitement automatisé de données à caractère personnel ayant pour finalité la création du réseau de santé Nephronor pour les personnes atteintes d'insuffisance rénale chronique en région Nord-Pas-de-Calais et d'un registre régional de néphrologie anonymisé
2005-216 11 octobre 2005	Délibération portant autorisation de mise en œuvre par le réseau de cancérologie de l'Arc Alpin d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'un réseau de cancérologie destiné aux professionnels de santé prenant en charge des patients atteints de cancer
2005-217 11 octobre 2005	Délibération portant autorisation de mise en œuvre par l'association du réseau de prévention et de prise en charge de l'obésité en pédiatrie sur le grand Lyon (REPOP-GL) d'une plate-forme d'échange pour les professionnels de santé
2005-218 11 octobre 2005	Délibération portant autorisation de mise en œuvre par la communauté de communes de la Thiérache du centre d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif

2005-219 11 octobre 2005	Délibération portant autorisation de mise en œuvre par la communauté de communes du Beaunois d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2005-220 11 octobre 2005	Délibération portant autorisation de mise en œuvre par la communauté de communes de la Boixe d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2005-221 11 octobre 2005	Délibération portant autorisation de mise en œuvre par le Syndicat intercommunal d'assainissement et d'eau potable (SIAEP) de Vannes ouest d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2005-222 11 octobre 2005	Délibération portant autorisation de mise en œuvre par la direction départementale de l'agriculture et de la forêt du Gers d'un traitement automatisé de données à caractère personnel ayant pour finalité de mettre en place un système d'information géographique à partir de données cadastrales
2005-223 11 octobre 2005	Délibération portant autorisation de mise en œuvre par le Syndicat intercommunal de gestion de l'entretien des stations d'épuration (SIGESE) de Lanester d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2005-224 11 octobre 2005	Délibération portant autorisation de mise en œuvre par le Syndicat Intercommunal de la Vallée de l'Ondaine (SIVO-Ondaine) d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2005-225 11 octobre 2005	Délibération portant autorisation de mise en œuvre par la communauté d'agglomération de Pau Pyrénées d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2005-226 11 octobre 2005	Délibération portant autorisation de mise en œuvre par la mairie de Niort d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2005-227 11 octobre 2005	Délibération portant autorisation de mise en œuvre par l'établissement public foncier de la Réunion (EPF Réunion) d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2005-228 11 octobre 2005	Délibération portant autorisation de mise en œuvre par l'établissement public foncier de Lorraine (EPF Lorraine) d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2005-229 11 octobre 2005	Délibération portant autorisation de mise en œuvre par l'Union régionale des médecins libéraux de Picardie (URMLP) - Réseau diabète Picardie d'un dossier médical partagé
2005-230 11 octobre 2005	Délibération portant autorisation de mise en œuvre par l'association Franc-Comtoise du diabète - Réseau de santé Gentiane, d'un dossier médical partagé
2005-231 11 octobre 2005	Délibération portant autorisation de mise en œuvre par l'association réseau diabète de Colmar d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'un dossier médical partagé pour des patients atteints de diabète de type 2 et l'évaluation du réseau
2005-232 18 octobre 2005	Délibération portant adoption d'une norme simplifiée concernant les traitements automatisés mis en œuvre par les collectivités locales et leurs groupements dotés d'une fiscalité propre aux fins de la lutte contre la vacance des logements
2005-233 18 octobre 2005	Délibération portant autorisation unique de mise en œuvre par le centre national des œuvres universitaires et scolaires d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des aides ponctuelles allouées aux étudiants dans le cadre de l'action sociale et le suivi statistique de l'activité de services sociaux des centres régionaux des œuvres universitaires et scolaires
2005-234 18 octobre 2005	Délibération portant autorisation de la mise en œuvre par la société Conforama d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre les chèques impayés
2005-235 18 octobre 2005	Délibération portant refus d'autorisation de la mise en œuvre par la Société des auteurs, compositeurs et éditeurs de musique (SACEM) d'un traitement de données à caractère personnel ayant pour finalités, d'une part, la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés « peer to peer », d'autre part, l'envoi de messages pédagogiques informant les internautes sur les sanctions prévues en matière de délit de contrefaçon
2005-236 18 octobre 2005	Délibération portant refus d'autorisation de la mise en œuvre par la Société civile des producteurs phonographiques (SCPP) d'un traitement de données à caractère personnel ayant pour finalités, d'une part, la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés « peer to peer », d'autre part, l'envoi de messages pédagogiques informant les internautes sur les sanctions prévues en matière de délit de contrefaçon

