COMMISSION
NATIONALE DE
L'INFORMATIQUE
ET DES LIBERTÉS

28e RAPPORT D'ACTIVITÉ 2007

ISBN : 978-2-11-007052-4

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

28e RAPPORT D'ACTIVITÉ 2007

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

Sommaire

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 modifiée en août 2004 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.

Avant-propos

Alex Türk, président de la CNIL

Bourrasques, averses et éclaircies...

La métaphore météorologique a ses vertus, celle de rendre compte de l'imprévisibilité de l'actualité, de sa brutalité parfois, de sa précaire sérénité aussi. Bourrasque d'abord, qui vint de l'ouest, de la volonté du Gouvernement américain d'imposer un effet extraterritorial à ses lois sécuritaires. Ainsi, en vertu d'un accord conclu entre l'Union européenne et le Gouvernement des États-Unis en juillet 2007, tous les passagers aériens à destination des États-Unis et recourant aux services de compagnies aériennes européennes voient, au nom de la légitime lutte contre le terrorisme, leurs données désormais transférées à plus d'une douzaine d'administrations américaines. Ce transfert des données passagers (dites PNR en anglais) est effectué sans contrôle de la part des Européens, pour une durée de 15 ans, et peut entraîner des refus d'embarquement pour des personnes qui auront bien des difficultés à obtenir des explications et à faire valoir leurs droits. De surcroît, les données transférées peuvent « en cas de nécessité », appréciée souverainement par les autorités américaines, porter sur des informations « sensibles » telles que les préférences alimentaires des personnes, leur état de santé, leurs opinions politiques ou leur origine ethnoraciale. En dépit de l'opposition résolue du Parlement européen et des « CNIL » européennes, ce nouvel accord a été signé. Il a le goût amer de l'échec pour notre modèle qui entend concilier la liberté et la sécurité, sans sacrifier l'une à l'autre.

Bourrasque encore, mais plus hexagonale cette fois, qui conduisit la commission chargée de mener une réflexion sur la réforme de nos institutions, présidée par M. Édouard Balladur, à préconiser le démantèlement de la CNIL au profit de la création d'un « défenseur des droits fondamentaux » regroupant d'autres autorités, telles que le Médiateur de la République, la HALDE, le Défenseur des enfants ou encore le Contrôleur général des prisons. Cette proposition est notamment fondée sur l'idée, aujourd'hui erronée, que notre Commission relève d'une autorité de médiation entre les usagers et l'administration. Or, depuis la loi du 6 août 2004, près de 70 % des décisions de la CNIL concernent le secteur privé. Notre Commission est désormais dotée de pouvoirs de conseil, de contrôles sur place et sur pièces, qu'elle entend développer, d'un pouvoir de sanction qui fait que le Conseil d'État l'a récemment qualifiée de « juridiction ». La CNIL n'est donc plus cette autorité chargée de rendre des avis sur les fichiers publics mais un véritable régulateur, du secteur

privé avant tout. Quel serait donc le gain pour nos concitoyens, en termes de protection de leurs libertés, d'une disparition d'un organe collégial et juridictionnel au profit d'une seule personne, aux compétences si étendues qu'elle ne pourrait raisonnablement les exercer ? Il est peu de dire que je m'interroge.

Averse ensuite, dont la France a le génie. En effet, notre pays s'interroge, depuis plusieurs années, sur l'efficacité de son modèle d'intégration républicain, sur la nécessité de lutter contre les discriminations. Or, pour lutter contre les discriminations, encore faut-il pouvoir les mesurer. Pour cela, il est nécessaire de procéder à l'observation statistique des différences, de la diversité sociale, « ethnique », religieuse, culturelle… ? Mais alors, quels critères utiliser pour analyser cette diversité ? Quelles méthodes employer ? Qui peut le faire ? Comment concilier cette nécessité de mieux connaître notre société avec l'interdiction prévue par la loi informatique et libertés de recueillir des données faisant apparaître « directement ou indirectement les origines raciales ou ethniques » des personnes ? Cette problématique est délicate car elle touche à l'essence même de ce qui fait notre identité, à notre conception de la République, à la façon dont on se perçoit et dont on est perçu par les autres.

Compte tenu de ces enjeux, la CNIL a engagé le débat en constituant un groupe de travail. Ce groupe a réalisé plus de 60 auditions et recueilli le point de vue de l'ensemble des acteurs concernés : chercheurs, organisations syndicales, représentants des grandes religions, mouvements associatifs, chefs d'entreprises…

À l'issue de ces travaux, nous avons publié, le 15 mai 2007, 10 recommandations dont l'une d'entre elles tendait à modifier notre loi afin de faciliter les recherches en matière de mesure de la diversité des origines, de la discrimination et de l'intégration tout en améliorant la protection des personnes, de leurs données ainsi que le caractère scientifique des enquêtes. Ces recommandations furent alors unanimement accueillies. Ceci conduisit deux parlementaires, membres de notre Commission, à déposer un amendement en ce sens lors de la discussion au Parlement du projet de loi relatif « à la maîtrise de l'immigration, à l'intégration et à l'asile ». Hélas, vérité d'hier ne l'était plus. Ce qui était consensuel se révéla, à notre grande surprise, polémique. Des commentaires, relevant davantage du pamphlet, prirent le dessus sur le débat de fond, juridique, technique, donc trop subtil pour être entendu. Par sa décision du 15 novembre 2007, le Conseil constitutionnel a censuré cet amendement en estimant qu'il était « sans lien » avec la loi. Le Conseil a également considéré que « si les traitements nécessaires à la conduite des études sur la mesure de la diversité des origines peuvent porter sur des données objectives, ils ne sauraient, sans méconnaître le principe énoncé par l'article 1er de la Constitution, reposer sur l'origine ethnique ou la race ». Soucieuse d'appliquer pleinement la décision du Conseil constitutionnel, comme se le doit toute autorité publique, notre Commission n'a pu que constater le désarroi des

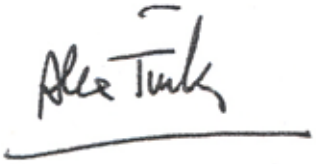
chercheurs face à la complexité de cette décision, certains organismes publics de renom abandonnant des recherches de crainte de ne pas la respecter. Un travail de pédagogie est donc nécessaire. Il doit être engagé sans tarder afin que la recherche française soit rassurée et puisse poursuivre, sereinement, ses travaux. Un récent ajout aux *Cahiers du Constitutionnel* (n° 23) s'y emploie et je m'en réjouis.

Quant aux éclaircies, la première d'entre elles vint, à son tour, d'outre-Atlantique et du règlement de l'affaire SWIFT. La place nous manque pour rappeler ici les interrogations que soulevait l'accès direct des autorités américaines à de nombreuses données bancaires européennes telles que le montant du contrat, son bénéficiaire, la société émettrice, toutes sortes d'informations ayant un rapport indirect avec la lutte contre le terrorisme mais comportant un risque de parenté réelle avec de l'espionnage industriel. Grâce aux efforts conjugués des « CNIL européennes », la base de données de cette entreprise de droit belge, située aux États-Unis, va être rapatriée en Europe. Dès lors, les autorités américaines ne seront plus en mesure d'y accéder en ce qui concerne les échanges intra-européens. Il s'agit d'une victoire importante dans une problématique voisine de celle des « PNR », emblématique d'un certain unilatéralisme juridique américain.

La seconde éclaircie, il faut le souligner, réside dans l'effort budgétaire significatif que le Gouvernement a consenti en notre faveur. Avec 10 créations d'emplois en 2007, 15 en 2008, notre Commission engage sa remise à niveau, mais demeure loin de ses homologues britanniques, allemands ou espagnols. Bien évidemment, ce mouvement devra être poursuivi. Il devra également se traduire par une réorganisation de l'implantation territoriale de la CNIL. En effet, ses nouvelles missions de conseil aux entreprises et aux administrations, d'animation du réseau des correspondants informatique et libertés, d'instruction des plaintes, de contrôle, commandent une déconcentration interrégionale de notre Commission, afin de la rapprocher de la réalité de l'activité économique, de la rendre plus réactive, plus accessible à nos concitoyens.

En un an, il aura été proposé à deux reprises, et par des organismes politiquement diamétralement opposés, la commission Balladur et les mouvements « alternatifs », qui envahirent notre Commission le 14 décembre dernier, de supprimer la CNIL. Quelle leçon en tirer ? J'en vois trois. La première est que ces évènements attestent au moins d'une chose : de l'indépendance de notre Commission. Il n'est rien de plus irritant qu'une institution indépendante dont les positions ne conviennent jamais pleinement à un groupe d'intérêt, quel qu'il soit. La deuxième, c'est que l'indépendance a un prix, qui peut se révéler élevé, mais qui doit toujours être maintenu. La dernière est que l'indépendance de notre Commission est aussi le fruit de ses 30 ans d'expérience. L'année du trentenaire de la création de la CNIL sera l'occasion d'y rendre hommage, au travers de l'organisation, des 15 aux 17 octobre 2008 à Strasbourg, de la conférence mondiale informatique et libertés.

Cette conférence, qui se déroulera dans l'hémicycle du Conseil de l'Europe, sera coorganisée par la CNIL et son homologue allemand, qui célèbrera également son 30e anniversaire. Autour de la question suivante, « comment protéger la vie privée dans un monde sans frontières », elle regroupera plus de 600 participants, venus du monde entier. Représentants des entreprises, d'associations, des autorités de protection des données et des Gouvernements, tous débattront, à l'heure de Facebook et de la convergence des technologies, de la question angoissante : la vie privée n'est-elle pas un espace en voie de disparition ? La France, qui fut précurseur en 1978, se devait de situer les problématiques de la protection de la vie privée à leur niveau pertinent aujourd'hui, à savoir au niveau international. Rendez-vous donc à Strasbourg !



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

LES TEMPS FORTS DE L'ANNÉE 2007

MESURER LA DIVERSITÉ : LES DIX RECOMMANDATIONS DE LA CNIL

Chacun s'accorde sur la nécessité de lutter contre les discriminations. Or, pour lutter contre les discriminations, encore faut-il pouvoir les identifier, les mesurer. Dès lors, quels critères utiliser ? Quelles méthodes statistiques employer ? Qui peut le faire ?

Cette problématique est complexe et délicate :

Complexe, car comme notre Commission a pu le constater, cette « mesure de la diversité » suscite une véritable « effervescence méthodologique », les chercheurs et statisticiens faisant preuve d'une grande imagination en ce domaine et n'étant pas forcément tous d'accord sur les outils à employer.