2005-237 18 octobre 2005	Délibération portant refus d'autorisation de la mise en œuvre par la Société civile des producteurs de phonogrammes en France (SPPF) d'un traitement de données à caractère personnel ayant pour finalités, d'une part, la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés « peer to peer », d'autre part, l'envoi de messages pédagogiques informant les internautes sur les sanctions prévues en matière de délit de contrefaçon
2005-238 18 octobre 2005	Délibération portant refus d'autorisation de la mise en œuvre par la Société pour l'administration du droit de reproduction mécanique (SDRM) d'un traitement de données à caractère personnel ayant pour finalité, d'une part, la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés « peer to peer », d'autre part, l'envoi de messages pédagogiques informant les internautes sur les sanctions prévues en matière de délit de contrefaçon
2005-239 3 novembre 2005	Délibération portant mise en demeure
2005-240 3 novembre 2005	Délibération portant mise en demeure
2005-241 3 novembre 2005	Délibération portant mise en demeure
2005-242 3 novembre 2005	Délibération portant mise en demeure
2005-243 3 novembre 2005	Délibération portant mise en demeure
2005-244 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par le lycée professionnel de Vedène d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2005-245 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par la société Keynectis d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux locaux
2005-246 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par la société FCI France d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès par reconnaissance des empreintes digitales
2005-247 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par la société Info Service Europe d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires de ses employés
2005-248 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par la société ferma d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux locaux
2005-249 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par le cabinet Lexvia d'un traitement automatisé des empreintes digitales et ayant pour finalité de sécuriser l'accès aux documents ainsi que leur envoi par courrier électronique
2005-250 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par la société Bouygues Telecom d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux
2005-251 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par la société Aermecanic d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux zones dites réservées
2005-252 3 novembre 2005	Délibération portant autorisation de la mise en œuvre par la société Plastic Omnium d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux locaux
2005-253 10 novembre 2005	Délibération portant autorisation de mise en œuvre par le lycée Jules-Fil d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2005-254 10 novembre 2005	Délibération portant avis sur un projet de décret relatif à la conservation des données de communications électroniques et modifiant le code des postes et des communications électroniques
2005-255 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la caisse primaire d'assurance maladie de Strasbourg d'un traitement automatisé de données à caractère personnel ayant pour finalité le suivi des audiences
2005-256 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la direction de la recherche, des études, de l'évaluation et des statistiques du ministère de l'Emploi, de la Cohésion sociale et du ministère de la Santé et des solidarités d'un traitement automatisé de données à caractère personnel ayant pour finalité de gérer, à des fins statistiques et épidémiologiques, les informations issues des trois certificats de santé rédigés dans les huit jours, le neuvième et le vingt-quatrième mois suivant la naissance des enfants

2005-257 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Caisse d'épargne de Haute-Normandie d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment et le financement du terrorisme
2005-258 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Caisse d'épargne d'Île-de-France d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment d'argent et le financement du terrorisme
2005-259 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Caisse d'épargne de Basse-Normandie d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment des capitaux et le financement du terrorisme
2005-260 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Caisse d'épargne et de prévoyance de Bourgogne d'un traitement automatisé de données à caractère personnel ayant pou finalité la lutte contre le blanchiment des capitaux provenant du trafic de stupéfiant ou d'activités criminelles organisés et le financement du terrorisme
2005-261 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Société Generali Proximité Assurance (GPA) d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment des capitaux et le financement du terrorisme
2005-262 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Caisse d'épargne et de prévoyance de Bretagne d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment et le financement du terrorisme