Délicate, car elle touche à l'essence même de ce qui fait notre identité, à notre conception de la République, à la façon dont on se perçoit et dont on est perçu par les autres. Délicate également car elle ne saurait remettre en cause le fait que la notion de race n'a aucune valeur scientifique.

Après avoir publié, en juillet 2005, ses premières recommandations sur le sujet, la CNIL a approfondi sa réflexion en procédant à plus de 60 auditions : chercheurs, statisticiens, organisations syndicales, représentants des grandes religions, mouvements associatifs, personnalités qualifiées, chefs d'entreprise…

Ces auditions ont montré une grande variété de points de vue, parfois des divergences, et la difficulté d'aboutir à un consensus. Néanmoins, un constat se dégage pour la CNIL : la France doit améliorer son appareil statistique et des réponses peuvent d'ores et déjà être apportées pour faire progresser la connaissance de notre société et, par là même, mieux lutter contre les discriminations.

À cet effet, la CNIL a rendu publiques au mois de mai 2007 ses dix recommandations qui ont été saluées pour leur pragmatisme, leur équilibre et leur juste audace.

Bon à savoir

LES DONNÉES SENSIBLES : QUE DIT LA LOI ?

Au sens de l'article 8 de la loi informatique et libertés, sont considérées comme sensibles et devant donc faire l'objet d'une protection particulière les « données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ».

Le traitement de ces données est interdit, sauf dérogations prévues par la loi, par exemple lorsque :
– le traitement statistique est réalisé par l'INSEE ou un service statistique ministériel et est autorisé par la CNIL ;
– le consentement exprès de la personne a été obtenu et une déclaration faite auprès de la CNIL ;
– l'enquête présente un intérêt public et est autorisée par la CNIL.

L'adresse, la nationalité et le lieu de naissance ne sont pas considérés par la CNIL comme des données « sensibles » au sens de l'article 8 de la loi. En effet, l'information sur le lieu de naissance de la personne fait partie de l'état civil et est considérée comme une donnée « objective ».

La Commission porte cependant une attention particulière au traitement des données relatives à la nationalité et au lieu de naissance dans les fichiers, la pertinence de leur collecte devant être dûment justifiée, au cas par cas, par le responsable du traitement.

Les dix recommandations de la CNIL en matière de mesure de la diversité

• **Ouvrir plus largement aux chercheurs** l'accès aux bases de données statistiques et aux fichiers de gestion.

• **Utiliser les données « objectives » relatives à l'ascendance des personnes** (nationalité et/ou lieu de naissance des parents) dans les enquêtes pour mesurer la diversité.

• **Ne pas intégrer de données sur l'ascendance des personnes** dans les fichiers des entreprises et des administrations (personnel et usagers).

• **Développer des études sur le « ressenti » des discriminations**, incluant le recueil de données sur l'apparence physique des personnes.

• **Admettre, sous certaines conditions, l'analyse des prénoms et des patronymes** pour détecter d'éventuelles pratiques discriminatoires.

• **Modifier la loi informatique et libertés pour assurer une meilleure protection des données sensibles** en garantissant le caractère scientifique des recherches et en harmonisant les procédures de contrôle des fichiers de recherche.

• **Refuser en l'état la création d'un référentiel national ethnoracial.**

• **Développer le recours à des experts**, tiers de confiance pour mener les études de mesure de la diversité.

• **Garantir la confidentialité et l'anonymat** par le recours aux techniques d'anonymisation.

• **Garantir l'effectivité des droits informatique et libertés en assurant la transparence.**

Les points forts de ces recommandations

Il est indispensable de permettre aux chercheurs d'accéder plus facilement aux fichiers de personnel, aux fichiers administratifs et aux bases statistiques publiques, dans le respect de la protection des données.

Pour mesurer la réalité de la discrimination vécue, il faut aussi développer les enquêtes par questionnaires auprès des personnes concernées. Dès lors qu'elles sont facultatives, fondées sur l'autodéclaration, et que les réponses sont confidentielles, des questions doivent pouvoir être posées sur la nationalité et le lieu de naissance des personnes et de leurs parents. Il est aussi important que les personnes qui se sentent discriminées indiquent les critères – apparence physique, langue, nom… – sur lesquels se fonde, selon elles, cette discrimination.

En outre, l'analyse des prénoms et des patronymes, sous certaines conditions – c'est-à-dire quand elle n'aboutit pas à un classement dans des catégories ethnoraciales – peut être utile pour détecter d'éventuelles pratiques discriminatoires.

À cet égard, la CNIL reste très réservée sur la création d'un référentiel ethnoracial. Les personnes auditionnées sont dans leur grande majorité hostiles à une telle nomenclature. Risques de renforcement des stéréotypes, de stigmatisation, classification incertaine, non scientifique, réductrice, approximative… : autant de raisons qui expliquent les réticences actuelles et qui justifient une attitude extrêmement réservée sur ce sujet. La Commission a estimé que la décision de principe de créer une telle nomenclature, si elle devait être utilisée de façon obligatoire, en particulier pour les statistiques publiques et pour le recensement, appartiendrait au Législateur sous le contrôle du Conseil constitutionnel.

Enfin, il est nécessaire de modifier la loi informatique et libertés afin d'assurer une meilleure protection des personnes et de leurs données sensibles, en garantissant le caractère scientifique des recherches et en renforçant le contrôle de la CNIL sur ces fichiers de recherche pour lesquels le seul consentement des personnes ne saurait suffire.

Les suites données à ces recommandations

Pour faire suite aux recommandations de la CNIL, Michèle Tabarot, députée des Alpes-Maritimes, et Sébastien Huyghe, député du Nord, tous deux membres de la CNIL, ont présenté un amendement au projet de loi relatif à la maîtrise de l'immigration, à l'intégration et à l'asile, visant à soumettre à autorisation de la CNIL les traitements de données faisant directement ou indirectement apparaître les origines raciales ou ethniques des personnes pour les besoins d'études ayant pour finalité « la mesure de la diversité des origines des personnes, de la discrimination et de l'intégration ». Afin de s'assurer de la qualité scientifique de ces études, il était prévu que la CNIL puisse saisir un comité désigné par décret. Afin de ne pas créer une nouvelle structure, il était envisagé de faire appel au conseil scientifique du Comité de concertation pour les données en sciences humaines et sociales, créé auprès des ministres de l'Économie, de l'Emploi, de l'Éducation nationale et de la Recherche.

Cette disposition, qui a suscité de vifs débats et controverses, faute sans doute d'une bonne compréhension de la problématique, a été adoptée par le Parlement mais a fait l'objet d'un recours devant le Conseil constitutionnel. Par une décision du 15 novembre 2007, le Conseil l'a déclaré contraire à la Constitution, estimant que cette disposition était sans lien avec une loi portant sur l'entrée et le séjour des étrangers en France.

Sur le fond, le Conseil a considéré que « si les traitements nécessaires à la conduite d'études sur la mesure de la diversité des origines des personnes, de la discrimination et de l'intégration peuvent porter sur des données objectives, ils ne sauraient, sans méconnaître le principe énoncé par l'article 1er de la Constitution, reposer sur l'origine ethnique ou la race [...] ».

Si cette décision semble ainsi fermer la porte à l'élaboration d'un référentiel ethno-racial en France, ce qui répond aux réserves exprimées sur ce point par la CNIL, elle laisse ouverte la question de savoir quels types d'études peuvent aujourd'hui être conduits dans le domaine de la mesure de la diversité, de la discrimination et de l'intégration. La réponse à cette question intéresse bien entendu au plus haut point le monde de la recherche.

Il reste à espérer que 2008 sera le temps de l'apaisement sur un sujet décidément trop passionnel et permettra d'examiner sereinement des projets de recherche qui fondamentalement n'ont d'autre but que d'améliorer la connaissance de notre société et de mieux lutter contre les discriminations.

Pour plus d'infos sur la collecte des données ethniques en Europe, lire le rapport d'études *Statistiques « ethniques » et protection des données dans les pays du Conseil de l'Europe*, réalisé par P. Simon (INED) et publié par la Commission européenne contre le racisme et l'intolérance du Conseil de l'Europe, octobre 2007, et disponible sur www.coe.int/ecri.

Le rapport et les recommandations de la CNIL sont disponibles sur www.cnil.fr

La CNIL conseille

Afin de garantir à la fois le sérieux scientifique des études sur la mesure de la diversité ou de la discrimination et la protection de la vie privée, la CNIL recommande aux organismes qui souhaitent réaliser de telles études de faire appel à des experts extérieurs indépendants (un organisme de recherche, par exemple) qui soient également des tiers de confiance à même de garantir la confidentialité des données et l'anonymat des personnes lors de la diffusion des résultats. À cet égard, la CNIL considère que les pouvoirs publics doivent encourager un recours beaucoup plus systématique aux techniques de chiffrement et d'anonymisation.

Les personnes enquêtées doivent être parfaitement informées des objectifs et des conditions de réalisation de l'enquête, du caractère facultatif de celle-ci, ainsi que de leurs droits d'opposition, d'accès et de rectification. Cette information, pourtant essentielle, est trop souvent négligée. Or, dans un domaine aussi sensible que la mesure de la diversité et la lutte contre les discriminations, elle constitue un facteur clé pour assurer l'adhésion, garantir la confiance et la participation pleine et entière de chacun.

De même, la consultation des instances représentatives du personnel en cas d'enquêtes menées dans le domaine de l'emploi est préconisée. De façon plus générale, il est souhaitable que le lancement des enquêtes nationales soit annoncé publiquement de façon à sensibiliser la population sur ces questions.

GÉRER LES FICHIERS CENTRAUX DE CRÉDIT ET DE LOGEMENT

Qu'est-ce que c'est ?

UN FICHIER CENTRAL DE CRÉDIT OU FICHIER POSITIF

Un fichier central de crédit regroupe des informations sur la situation financière des personnes, qu'elles présentent, ou non, des impayés. On l'appelle communément fichier positif par opposition au fichier négatif qui ne recense que les incidents de paiement en matière de crédit.

La mise en place de fichiers permettant à l'ensemble d'un secteur d'activité, qu'il s'agisse des établissements de crédit ou des bailleurs professionnels, d'avoir des informations sur les risques d'insolvabilité des personnes, suscite une grande vigilance de la part de la CNIL compte tenu du risque évident d'exclusion sociale des personnes concernées.