2005-263 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Caisse d'épargne et de prévoyance du Pas-de-Calais d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment et le financement du terrorisme
2005-264 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Caisse d'épargne de Côte d'Azur d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment des capitaux provenant du trafic de stupéfiants ou d'activités criminelles organisées et le financement du terrorisme
2005-265 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Banque de Neuflize d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment des capitaux et le financement du terrorisme
2005-266 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Banque NSM entreprises d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment des capitaux et le financement du terrorisme
2005-267 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la société ABN AMRO Bank NV succursale de paris d'un traitement automatisé de données à caractère personnel ayant pour finalité la détection des scénarios de blanchiment de capitaux
2005-268 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la Société Marseillaise de Crédit d'un traitement automatisé de données à caractère personnel ayant pour finalité la détection et gestion d'opération douteuses sur les comptes de la clientèle
2005-269 10 novembre 2005	Délibération portant autorisation de mise en œuvre par le Crédit Agricole Sud Rhône Alpes d'un traitement automatisé de données à caractère personnel ayant pour finalité la consignation des opérations réalisées par des clients occasionnels
2005-270 10 novembre 2005	Délibération portant autorisation de mise en œuvre par la BNP PARIBAS d'un traitement automatisé de données à caractère personnel ayant pour finalité la « surveillance réglementaires dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme »
2005-271 3 novembre 2005	Délibération clôturant une procédure
2005-272 17 novembre 2005	Délibération portant avis sur le traitement de données à caractère personnel mettant en œuvre un dispositif de vote électronique pour les élections au barreau de Paris de 2005
2005-273 17 novembre 2005	Délibération portant avis sur le traitement de données à caractère personnel mettant en œuvre un dispositif de vote électronique pour les élections au barreau de Nanterre de 2005
2005-274 17 novembre 2005	Délibération portant avis sur le traitement de données à caractère personnel mettant en œuvre un dispositif de vote électronique pour les élections au barreau de Lyon de 2005
2005-275 17 novembre 2005	Délibération portant avis sur le traitement de données à caractère personnel mettant en œuvre un dispositif de vote électronique pour les élections aux conseils de quartier de la mairie d'Issy-les-Moulineaux de 2005
2005-276 17 novembre 2005	Délibération portant modification de la norme simplifiée n° 48 concernant les traitements automatisés de données à caractère personnel relatif à la gestion des fichiers de clients et de prospects et portant abrogation des normes simplifiées 11, 17 et 25
2005-277 17 novembre 2005	Délibération modifiant la norme simplifiée n° 46 destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organisations publics et privés pour la gestion de leurs personnels

2005-278 17 novembre 2005	Délibération portant refus d'autorisation de mise en œuvre par la MAAF Assurances SA d'un traitement automatisé de données à caractère personnel basé sur la géolocalisation des véhicules
2005-279 22 novembre 2005	Délibération portant avis sur le projet de décret instituant le passeport électronique et sur les modifications apportées au traitement DELPHINE permettant l'établissement, la délivrance et la gestion des passeports
2005-280 22 novembre 2005	Délibération portant avis sur le projet d'ordonnance relatif aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
2005-281 22 novembre 2005	Délibération portant autorisation de la mise en œuvre par la Cité des sciences et de l'industrie d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux
2005-282 22 novembre 2005	Délibération portant autorisation de la mise en œuvre par la direction régionale des services pénitentiaires (DRSP) de Marseille d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès à l'armurerie
2005-283 22 novembre 2005	Délibération portant autorisation de la mise en œuvre par le conseil général de la Côte d'Or d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux locaux
2005-284 22 novembre 2005	Délibération décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle
2005-285 22 novembre 2005	Délibération portant recommandation sur la mise en œuvre par des particuliers de site web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle
2005-286 22 novembre 2005	Délibération portant autorisation de mise en œuvre par la Caisse centrale de la mutualité sociale agricole d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion de la couverture des non-salariés agricoles contre les accidents du travail et les maladies professionnelles
2005-287 22 novembre 2005	Délibération portant autorisation de mise en œuvre par le GIP réseau douleur soins palliatifs de Hautes-Pyrénées, ARCADE d'un traitement automatisé de données à caractère personnel ayant pour finalité la prise en charge coordonnée de patients en soins palliatifs
2005-288 24 novembre 2005	Délibération portant mise en demeure
2005-289 24 novembre 2005	Délibération portant mise en demeure
2005-290 24 novembre 2005	Délibération portant mise en demeure
2005-291 24 novembre 2005	Délibération portant mise en demeure
2005-292 24 novembre 2005	Délibération portant mise en demeure
2005-293 24 novembre 2005	Délibération portant mise en demeure
2005-294 24 novembre 2005	Délibération portant mise en demeure
2005-295 1er décembre 2005	Délibération portant avis sur un projet de décret en conseil d'État relatif au certificat de décès et modifiant le Code général des collectivités territoriales
2005-296 22 novembre 2005	Délibération portant adoption d'une norme simplifiée relative aux traitements de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet
2005-297 1er décembre 2005	Délibération portant autorisation unique de certains traitements de données à caractère personnel mis en œuvre dans des organismes financiers au titre de la lutte contre le blanchiment de capitaux et le financement du terrorisme
2005-298 8 décembre 2005	Délibération portant autorisation de la mise en œuvre par la société ED d'un traitement automatisé de données à caractère personnel ayant pour finalité d'assurer une protection contre la fraude par chèque bancaire
2005-299 8 décembre 2005	Délibération portant autorisation de mise en œuvre par la direction de la recherche, des études, de l'évaluation et des statistiques du ministère de l'Emploi, de la Cohésion sociale et du ministère de la Santé et des Solidarités d'un traitement automatisé de données à caractère personnel ayant pour finalité d'exploiter, à des fins statistiques, les informations collectées lors de l'enquête « événements de vie et santé »

2005-300 8 décembre 2005	Délibération portant autorisation de mise en œuvre d'un dispositif expérimental baptisé « FAST-État-civil » entre la caisse d'allocations familiales et la mutualité sociale agricole du département des Deux-Sèvres, d'une part, et les communes de Bressuire, Niort, Parthenay, Saint-Maixent et Thouars, d'autre part
2005-301 8 décembre 2005	Délibération portant autorisation, de mise en œuvre par la caisse primaire d'assurance maladie de Strasbourg d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'une base de données des auteurs présumés de fraudes
2005-302 8 décembre 2005	Délibération portant autorisation de mise en œuvre par l'association Réseau ONCOMIP d'un système de données de santé dans le cadre de comités de concertation pluridisciplinaires
2005-303 8 décembre 2005	Délibération portant autorisation de mise en œuvre par l'association du réseau de prise en charge de l'insuffisance cardiaque au sein de l'Isère, d'un traitement automatisé de données à caractère personnel ayant pour finalité la saisie et le partage sécurisés d'informations médicales et paramédicales « patients » entre les professionnels de santé du réseau RESIC 38
2005-304 8 décembre 2005	Délibération portant avis sur le projet d'arrêté présenté par l'agence pour le développement de l'administration électronique et créant le téléservice « monservicepublic.fr »
2005-305 8 décembre 2005	Délibération portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle
2005-306 13 décembre 2005	Délibération portant avertissement à l'encontre de la société GE Money Bank
2005-307 13 décembre 2005	Délibération portant avertissement à l'encontre de la société Banque Populaire Val-de-France
2005-308 13 décembre 2005	Délibération portant mise en demeure
2005-309 13 décembre 2005	Délibération portant mise en demeure
2005-310 13 décembre 2005	Délibération portant mise en demeure
2005-311 13 décembre 2005	Délibération portant mise en demeure
2005-312 20 décembre 2005	Délibération portant avis sur le projet de décret pris pour l'application de la loi n° 78-753 du 17 juillet 1978 modifiée par l'ordonnance n°2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques
2005-313 20 décembre 2005	Délibération portant avis sur le projet de décret modifiant le décret n° 2004-1266 du 25 novembre 2004 pris pour l'application de l'article 8-4 de l'ordonnance n° 45-262658 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 des données à caractère personnel relative aux ressortissants étrangers sollicitant la délivrance d'un visa
2005-314 20 décembre 2005	Délibération modificative de la délibération du 3 février 2005 autorisant une expérimentation présentée par la société Axa France ayant pour finalité d'accéder, sous forme anonymisée, aux données de santé figurant sur les feuilles de soins électroniques
2005-315 20 décembre 2005	Délibération portant autorisation de mise en œuvre par la caisse régionale d'assurance maladie d'Île-de-France d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des infractions aux dispositions du Code de la Sécurité sociale relatives aux règlements des pensions d'invalidité
2005-316 20 décembre 2005	Délibération portant autorisation de mise en œuvre par l'association pour le développement du dossier médical informatisé (ADDMI) d'un traitement automatisé de données à caractère personnel ayant pour finalité la création d'un dossier médical informatisé en réseau pour des patients traités en cancérologie dans l'ouest parisien
2005-317 20 décembre 2005	Délibération portant autorisation de mise en œuvre par le Syndicat mixte des transports en commun (SMTC) de Toulouse d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales

Crédits photo :