La question de la légitimité et de la proportionnalité de l'introduction d'une centrale de crédit positive se pose tant en termes d'atteinte à la vie privée qu'en termes d'efficacité et de coûts. La Commission s'est toujours refusée à reconnaître la légitimité de la mise en place d'une telle centrale en l'absence d'un encadrement légal spécifique (rapport sur les « centrales positives » de janvier 2005 ; rapport d'activité 2005). Elle estime que seul le Législateur a compétence pour se prononcer sur l'utilité sociale d'un « fichier positif » dans le secteur du crédit et pour préciser les finalités et le contenu de cette base de données. Dans le droit fil de cette position, elle a refusé d'autoriser la mise en œuvre par la société Experian d'une centrale de crédit (délibération du 8 mars 2007).

Et le droit au logement opposable ?

Par ailleurs, elle a refusé d'autoriser la société Infobail à mettre en œuvre deux traitements relatifs à l'information des professionnels de l'immobilier sur la gestion des impayés ou le recensement des locataires d'immeuble d'habitation respectant leurs obligations de paiement. La CNIL a considéré que ces fichiers portaient atteinte au droit au logement institué par le Législateur, auquel il revient de se prononcer sur la constitution de fichier tant « négatif » que « positif » dans le secteur du logement (délibérations du 10 juillet 2007).

Questions à ...

PHILIPPE NOGRIX

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

Pourquoi avoir refusé la centrale de crédit d'Experian ?

Trois raisons ont motivé ce refus :
– des informations couvertes par un secret légalement protégé, à savoir le secret bancaire, auraient été transférées de façon massive, en l'absence de toute base législative, à une société de services qui ne relève pas de la loi bancaire et dont l'activité n'est pas soumise à la règle du secret bancaire ;
– les clients n'auraient pas été informés dans des conditions satisfaisantes des conséquences de la signature de la clause de levée du secret bancaire ;
– la transmission aux établissements adhérents à la centrale des informations relatives à une personne au moment de l'instruction d'une demande de crédit, sous la forme d'un rapport très détaillé sur les crédits en cours ou intégralement remboursés depuis moins de trois ans, auraient permis un profilage économique des particuliers concernés. De telles informations étaient susceptibles d'être conservées dans les fichiers informatisés des organismes destinataires et ainsi d'être utilisées au-delà de l'instruction d'une demande de crédit, notamment à des fins commerciales.

Pourtant, la CNIL a autorisé des échanges d'informations au sein des groupes bancaires. Quelles sont les différences avec le dossier Experian ?

La CNIL a effectivement autorisé plusieurs filiales spécialisées dans le crédit à la consommation de groupes bancaires, en 2005, le Crédit agricole (FINAREF et SOFINCO) et en 2006, BNP Paribas (CETELEM et COFINOGA) à partager des informations sur les emprunteurs à des fins de prévention des impayés en dégageant cinq critères que ne remplissait pas totalement la société Experian :
– la légitimité de la finalité : la prévention de la fraude et des impayés ;
– le caractère ponctuel et limité des échanges d'informations entre les organismes bénéficiaires : aucune base centralisée n'est créée. Les fichiers clients des organismes ne peuvent pas être enrichis à partir des données transmises par le système de requête ;
– la qualité des organismes bénéficiant de l'échange des données : des sociétés spécialisées dans le crédit à la consommation, donc soumises au secret bancaire ;
– l'existence d'une communauté de risque financier entre ces organismes, qui se traduit par l'exercice d'un contrôle effectif de certaines des sociétés sur les autres ou la gestion du risque pour le compte de tiers ;
– l'autorisation explicite du client de partager des informations couvertes par le secret bancaire qui suppose notamment qu'il soit clairement informé sur les finalités et les bénéficiaires de l'échange.

Dernière minute

Lors de son audition par la commission des Affaires économiques de l'Assemblée nationale le 16 janvier 2008, Alex Türk a insisté sur l'importance croissante du pouvoir de régulation économique de la CNIL. Il a rappelé les problématiques majeures qui se posent dans ce domaine, en soulignant que les technologies utilisées soulèvent des enjeux importants en matière de protection de la vie privée. Ainsi, le traçage des personnes par la biométrie, la vidéosurveillance et la géolocalisation posent la question du respect des droits des salariés.

Les dossiers Discovery (transfert aux États-Unis d'informations contenues dans des disques durs appartenant à des salariés français), SWIFT (transmission aux États-Unis de données bancaires) et PNR (transmission d'informations sur les passagers aériens aux services de sécurité américains) mettent en lumière les profondes divergences de vues entre les Européens et les Américains concernant le niveau de protection des données. Ces dispositifs, mis en place par les États-Unis pour renforcer la lutte contre le terrorisme, posent en effet des questions fondamentales en matière de protection des données et parfois même en matière de souveraineté économique des États.

Concernant les fichiers centraux de crédit, la Commission considère qu'elle est allée au bout de sa réflexion et qu'il appartient désormais au Législateur de se prononcer sur la création d'un tel outil.

ENCADRER LA BIOMÉTRIE

Les chiffres 2007 : une explosion des demandes

Au cours de l'année 2007, **515 dispositifs biométriques** ont été soumis à la CNIL, soit une augmentation de plus de 43 % par rapport à 2006.

449 d'entre eux entrent dans le cadre d'un engagement de conformité en matière de biométrie adopté par la CNIL en 2006 afin d'encadrer les modalités d'utilisation et simplifier les formalités déclaratives de certains dispositifs biométriques (autorisations uniques) :
– 90 utilisent le contour de la main pour le contrôle d'accès, la gestion des horaires et de la restauration sur les lieux de travail ;
– 275 utilisent l'empreinte digitale exclusivement enregistrée sur un support individuel pour le contrôle de l'accès aux locaux sur les lieux de travail ;
– 84 utilisent le contour de la main pour l'accès au restaurant scolaire.

La Commission a également examiné en séance 66 dispositifs qui n'entraient pas dans le champ d'application des autorisations uniques précitées : **21 ont fait l'objet d'un refus d'autorisation**, 45 ont été autorisés.

Enfin, plus de 120 demandes d'autorisation sont encore en cours d'instruction par les services de la Commission.

Qu'est-ce que c'est ?

LA BIOMÉTRIE

La biométrie regroupe 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...).

MÉMO BIOMÉTRIE

- **en 2005, la CNIL a autorisé la mise en œuvre de 34 dispositifs biométriques et en a refusé 5 ;**
- **en 2006, elle en a autorisé 351 et refusé 9 ;**
- **en 2007, elle en a autorisé 494 et refusé 21.**

Les titres biométriques

Le visa biométrique ou VISABIO

Saisie par le ministère de l'Intérieur d'un projet de décret portant création d'un fichier relatif aux ressortissants étrangers sollicitant la délivrance d'un visa, la Commission a rendu son avis le 10 juillet 2007 (délibération n° 2007-195).

Le nouveau dispositif, dénommé VISABIO, qui généralise les expérimentations menées depuis 2004 dans le cadre du programme BIODEV, devrait concerner, chaque année, plus de 2 millions d'étrangers ressortissants de pays soumis à l'obligation de visa. Le dispositif envisagé prévoit le recueil et la conservation, dans une base centrale, de données biométriques (photographie numérisée du visage et empreintes digitales des dix doigts), associées aux données d'identité déjà recueillies dans le cadre de la procédure de demande de visa.

Tout en observant que l'usage de données biométriques peut présenter de réels avantages dans le cadre de la vérification de l'identité des porteurs et de l'authenticité des titres, la Commission a estimé qu'il devait être entouré de strictes garanties. Elle a notamment regretté qu'il ne soit pas envisagé de recourir à la simple conservation par l'intéressé de ses propres données biométriques dans une carte individuelle, hypothèse qui soulève moins de problèmes du point de vue de la protection des données à caractère personnel. En effet, dans ce cas, seule la personne concernée détient le support dans lequel ces dernières sont enregistrées.

La Commission a également souligné que le recueil des empreintes digitales des mineurs dès l'âge de 6 ans ne pouvait être considéré comme une simple mesure d'ordre technique et que son principe méritait de faire l'objet d'un large débat.

Le passeport biométrique

Saisie à l'automne par le ministère de l'Intérieur, la Commission s'est prononcée sur ce projet de décret le 11 décembre 2007 (délibération n° 2007-365).

Ce projet vise à mettre la France en capacité d'émettre, avant le 28 juin 2009, des passeports dotés d'un composant électronique contenant non seulement l'image numérisée du visage mais aussi celle de deux empreintes digitales, conformément aux dispositions du règlement du Conseil européen du 13 décembre 2004.

Dans le même temps, il apporte des modifications significatives au fichier de gestion des passeports, dénommé DELPHINE puisqu'il prévoit la conservation dans cette base de l'image numérisée du visage du demandeur et des empreintes digitales de huit doigts.

Constatant que le dispositif envisagé conduisait à la mise en place de la première base centralisée de données biométriques à finalité administrative portant sur des ressortissants français, la Commission a émis un certain nombre de réserves à son propos.

Elle a notamment rappelé que le traitement, sous une forme automatisée et centralisée, de telles données ne pouvait être admis que dans la mesure où il était justifié par un impératif de sécurité ou d'ordre public.

À cet égard, la Commission a considéré que, si légitimes soient-elles, les finalités invoquées, à savoir l'amélioration du processus de délivrance et de renouvellement des titres ainsi que la lutte contre la fraude documentaire, ne justifiaient pas la conservation, sur le plan national, de données biométriques telles que les empreintes digitales et que le traitement mis en œuvre serait de nature à porter une atteinte excessive à la liberté individuelle.

En outre, même si le ministère de l'Intérieur a insisté sur le fait qu'il ne serait pas possible de procéder à une recherche en identification à partir de l'image numérisée des empreintes digitales (il ne sera pas possible de retrouver les données d'état civil d'une personne à partir de ses empreintes digitales) et que le système ne comporterait pas de dispositif de reconnaissance faciale à partir de l'image numérisée de la photographie (il ne sera pas possible de retrouver les données d'état civil des personnes à partir de l'image du visage), la conservation dans une base centrale des images numérisées du visage et des empreintes digitales semble disproportionnée.

Enfin, la Commission a regretté que ce nouveau cadre soit défini par voie réglementaire, les modifications introduites par le projet de décret étant bien plus importantes que celles commandées par les engagements européens de la France. L'ampleur de la réforme et l'importance des questions justifieraient sans doute le dépôt d'un projet de loi, lequel permettrait l'engagement d'un vaste débat public.

Bon à savoir

Le premier passeport biométrique devrait être délivré par la France courant octobre 2008. Le 28 juin 2009, l'ensemble des passeports délivrés par les autorités françaises devra répondre aux prescriptions du règlement européen du 13 décembre 2004.

Les programmes de recherche

Pour la première fois, la CNIL a autorisé le 18 janvier et le 4 octobre 2007 la mise en œuvre de trois programmes de recherche dans le domaine de la biométrie.

Deux de ces autorisations concernent des projets publics présentés par l'université d'Évry-Val d'Essonne et le Groupement des écoles de télécommunications (GET). Ces programmes ont pour objet :
– l'évaluation des procédés de reconnaissance biométrique ;
– la constitution de bases de données biométriques « multimodales », c'est-à-dire combinant l'utilisation de plusieurs biométries (visages en deux et trois dimensions, iris, empreintes digitales, forme de la main).

La troisième autorisation porte sur un projet européen coordonné par la société Sagem Défense Sécurité réunissant douze autres partenaires. Il a pour finalité l'amélioration des dispositifs de reconnaissance du visage en trois dimensions et la sécurisation des données biométriques.

Ces programmes de recherche, qui reposent sur la participation de volontaires, revêtent une grande importance, car ils sont un moyen pour la CNIL de disposer d'évaluations fiables sur l'état des techniques. Des bilans relatifs aux résultats de ces recherches seront communiqués à la Commission.

Reconnaissance vocale et réseau veineux

L'année 2007 a également été l'occasion d'examiner la première demande d'installation d'un système de reconnaissance vocale. Il s'agit d'un dispositif ayant pour objet de sécuriser et de faciliter la gestion et la réinitialisation des mots de passe utilisés pour accéder au système d'information de la société Michelin. Ce procédé permet de générer et de réinitialiser automatiquement les mots de passe, notamment lorsque la personne les a oubliés. À cette occasion, la Commission s'est assurée de la bonne information des employés et du fait que toutes les mesures étaient prises pour garantir la sécurité des données et prévenir les risques d'usurpation d'identité.

De même, la CNIL a examiné pour la première fois le 8 novembre 2007 cinq dispositifs reposant sur la reconnaissance du réseau veineux du doigt de la main et ayant pour objet le contrôle de l'accès aux locaux ou à des systèmes d'information. Après avoir effectué une expertise technique approfondie de cette technologie, la CNIL a considéré que le réseau veineux, en l'état actuel de la technique, est une **biométrie sans trace** dont l'enregistrement dans une base de données ne comporte pas de risques particuliers au regard de la protection des données.

Qu'est-ce que c'est ?

BIOMÉTRIE SANS TRACE OU AVEC TRACE

Parmi toutes les données biométriques utilisées aujourd'hui, certaines présentent la particularité de pouvoir être capturées et utilisées à l'insu des personnes concernées. C'est le cas, par exemple, des empreintes génétiques puisque chacun laisse involontairement derrière soi des traces, même infimes, de son corps, dont on peut extraire l'ADN. C'est également le cas des empreintes digitales, dont on laisse aussi des traces, plus ou moins facilement exploitables, dans beaucoup d'actes de la vie courante.

D'autres données biométriques ne présentent pas, du moins dans l'état actuel de la technique, cette particularité : c'est le cas, par exemple, du réseau veineux du doigt ou du contour de la main, car ces données biométriques laissent peu de trace au quotidien, voire aucune.

La biométrie avec trace impose donc une vigilance toute particulière de la part des personnes concernées.

Une grille d'analyse concernant l'usage des empreintes digitales

C'est en 1997 que la Commission s'est prononcée pour la première fois sur un dispositif reposant sur la reconnaissance des empreintes digitales. Dix ans après, la Commission a estimé nécessaire de préciser sa position et vient de présenter, dans un document public, les principaux critères sur lesquels elle se fonde pour autoriser ou refuser le recours à des dispositifs reposant sur la **reconnaissance des empreintes digitales avec stockage** sur un terminal de lecture-comparaison ou sur un serveur.

Cette grille d'analyse repose sur le constat que :
– l'empreinte digitale est une biométrie à trace. Chaque personne laisse des traces de ses empreintes digitales, exploitables plus ou moins facilement, dans beaucoup de circonstances de la vie courante, par exemple sur un verre, sur une poignée de porte, etc. ;
– **ces traces peuvent être capturées à leur insu** et être utilisées notamment pour usurper leur identité (utiliser l'exemplaire de l'empreinte prélevée pour frauder un dispositif de reconnaissance d'empreintes digitales).

La prise en compte de ces particularités et des risques associés a amené la CNIL à distinguer les dispositifs en fonction du mode de stockage des empreintes :
– stockage sur un support individuel (carte à puce ou clé USB) = risque limité, car **la personne a la maîtrise de sa donnée biométrique** qui ne peut pas être utilisée pour l'identifier à son insu ;
– stockage sur le terminal de lecture-comparaison ou sur un serveur = risque plus important, car la personne perd la maîtrise de sa donnée qui est détenue par un tiers. En cas d'intrusion dans le système, on peut accéder à l'ensemble des empreintes.

Ainsi, la Commission n'autorise la mise en œuvre de dispositifs reposant sur la reconnaissance des empreintes digitales avec un enregistrement dans une base de données que s'ils sont justifiés par un fort impératif de sécurité et satisfont à quatre exigences :
– **la finalité** du dispositif doit être limitée au contrôle de l'accès d'un nombre limité de personnes à une zone bien déterminée, représentant ou contenant un enjeu majeur dépassant l'intérêt strict de l'organisme tel que la protection de l'intégrité physique des personnes, celle des biens et des installations ou encore celle de certaines informations ;

– **la proportionnalité** : il importe de savoir si le système proposé est le mieux adapté à la finalité préalablement définie eu égard aux risques qu'il comporte en matière de protection des données à caractère personnel et aux autres systèmes utilisables ;
– **la sécurité** : le dispositif doit permettre à la fois une authentification et/ou une identification fiable des personnes et comporter toutes les garanties de sécurité pour éviter la divulgation des données ;
– **l'information** des personnes concernées doit être réalisée dans le respect de la loi informatique et libertés et, le cas échéant, du Code du travail.

Les contrôles

Plus de **25 missions de contrôle sur place** ont été effectuées au cours de l'année 2007. Elles visaient à apprécier les conditions dans lesquelles sont mis en œuvre, au regard de la loi informatique et libertés, des dispositifs de reconnaissance biométrique. Plusieurs enseignements peuvent être retirés de ces contrôles :
– les dispositifs de reconnaissance de l'empreinte digitale reposent trop souvent sur une centralisation des données biométriques, sans qu'un fort impératif de sécurité justifie un tiers et lui permettre de les conserver n'est jamais un acte anodin, surtout lorsqu'il s'agit de l'empreinte digitale qui est une biométrie à trace pouvant être capturée et utilisée à l'insu des personnes.

Regards croisés

FRANÇOIS GIQUEL

Vice-président, conseiller maître honoraire à la Cour des comptes
En charge du secteur « Justice »

Quels sont les éléments déclencheurs qui ont poussé la Commission à préciser sa doctrine concernant les dispositifs reposant sur l'enregistrement des empreintes digitales dans une base de données ?

F. Giquel : compte tenu de l'évolution technologique dans le domaine de la biométrie et de la diversité des situations rencontrées, il est apparu indispensable de rappeler et de préciser les principaux critères sur lesquels la CNIL se fonde pour examiner les demandes d'autorisation qui lui sont adressées. Il était nécessaire de permettre aux entreprises, administrations et collectivités locales qui envisagent de se doter de tels dispositifs de se poser « les bonnes questions informatique et libertés » avant de prendre leur décision et de déposer une demande d'autorisation auprès de la CNIL.

Qu'est-ce qui justifie l'attention particulière de la Commission concernant ce type de dispositif ?

D. Gasse : à la différence de toute autre donnée d'identité, la donnée biométrique n'est pas attribuée par un tiers ou choisie par la personne : elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable. Elle appartient donc à la personne qui l'a générée. On comprend dès lors que toute possibilité de détournement ou de mauvais usage de cette donnée fait peser un risque majeur sur son identité. Confier ses données biométriques à

DIDIER GASSE

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

Quels sont les critères retenus par la Commission pour apprécier le caractère proportionné ou non d'un dispositif reposant sur l'enregistrement des empreintes digitales dans une base de données ?

F. Giquel : d'une manière générale, l'objectif poursuivi par le recours au stockage des empreintes digitales dans une base de données pourra presque toujours être atteint grâce à une autre technologie reposant sur le stockage de l'empreinte dans un support individuel (carte à puce). Néanmoins, une base centrale peut présenter un avantage lorsque l'accès doit être assuré à tout moment et sans délai, pour faire face à des situations d'urgence nécessitant une intervention aussi rapide que possible.

D. Gasse : notons également que dans la mesure où il s'agit de situations où l'enjeu de sécurité est majeur, la pertinence, l'adéquation et le caractère non excessif d'un système avec une base d'empreintes digitales sont aussi examinés au regard du nombre des personnes concernées : plus la zone est circonscrite et le nombre de personnes concernées réduit, plus les inconvénients d'une base d'empreintes digitales diminuent.

réellement un tel choix. Il peut s'agir d'une méconnaissance de la part du responsable de traitement des préconisations de la CNIL ou d'un mauvais paramétrage du logiciel qui conduit, à l'insu de son utilisateur, à une telle situation ;
– l'information des personnes est manifestement insuffisante, essentiellement en ce qui concerne les finalités du traitement et l'existence des droits d'accès et d'opposition ;
– la mise en place de dispositifs de reconnaissance biométrique ne s'accompagne pas des mesures de sécurité nécessaires : les logiciels de gestion d'accès et les bases de données biométriques ainsi constituées ne sont pas suffisamment protégés.

Lorsque les manquements relevés à l'occasion des missions de contrôle ont été considérés comme sérieux (en cas d'absence d'autorisation de la Commission par exemple), la formation contentieuse de la CNIL, compétente pour prononcer des sanctions, a été saisie afin de garantir que l'organisme contrôlé modifie les caractéristiques du traitement qu'il met en œuvre.

Des discussions sont par ailleurs actuellement en cours entre la Commission et des sociétés commercialisant des dispositifs biométriques. L'objectif est que ces sociétés s'engagent à :
– informer leurs clients de la nécessité de demander l'autorisation de la Commission pour la mise en œuvre de traitements biométriques ;
– sensibiliser leurs commerciaux aux dispositions informatique et libertés ;
– supprimer de leurs supports publicitaires toute indication trompeuse laissant supposer que la CNIL aurait labellisé leurs dispositifs biométriques (la CNIL n'a pour l'heure pas encore utilisé son pouvoir de labellisation).

AFFAIRE SWIFT : VERS UNE SORTIE DE CRISE

La presse américaine a révélé en juin 2006 l'existence d'un programme de surveillance des transactions bancaires internationales, mis en place par la CIA peu après les attentats du 11 septembre 2001. Ces révélations ont indiqué que la CIA et le département du Trésor américain bénéficiaient d'un accès, depuis des années, à des millions de données transitant par SWIFT, principal réseau international de messagerie utilisé dans le domaine bancaire (*cf.* rapport annuel 2006).

Cet accès, mis en place au titre de la lutte contre le financement du terrorisme, permet de surveiller non seulement les transferts financiers vers les États-Unis mais également tous les autres types de transactions réalisés par SWIFT, y compris à l'intérieur de l'Union européenne. Sont ainsi communiqués le montant de la transaction, la devise, la date valeur, le nom du bénéficiaire, le client qui a demandé la transaction financière et son institution financière. L'objectif officiel consiste à identifier des personnes supposées liées à des activités de financement du terrorisme. Mais les craintes d'utilisation à d'autres fins, moins sécuritaires et plus économiques, ne peuvent être éludées.

Le Groupe de coordination des CNIL européennes (Groupe de l'article 29, ou G29) dans son avis de novembre 2006, a jugé que la société SWIFT n'avait pas respecté les règles européennes de protection des données, notamment en prêtant son concours à la mise en œuvre du programme de surveillance des données bancaires et financières par les autorités américaines. Il a jugé également que les institutions financières avaient une part de responsabilité dans cette affaire.

Un an après, on peut parler de sortie de crise. Le G29 a publié un communiqué de presse le 11 octobre 2007 pour saluer les progrès substantiels accomplis par SWIFT pour se mettre en conformité avec les principes de protection des données.

L'achèvement des négociations Europe – États-Unis

Au printemps 2007, la Commission européenne et le Conseil ont négocié avec le gouvernement américain un certain nombre de garanties afin de définir les règles d'usage des données stockées aux États-Unis dans la base SWIFT par les autorités américaines. Ces garanties concernent la limitation des usages à la lutte contre le terrorisme, le respect du principe de nécessité, des durées de conservation de cinq ans et la nomination d'une « personnalité européenne éminente » ayant compétence pour vérifier le bon fonctionnement du programme de surveillance (Jean-Louis Bruguière).

Cet accord politique a fait l'objet d'un échange de lettres qui ont été publiées par la Commission européenne.

Qu'est-ce que c'est ?

SWIFT *(Society for Worldwide Interbank Financial Telecommunication)*

Il s'agit d'une société coopérative de droit belge fondée en 1973, qui offre aux banques un ensemble de services, dont un système de messagerie sécurisée. Une grande partie des transferts bancaires internationaux transite aujourd'hui par cette société, dont les services sont devenus incontournables pour les milieux concernés.

Une architecture technique complètement restructurée

L'architecture actuelle de SWIFT repose sur le principe d'une copie systématique de tous les messages dans deux centres opérationnels, l'un aux Pays-Bas, l'autre aux États-Unis. Ainsi, quelles que soient leur origine et leur destination, ces messages sont actuellement stockés durant 148 jours dans le centre opérationnel américain.

Cependant, à la fin de l'année 2009, cette architecture sera intégralement modifiée avec l'implantation d'un nouveau centre opérationnel en Suisse. Les messages émis par les clients de banques européennes seront systématiquement copiés dans les deux centres européens (Suisse et Pays-Bas), et ne transiteront plus par le serveur américain. La surveillance américaine ne s'exercera donc pas, en particulier, sur les messages concernant des transferts intra-Union européenne. Les messages en provenance ou à destination des États-Unis seront quant à eux systématiquement stockés dans le centre opérationnel américain.

C'est votre droit

Dès le printemps 2007, la Commission européenne a rappelé avec fermeté aux autorités membres du G29 l'importance du fait qu'elles s'assurent que les banques informent leurs clients utilisateurs de SWIFT de l'existence de transferts de données potentiels vers les autorités américaines, aux fins de lutte contre le terrorisme. La rédaction de notices d'information uniformes, applicables à toute l'Union européenne, ne s'avérant pas réaliste, c'est une coopération entre autorités et fédérations bancaires nationales qui a été retenue. La CNIL a ainsi œuvré en ce sens avec la FBF et plusieurs réseaux bancaires. Vous devez donc désormais être informé par votre banquier de ces transferts.

Questions à …

GEORGES DE LA LOYÈRE

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

Qu'est-ce qui vous fait dire que l'affaire SWIFT est derrière nous ?

De nombreux progrès ont été accomplis par SWIFT dans son programme de mise en conformité par rapport à l'avis du G29 de novembre 2006. Un an plus tard, on peut souligner :
– l'aboutissement des procédures d'adhésion de la filiale américaine de SWIFT au Safe Harbor ;
– la révision des documents contractuels de SWIFT,
– la mise au point d'une nouvelle charte de protection des données (*privacy policies*) ;
– la modification substantielle de l'architecture technique de son réseau, selon une logique de «régionalisation». Il est incontestable que cette modification de l'architecture technique du réseau SWIFT permet de parler de sortie de crise.

Quelles conséquences en tirez-vous ?

L'existence de tels programmes de surveillance doit inciter la CNIL, ses homologues européens, comme les gouvernements et les institutions européennes, à rester extrêmement vigilants quant au phénomène de centralisation, pour des raisons techniques, d'informations massives et parfois sensibles sur le territoire d'États étrangers, notamment aux États-Unis.

LA VIDÉOSURVEILLANCE SOUS L'ŒIL DE LA CNIL

La CNIL toujours plus sollicitée

La Commission constate depuis cinq ans un fort accroissement des formalités déclaratives relatives à la vidéosurveillance. Le nombre de déclarations est en augmentation constante depuis 2002, avec des augmentations fortes en 2004 (quatre fois plus de dossiers qu'en 2003) et 2006 (trois fois plus de dossiers qu'en 2005, soit quasiment 20 fois plus de dossiers qu'en 2003).

L'augmentation se poursuit en 2007 : la CNIL a ainsi enregistré **1317 déclarations** relatives à des systèmes de vidéosurveillance, pour un total de **2980 déclarations sur la période 2002-2007**. Chaque déclaration concerne, dans la grande majorité des cas, plusieurs caméras.

Le nombre de plaintes relatives à la vidéosurveillance est passé de 114 en 2006 à 121 en 2007.

Typologie des plaintes relatives à la vidéosurveillance en 2007 :
- 70 concernent le secteur « travail » ;
- 20, le secteur « logement » (problème de copropriété et de voisinage) ;
- 13, les collectivités locales et les polices municipales ;
- 3, l'Éducation nationale ;
- les 15 restantes, divers autres secteurs.

En 2007, le service des contrôles a été amené à contrôler les dispositifs de vidéosurveillance dans huit organismes.

Une nécessaire clarification du régime de la vidéosurveillance

À l'occasion de l'audition à la CNIL, le 22 novembre 2007, de Michèle Alliot-Marie, ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales, la Commission a rappelé que les saisines de la CNIL étaient toujours plus nombreuses sur ce thème. Par conséquent, une clarification des textes applicables et surtout une harmonisation voire une unification des régimes de formalités (entre la CNIL et les commissions départementales de vidéosurveillance) apparaît nécessaire. De fait, la loi du 21 janvier 1995 a été adoptée à une époque où la vidéosurveillance s'effectuait essentiellement avec des enregistrements analogiques sur bande magnétique. Elle doit aujourd'hui être revue à l'aune des évolutions technologiques.

En outre, l'existence de deux régimes juridiques différents selon que le système de vidéosurveillance est installé dans un lieu public ou privé apparaît peu claire et compréhensible. L'attribution à la CNIL d'un pouvoir de **contrôle unique** sur les systèmes de vidéosurveillance, quel que soit le lieu d'installation, est une piste intéressante, s'inscrivant dans le cadre d'une refonte des textes légaux relatifs à la vidéosurveillance. Elle ne pourrait néanmoins s'acquitter d'une telle tâche sans une augmentation significative de ses moyens.

Questions à ...

JEAN-MARIE COTTERET

Professeur émérite des universités
Commissaire en charge du secteur « Intérieur, défense »

Quel est votre regard sur le développement de la vidéosurveillance dans notre société ?

La question de la vidéosurveillance est symptomatique du problème d'ensemble auquel sont confrontées les autorités de protection des données. Le développement des dispositifs de vidéosurveillance vise à la fois à répondre aux exigences de sécurité collective de nos concitoyens – ne parle-t-on pas aussi de « vidéoprotection » (terme utilisé par Michèle Alliot-Marie lors de son audition à la CNIL en novembre 2007) – et s'explique par un fort développement des technologies disponibles. Mais il ne doit pas conduire à une surveillance généralisée qui pourrait être privative de libertés.

Les récentes annonces gouvernementales (installation de près de 90 000 caméras dans des lieux publics, projet d'interconnexion des images des réseaux de vidéosurveillance de la RATP, de la SNCF, mais aussi de lieux de cultes, de certaines entreprises et grands magasins) ont renforcé la nécessité d'une réflexion sur les moyens accordés aux organismes de contrôle de ces dispositifs.

Sur le plan technologique, la « vidéosurveillance IP », permettant la transmission et la consultation à distance des images *via* internet ou un terminal mobile est désormais de plus en plus courante. De même, les logiciels « d'analyse intelligente » des images (visant à permettre la détection de « comportements suspects » ou d'objets abandonnés, le décompte du nombre de passants, le suivi de personnes dans une foule, etc.) sont une réalité.

Quel rôle précis la CNIL peut-elle jouer dans le cadre de ce développement ?

Si notre société a peut-être à en espérer une amélioration du niveau de sécurité collective, il faut, pour en assurer la légitimité, garantir également les libertés. Plusieurs conditions sont nécessaires à cette fin. Tout d'abord il faut définir clairement l'objectif poursuivi, ainsi que les moyens mis en œuvre pour l'atteindre. Il s'agit aussi de faire en sorte que notre Commission soit dotée des moyens nécessaires de contrôle afin de garantir le droit des personnes. Enfin, il faut veiller à ce qu'un dispositif d'évaluation soit mis en place afin d'établir un bilan objectif après une période de développement du processus. C'est sous réserve du respect de ces conditions que nos concitoyens pourront à la fois adhérer aux mesures visant à renforcer le niveau de sécurité collective et voir respecté leur droit fondamental à la protection de leurs données personnelles.

Qu'est-ce que c'est ?

LA RECONNAISSANCE FACIALE

En s'appuyant sur une base de photographies préenregistrées reliée à un système de vidéosurveillance et à un dispositif de reconnaissance automatique des visages, il est désormais techniquement possible d'identifier un individu dans une foule. Si cette technologie n'en est qu'à ses balbutiements, il importe de comprendre que son caractère intrusif est croissant puisque la liberté d'aller et venir anonymement pourrait être remise en cause.

L'INVASION DES PUCES !

Comment sont-elles utilisées ?

Les puces sans contact envahissent peu à peu notre quotidien. Elles utilisent plusieurs technologies comme RFID ou NFC.

Aujourd'hui, elles sont déjà présentes dans les titres de transports (passe Navigo ou carte Vélib'), les passeports électroniques, les badges d'accès aux immeubles (Vigik), les porte-monnaie électroniques, les clés de contact des voitures, la logistique pour la gestion des bagages dans les aéroports ou les stocks dans les magasins.

La technologie de radio-identification (RFID) devient ainsi un enjeu économique majeur, notamment dans les applications de la distribution et du transport.

Mais l'avenir promet des applications encore plus diversifiées. Les puces permettront sans doute de connaître instantanément le contenu d'un caddie au supermarché. Elles pourront analyser les objets achetés ; les produits de luxe seront « tagués » pour éviter les contrefaçons ; les paiements seront sans contact quand des lecteurs NFC équiperont les téléphones. Les médicaments et poches de sang seront « tagués » pour assurer ainsi une meilleure traçabilité.

Dans certaines maternités, des expérimentations sont par ailleurs en cours pour équiper les nouveau-nés de bracelets RFID, afin d'éviter les kidnappings. En Espagne, des puces RFID sont injectées sous la peau pour servir de moyen de paiement dans certaines discothèques, ce qui apparaît tout à fait disproportionné.

Quels enjeux informatique et libertés ?

Cette technologie soulève de nouvelles problématiques en matière de protection des données personnelles au premier rang desquelles figure leur (quasi) invisibilité. Comment garantir le respect de la loi en présence de technologies invisibles ?

En outre, n'importe qui, dès lors qu'il est muni du lecteur adéquat, peut lire le contenu d'une puce RFID. Et une puce peut comporter des données personnelles (ou qui peuvent devenir personnelles par interconnexion à une base) permettant ainsi d'identifier à distance son porteur. Si tous ces objets journaliers (carte de transport, vêtement, téléphone, voiture, bracelet…) sont ainsi « tagués », il sera possible de **pister les individus** dans tous les actes de la vie quotidienne.

Certes, aujourd'hui, les systèmes RFID ne permettent pas une surveillance continue des individus. Par exemple, l'utilisation d'un passe Navigo permet seulement de connaître la station de métro où est entré un usager et éventuellement celle où il est sorti. Il n'est pas possible de connaître le trajet effectué, d'autant que la CNIL a limité la durée de conservation de ces données à deux jours, et uniquement à des fins de détection de la fraude.

Qu'en sera-t-il demain ? En théorie, une surveillance plus précise des individus serait possible, mais elle nécessiterait des moyens considérables, à savoir un maillage de lecteurs pouvant lire à plusieurs mètres les puces portées par les personnes.

Qu'est-ce que c'est ?

RFID (*Radio Frequency Identification*)

Les puces RFID permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micropuce (également dénommée étiquette ou *tag*) et d'une antenne qui dialoguent par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. Pour les applications dans la grande distribution, leur coût est d'environ 5 centimes d'euros.

D'autres puces communicantes, plus intelligentes ou plus petites, ont fait leur apparition avec l'avènement de l'internet des objets. Certains prototypes sont quasi invisibles (0,15 millimètre de côté et 7,5 micromètres d'épaisseur) alors que d'autres, d'une taille de 2 mm², possèdent une capacité de stockage de 512 kilooctets et échangent des données à 10 mégabits par seconde.

NFC (*Near Field Communications*)

C'est un standard de communication développé depuis 2002 qui permet à différents types de puces de communiquer et interopérer. Les distances de communication pour un débit maximal de 424 kbps sont de 10 cm.

Quelles solutions pour concilier RFID et vie privée ?

Dans les transports, il est essentiel que des systèmes permettant de continuer à voyager anonymement continuent d'exister.

Dans la grande distribution, les puces équipant les produits vendus en supermarché devraient pouvoir être neutralisées automatiquement lors du passage en caisse (par déactivation ou retrait physique). Des dispositifs techniques garantissant la neutralisation des RFID devraient donc être incorporés dès leur fabrication, quand la puce n'a pas d'application prévue au-delà du point de vente. Des solutions existent déjà mais la recherche doit encore progresser pour trouver des moyens pratiques de mise en œuvre.

La CNIL collabore dans cet esprit avec le pôle Industries du commerce de la région Nord afin d'accompagner le déploiement des technologies RFID.

Par ailleurs, une information claire et précise des consommateurs sur l'usage de ces puces, sur les traitements effectués ainsi que sur les moyens mis à leur disposition pour lire le contenu de la puce et vérifier si elle est ou non active devrait être disponible.

Enfin, des normes de sécurité doivent être promues pour garantir que les informations personnelles éventuellement contenues dans les puces ne puissent être lues à distance par des tiers à l'insu des personnes.

Du fait de leur dissémination massive, de la nature individuelle des identifiants de chacun des objets marqués, de leur caractère invisible et des risques de profilage des individus, la CNIL suit avec une **vigilance toute particulière** le développement de ces nouvelles technologies. En contact régulier avec les acteurs industriels du domaine, au niveau national et européen, elle participe actuellement à l'élaboration d'une première recommandation européenne qui devrait être adoptée au premier semestre 2008. Il s'agit de rappeler que le développement de ces technologies doit nécessairement s'accompagner d'une prise en compte des principes clés de la protection des données : finalité, proportionnalité, transparence et sécurité.

Faut-il encadrer précisément l'usage de ces technologies ? Dès lors que les dispositifs RFID utilisés donnent lieu à l'identification directe ou indirecte d'une personne physique, la loi informatique et libertés s'applique. De ce point de vue, il n'apparaît pas nécessaire d'adopter une législation particulière, mais peut-être faut-il adapter la loi informatique et libertés pour prendre en compte spécifiquement cette technologie. Il appartiendra au groupe de travail constitué au sein de la CNIL pour évaluer l'application de la loi et proposer le cas échéant une révision de celle-ci, d'apprécier si un ajout est nécessaire sur ce point (*cf.* p. 75).

LA CNIL EN ACTION

Questions à ...

YANN PADOVA

Secrétaire général de la CNIL

Pourquoi avoir souhaité une modification de l'organisation interne de la CNIL ?

La modification de la loi informatique et libertés de 2004 implique un changement profond des méthodes de la CNIL, tout en réaffirmant ses principes. Désormais, l'accent est mis sur la pédagogie, le conseil mais aussi sur un contrôle renforcé des fichiers les plus sensibles pour les libertés puisque la loi prévoit désormais que la CNIL doit les autoriser préalablement et expressément. C'est le cas notamment, pour les dispositifs faisant appel à la biométrie ou encore ceux susceptibles d'exclure une personne de l'accès à un bien ou à un service, que l'on qualifie parfois de « listes noires ». En outre, la loi de 2004 confère désormais à la CNIL le pouvoir de mener des contrôles sur place et sur pièces, dans les horaires des perquisitions judiciaires. À l'issue de ces contrôles, notre Commission peut prononcer des sanctions, notamment financières, ce qui est nouveau et l'apparente à une juridiction.

Afin de mieux répondre à ces nouvelles missions, le président Alex Türk et moi-même avons souhaité modifier l'organisation interne de la CNIL. Le 1er juillet 2007, deux nouvelles directions ont été créées pour répondre plus efficacement aux demandes des usagers et des professionnels.

Quels sont les deux axes principaux de cette nouvelle organisation ?

Une capacité d'analyse juridique et technique renforcée d'une part, une plus grande ouverture vers les usagers et une meilleure application de la loi d'autre part.

En pratique, la Direction des affaires juridiques, internationales et de l'expertise, au-delà de l'analyse juridique des questions informatique et libertés, intègre un service de l'expertise informatique renforcé répondant aux nombreux besoins d'évaluation technique mais également de prospective technologique. La dimension internationale, au cœur de nombreuses problématiques tant normatives que technologiques, et dont les implications au niveau national sont nombreuses et parfois immédiates, explique le rattachement de ce service à cette direction.

La Direction des relations avec les usagers et du contrôle a pour vocation de mieux accueillir et d'aider les citoyens qui sollicitent l'aide de la CNIL pour la défense de leurs droits. C'est pourquoi, le service en charge de l'accueil et du renseignement téléphonique, mais aussi celui dédié au développement des correspondants informatique et libertés, se trouvent dans cette direction. Cette nouvelle direction regroupe également les services des plaintes, du contrôle et des sanctions et s'attache, ainsi, à conforter les droits des personnes en contrôlant et sanctionnant, si besoin, les organismes qui ne respecteraient pas ces droits.

Ces deux directions travaillent en parfaite synergie, au bénéfice d'un meilleur service pour les professionnels et les usagers.

PROTÉGER

Un nombre record de plaintes reçues en 2007

En 2007, la CNIL a reçu **4455 plaintes** pour non-respect de la loi informatique et libertés, soit une augmentation de 25 % par rapport à 2006. La CNIL reçoit aujourd'hui deux fois plus de plaintes qu'il y a dix ans !

Cette évolution montre que les « citoyens-consommateurs » sont de plus en plus conscients de leurs droits informatique et libertés, et de plus en plus soucieux de les voir respectés.

La CNIL est là pour les y aider. L'intervention du service des plaintes auprès des responsables de fichiers permet de trouver une issue favorable à beaucoup de situations. Ainsi, découle d'une plainte près de la moitié des contrôles réalisés par la CNIL et des mises en demeure adressées aux responsables de fichiers par la formation contentieuse de la CNIL.

Les secteurs les plus concernés en 2007 sont : banque-crédit, prospection commerciale, travail, télécommunications. Cinq cas concrets permettent d'illustrer les difficultés rencontrées par des particuliers et l'action régulatrice de la CNIL.

Alex Türk et Dominique Roux signant la convention de partenariat

Qu'est-ce que c'est ?

SIGNAL SPAM

La plate-forme nationale www.signal-spam.fr est lancée depuis mai 2007. Elle permet aux internautes de signaler en un clic leurs courriers indésirables. Cette initiative est issue d'une concertation entre pouvoirs publics et professionnels de l'internet, à laquelle la CNIL a été associée. Depuis l'inauguration de ce service, des dizaines de milliers d'internautes se sont inscrits et des millions de messages indésirables ont été ainsi transmis à Signal Spam. L'objectif de Signal Spam est de recueillir et traiter les plaintes des internautes, puis de les rediriger vers les acteurs de la lutte contre le spam en fonction des missions et compétences de chacun, qu'il s'agisse des pouvoirs publics ou des professionnels de l'internet.

La CNIL et Signal Spam, partenaires dans la lutte contre le spam

La convention de partenariat signée le 30 octobre 2007 entre la CNIL et l'association Signal Spam définit les modalités de coopération entre les deux institutions et prévoit notamment :
– la transmission régulière à la CNIL de données statistiques sur les signalements reçus ;
– la possibilité pour Signal Spam de saisir la CNIL d'une plainte contre un « spammeur » identifié afin qu'elle puisse mettre en œuvre ses pouvoirs de contrôle et de sanction ;
– la réalisation d'actions concertées en France ou au niveau international (actions de communication, définition de recommandations pour mieux lutter contre le spam) ;
– la désignation de correspondants au sein des deux organismes partenaires et le principe de rencontres régulières pour garantir l'efficacité du partenariat.

Ça la fiche mal

Interdit à tort de carte bancaire pendant deux ans

▶ À la suite du retrait de sa carte bancaire et d'une inscription au Fichier central des chèques (FCC), Monsieur D. ne peut plus avoir de carte bancaire ni ouvrir de compte dans une autre banque. Il conteste le bien-fondé de cette inscription. N'obtenant pas de réponse de sa banque, il adresse une plainte à la CNIL plus d'un an et demi après avoir été inscrit au FCC. La banque confirme rapidement que cette inscription est infondée et qu'elle procède à sa radiation auprès de la Banque de France. Plusieurs mois après, Monsieur D. informe la CNIL qu'il est toujours inscrit dans le FCC. Quelques jours plus tard, son inscription est automatiquement supprimée par la Banque de France, à l'expiration du délai maximum d'inscription de deux ans. Mise en demeure de s'expliquer sur cette situation par la CNIL, la banque indique que le défaut de suppression de l'inscription résulte d'une erreur dans la demande adressée à la Banque de France qui n'a ainsi pas pu prendre la demande de suppression. La banque précise les mesures qu'elle prend en interne afin que les demandes adressées à la Banque de France soient désormais réalisées correctement. Grâce à l'action de la CNIL, d'autres clients de cette banque ne devraient pas connaître à leur tour les difficultés rencontrées par Monsieur D. dans sa vie quotidienne.

Publicité non désirée : l'arroseur arrosé !

▶ Madame C. reçoit chez elle, sur son télécopieur, une publicité pour une société spécialisée dans la vente de vêtements qui mentionne être « en conformité avec la loi CNIL ». Ne désirant plus recevoir cette publicité, elle manifeste son opposition en adressant une télécopie au numéro indiqué. Malgré ses démarches, elle continue à recevoir en nombre cette même publicité. Elle décide alors d'alerter la CNIL. Sur la base de plusieurs dizaines d'autres plaintes contre cette même société de vente, la CNIL la met en demeure de respecter le droit d'opposition de Madame C. et des autres plaignants, et de se conformer à l'ensemble de ses obligations informatique et libertés. Même si les envois de télécopies publicitaires cessent, la CNIL constate que la société ne se conforme pas, dans le délai fixé, à toutes ses demandes. En conséquence, elle lui inflige une sanction pécuniaire de 5 000 euros. Du fait des manquements constatés, cette sanction s'accompagne d'une mesure de publicité sur le site internet de la CNIL.

Privée de téléphone mobile à cause d'un homonyme

▶ Mademoiselle B. demande l'ouverture d'une ligne de téléphonie mobile dans un point de vente. Un refus lui est opposé au motif qu'elle est inscrite dans le fichier Préventel, qui recense les impayés de la téléphonie mobile et interdit tout nouvel abonnement à défaut de remboursement des sommes dues. N'ayant jamais été cliente d'un opérateur de téléphonie mobile, elle interroge l'organisme responsable de ce fichier et apprend que figure dans Préventel « un homonyme exact au lieu de naissance près » (nom, prénom, date de naissance). Mademoiselle B. produit auprès de l'opérateur des justificatifs prouvant sa bonne foi, mais le point de vente persiste à considérer qu'elle pourrait être la débitrice défaillante inscrite dans le fichier Préventel. Face à ce nouveau refus injustifié, elle saisit la CNIL, qui demande alors au responsable du fichier Préventel de lui préciser le département de naissance et l'adresse postale de l'homonyme de Mademoiselle B. Ces données sont effectivement totalement différentes de celles de Mademoiselle B. La CNIL communique ces informations au correspondant informatique et libertés de l'opérateur responsable du point de vente, lui demandant de réexaminer la demande d'abonnement de Mademoiselle B. Un mois plus tard, l'opérateur reconnaît la bonne foi de Mademoiselle B et précise qu'une offre d'abonnement, assortie d'un geste commercial en guise de dédommagement, lui a été proposée.

Mal fichée et mal logée

▶ Madame M., en attente d'un logement social, souhaite compléter son dossier de demande de logement en informant de la naissance de son fils. Elle découvre que son dossier informatique fait état de deux précédents refus de sa part de propositions de logement social. Or, le premier refus était lié à une localisation inadaptée du logement proposé, et le second était imputable au bailleur social qui avait retiré sa proposition. Ces mentions sont d'autant plus préjudiciables à Madame M. qu'existe, dans son département, un fichier commun de la demande locative accessible aux différents bailleurs sociaux. Depuis ses deux « refus », plus aucun logement ne lui est proposé. La CNIL interroge les bailleurs à l'origine des différentes inscriptions. Elle leur demande de mentionner dans le dossier, d'une part, l'arrivée d'un enfant au foyer de Madame M. et, d'autre part, de clarifier les motifs du second « refus », non imputable à Madame M. Les organismes concernés donnent rapidement une suite favorable. Grâce à l'intervention de la CNIL, Madame M. peut à nouveau se voir proposer des logements adaptés à sa situation.

La boîte à signalement

Environ une vingtaine de messages par jour parvient à la CNIL à partir de la boîte à signalement disponible sur son site internet. Ce dispositif permet à toute personne qui le souhaite de témoigner d'un problème rencontré et d'alerter la CNIL. Ces témoignages ne sont pas des plaintes, mais permettent à la CNIL de se saisir d'un problème ou d'identifier de nouveaux sujets relatifs à la vie quotidienne susceptibles de poser des difficultés au regard de la protection des données. Ils déclenchent parfois une mission de contrôle sur place auprès de l'organisme mis en cause. Ils permettent enfin à la CNIL d'affiner son information en la ciblant davantage et en l'adaptant aux préoccupations des citoyens.

Ces signalements portent dans leur grande majorité sur les secteurs du marketing (personnes qui reçoivent des spams ou de la publicité non sollicitée), des télécommunications (questions liées à l'utilisation de la téléphonie mobile ou d'internet), de la banque ou du crédit (problèmes liés à des inscriptions dans des fichiers d'incidents de paiement) et de l'emploi (questions portant sur les relations entre salariés et employeurs lorsqu'elles impliquent l'usage de fichiers informatiques : géolocalisation, vidéosurveillance, dispositifs de contrôle d'accès ou de contrôle des horaires, etc.).

Comment ça marche ?

En application de l'article 41 de la loi informatique et libertés, toute personne peut demander à la CNIL de vérifier les renseignements pouvant la concerner dans les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique. Les vérifications sont effectuées par les membres de la Commission, magistrats du Conseil d'État, de la Cour de cassation ou de la Cour des comptes.

Principaux fichiers concernés par cette procédure :
– les fichiers des Renseignements généraux pour une candidature, ou par simple curiosité ;
– les fichiers de police judiciaire – STIC et JUDEX – par exemple dans le cas de refus d'agrément ;
– le système d'information Schengen dans le cas de refus de visa.

Le droit d'accès indirect

En 2007, la CNIL a reçu **2 660 demandes** de droit d'accès indirect, soit une augmentation de 67 % par rapport à l'année 2006. Cette croissance s'est nettement accélérée suite à la médiatisation en février 2007 de la demande d'accès aux fichiers des Renseignements généraux présentée par Bruno Rebelle, membre du comité de campagne de Ségolène Royal.

Ces demandes concernent en règle générale plusieurs fichiers et nécessitent en conséquence de nombreuses vérifications. Par exemple, pour les fichiers de police judiciaire, les magistrats de la CNIL effectuent des vérifications dans le Système de traitement des infractions constatées (STIC), dans les fichiers de la sécurité publique des commissariats de police, dans le système judiciaire de documentation et d'exploitation (JUDEX) de la gendarmerie nationale.

Les magistrats de la CNIL en charge du droit d'accès indirect ont procédé en 2007 à **92 missions d'investigation** : 72 au ministère de l'Intérieur, 20 au ministère de la Défense. Ainsi, la CNIL a clôturé **2 350 demandes** (soit 71 % de plus qu'en 2006). Toutefois, le stock de demandes de DAI à traiter reste important. Après la demande de Bruno Rebelle, qui a fait l'objet de nombreux articles et reportages télé, plus de 500 personnes ont demandé l'accès à leur dossier des Renseignements généraux. 90 % d'entre elles étaient inconnues ; le traitement de leur demande a donc pu être très rapide et a été effectué dans le courant de l'année civile. Tel n'est pas le cas pour les personnes connues des services des Renseignements généraux et pour lesquelles il convient de procéder à des recherches à la fois dans le fichier informatique d'indexation détenu par la Direction centrale des renseignements généraux (DCRG), dans les dossiers, individuels ou collectifs, conservés par les sections spécialisées de la DCRG, et dans les dossiers individuels détenus par les directions régionales et départementales des renseignements généraux.

Les demandes clôturées en 2007 concernent pour une large part des saisines reçues au cours des années 2002 à 2006 et 25 % seulement datent de 2007. L'instruction de ces demandes a nécessité **5 000 vérifications** de dossiers.

Au 1er janvier 2008, 2 813 saisines sont en cours (arrivées entre 2002 et 2007) dont 1 714 (soit 61 %) datant de 2007, 658 de 2006 (soit 23 %).

Bilan des 5000 vérifications effectuées au titre du droit d'accès indirect pour les 2350 demandes clôturées en 2007

	Nombre de vérifications	% sur le nombre total de vérifications
MINISTÈRE DE L'INTÉRIEUR	**3761**	**75**
Renseignements Généraux	*912*	*18*
Police Judiciaire – STIC	*1259*	*25*
Sécurité publique – commissariats	*1180*	*23*
Direction de la surveillance du territoire et Direction centrale de la sécurité du CEA	*61*	*2*
Système d'information Schengen	*349*	*7*
MINISTÈRE DE LA DÉFENSE	**1239**	**25**
Gendarmerie nationale (JUDEX)	*1199*	*24*
Direction de la protection de la sécurité de la défense (DPSD)	*20*	*0,5*
Direction générale de la sécurité extérieure (DGSE)	*20*	*0,5*
TOTAL	**5000**	**100**

Les fichiers des Renseignements généraux

Bilan des 912 vérifications effectuées dans les fichiers des Renseignements généraux pour les demandes clôturées en 2007

	Nombre de vérifications	% sur le nombre total de demandes aux RG
Requérants non fichés aux RG	**748**	82
Requérants fichés aux RG	**164**	18
Dossier non communicable	*8*	*1*
Dossier partiellement communicable	*7*	*1*
Dossier totalement communicable	*149*	*16*

Sur les 156 communications totales ou partielles, 61 (soit 39 %) ont eu lieu dans les locaux de la CNIL, et 88 (soit 61 %) à la préfecture du lieu de domicile du requérant. Comme les années précédentes, le ministre de l'Intérieur n'a refusé aucune des propositions de communication de dossier faites par les membres de la CNIL.

À la suite de ces communications, neuf requérants ont rédigé une note d'observation qui a été insérée dans le dossier des Renseignements généraux les concernant. Par ailleurs, il a été procédé à la suppression totale ou partielle de 19 dossiers.

Les fichiers de police judiciaire – STIC et JUDEX

Bilan des 2458 vérifications effectuées dans les fichiers STIC et JUDEX pour les demandes clôturées en 2007

	Nombre de vérifications	% sur le nombre total de demandes aux fichiers de PJ
Requérants non fichés en tant que mis en cause par le STIC ou le JUDEX	**1430**	58
Requérants fichés en tant que mis en cause par le STIC ou le JUDEX	**1028**	42
Enregistrement exact	*460*	*45*
Modification ou suppression de l'enregistrement à la suite d'une anomalie dont le gestionnaire du fichier (police ou gendarmerie) est à l'origine	*242*	*24*
Modification ou suppression de l'enregistrement à la suite d'une anomalie provenant des parquets	*326*	*31*

Chacun des articles 7 des décrets STIC (14 octobre 2006) et JUDEX (20 novembre 2006) fixe les durées de conservation des informations en fonction de la gravité des faits commis et de leur qualification enregistrée dans les fichiers de police judiciaire.

Au cours des vérifications opérées par les magistrats de la CNIL, il peut y avoir :
– une **requalification** des faits : la qualification des faits initialement retenue par les services de police peut être redéfinie par l'autorité judiciaire et se substituer à la qualification initialement enregistrée dans le fichier ;
– une **mise à jour ou une suppression** en raison de suites judiciaires favorables à l'intéressé : si une personne a bénéficié d'une mesure de classement sans suite pour insuffisance de charges, d'une décision de non-lieu, de relaxe ou d'acquittement devenue définitive, le fichier est mis à jour compte tenu des suites judiciaires favorables. Il convient de préciser que le procureur de la République peut, pour des raisons tenant à la finalité du fichier, prescrire le maintien des données personnelles enregistrées.

Les délais de traitement des investigations dans les fichiers de police judiciaire sont très longs pour les personnes enregistrées en tant que mises en cause car les services de police judiciaire centralisent aux sièges des directions des ministères concernés les dossiers de procédure conservés par les unités départementales et régionales.

Ensuite, ces services saisissent les procureurs de la République des tribunaux compétents pour connaître les suites judiciaires des affaires enregistrées dans le STIC ou dans JUDEX, et recueillir leur accord de communication en cas de maintien du signalement.

Les statistiques indiquées ci-dessus peuvent présenter des différences avec celles produites par les ministères de l'Intérieur et de la Défense, dans la mesure où la CNIL n'a pas la même définition de la notion de « saisine clôturée ». En effet, pour la CNIL, la saisine (ou demande) n'est considérée comme clôturée que lorsque l'intéressé a été rendu destinataire de la lettre de notification du président de la CNIL lui indiquant les résultats des vérifications opérées et, le cas échéant, lui communiquant sa fiche après accord du ministère de l'Intérieur ou de la Défense, et du parquet.

Le système d'information Schengen (SIS)

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 4058 demandes de droit d'accès dont 371 pour les saisines clôturées en 2007.

Sur les 371 requêtes traitées en 2007, 37 % d'entre elles (139 personnes) concernaient des personnes signalées, dont :
– 74 signalements français, soit 53 % ;
– 40 signalements italiens, soit 29 % ;
– 10 signalements allemands, soit 7 %.

Les 11 % restants concernent des signalements espagnols, néerlandais, grecs, norvégiens…

Qu'est-ce que c'est ?

LE SYSTÈME D'INFORMATION SCHENGEN (SIS)

Il est composé d'une base centrale située à Strasbourg et, dans chaque pays participant à l'espace Schengen, de bases nationales. Les informations concernent essentiellement des personnes :
– recherchées pour arrestation aux fins d'extradition ;
– étrangères, signalées aux fins de non-admission dans l'espace Schengen suite à une décision administrative ou judiciaire ;
– signalées aux fins de surveillance discrète ou de contrôle spécifique.

Ça la fiche mal

L'IMPOSSIBILITÉ DE PRÉSENTER UN CONCOURS OU D'ACCÉDER À UN EMPLOI

L'enregistrement d'un témoin en tant que mis en cause

▶ **Mademoiselle C., souhaitant présenter un concours d'entrée à une école de police, était enregistrée dans le STIC en tant que mise en cause, alors qu'elle avait été uniquement entendue en tant que témoin dans une affaire de trafic de produits anabolisants par la sûreté départementale compétente. À l'issue du contrôle de la CNIL, les informations la concernant ont été supprimées du STIC, et cette personne a pu, de nouveau, présenter le concours qu'elle souhaitait.**

La mise à jour du STIC sur le fondement de classement sans suite pour insuffisance de charges

▶ **Mademoiselle L., a dû interrompre une formation pour devenir hôtesse de l'air lorsqu'elle s'est vue refuser son badge d'accès à la zone aéroportuaire. Cette personne était en effet enregistrée dans le STIC en tant que mise en cause dans une affaire de falsification et d'usage frauduleux de chèque. À l'issue des investigations menées par la CNIL, ayant été totalement mise hors de cause, les informations ont été supprimées du STIC en raison du classement sans suite de la procédure pour insuffisance de charges. Cette personne a donc été en mesure de poursuivre sa formation.**

La suppression des données enregistrées dans le STIC en raison de l'absence d'archives de procédure

▶ **Monsieur E. postulait pour un emploi d'agent de sécurité mais avait été mis en cause dans des procédures de vol datant de 1998. Informé par la préfecture de cette situation, son employeur n'a pu le recruter. À la suite de l'intervention de la CNIL, il a été radié du STIC en raison de l'absence d'archives dans les services de police. En conséquence, la préfecture du département de son lieu de résidence a été informée de la suppression de ces données afin qu'elle puisse reconsidérer sa demande d'agrément pour exercer la profession d'agent de sécurité.**

L'IMPOSSIBILITÉ DE CRÉER SON ENTREPRISE

L'expiration du délai de conservation

▶ **Monsieur D. souhaitait créer une société de surveillance et de gardiennage privés. Or, il a fait l'objet d'un refus d'agrément de la part du préfet territorialement compétent au motif qu'il était fiché dans le STIC en tant que mis en cause. À l'issue du contrôle de la CNIL, les informations enregistrées dans le STIC concernant le requérant ont été supprimées, la durée de conservation des données étant dans le cas d'espèce expirée, ce qui lui a enfin permis de créer son entreprise. En effet, les données n'avaient pas été supprimées par le logiciel d'épurement en raison de l'absence de précision du nombre de jours d'interruption temporaire de travail, qui a une conséquence directe sur la durée de conservation des informations dans le STIC.**

LE RISQUE DE PERTE D'UN EMPLOI

L'enregistrement d'informations infondées dans le STIC

▶ **Monsieur B. occupait un emploi dans une société de sécurité. À l'occasion de l'instruction de sa demande de renouvellement d'habilitation pour accéder aux zones réservées aéroportuaires, au cours de laquelle les fichiers de police judiciaire peuvent être consultés, il s'est avéré qu'il était fiché dans le STIC en tant que mis en cause, ce qui était susceptible de conduire le préfet territorialement compétent à refuser cette habilitation et, de fait, à lui faire perdre son emploi. Au terme des investigations menées par la CNIL, il est apparu que Monsieur B. était enregistré dans le STIC à tort, puisque les faits de violence volontaire retenus à son encontre n'ayant pas entraîné d'interruption temporaire de travail, il n'était passible que d'une contravention de 4e classe. En conséquence, Monsieur B. a conservé son emploi.**

La mise à jour du STIC sur le fondement de classement sans suite pour infraction insuffisamment caractérisée

▶ **Dans ce cas également, Monsieur P. occupait un emploi dans une société de sécurité. Sa demande d'habilitation pour travailler sur des sites aéroportuaires a fait l'objet d'un refus de la part du préfet en raison de son inscription dans le STIC. À l'issue des investigations menées par la CNIL, les informations concernant Monsieur P. ont été supprimées du STIC au motif que l'infraction était insuffisamment caractérisée. En conséquence, la situation professionnelle de Monsieur P. a pu être réexaminée.**

INFORMER, CONSEILLER

Informer au quotidien

Partenariat France Info

Depuis le mois d'octobre 2007, France Info propose, en partenariat avec la CNIL, un rendez-vous hebdomadaire informatique et libertés dans l'émission « Le droit d'info » présentée par Karine Duchochois. Ainsi, chaque mercredi, une chronique répond à une question très pratique, touchant souvent à la vie quotidienne, permettant d'aborder de façon pragmatique les droits à la protection des données personnelles qui sont encore trop méconnus et de faire connaître les actions de la CNIL dans la défense de ces droits.

Le tour de France des régions et les interventions de la CNIL

La CNIL continue son tour de France des régions. Trois régions ont été visitées en 2007 : Languedoc-Roussillon, Picardie et Pays de la Loire, ce qui porte leur nombre total à 14. Initiée en janvier 2005, cette nouvelle démarche d'information et de communication de proximité a permis de rencontrer environ 7 000 personnes : entreprises, administrations, collectivités locales, élus, associations, journalistes, citoyens, avocats, professionnels de la santé et de l'éducation, acteurs sociaux, etc.

En 2007, les agents ou membres de la CNIL ont participé à **155 colloques, séminaires, conférences ou animations de formations** sur la loi informatique et libertés ou la fonction de correspondant informatique et libertés auprès d'entreprises, d'administrations, de collectivités locales, d'organisations professionnelles, d'universités, etc.

Le site cnil.fr

Le site de la CNIL a connu un accroissement important de son nombre de visiteurs : dans l'année, le nombre de visiteurs est passé de 1 320 000 à 1 850 000, soit une moyenne de 5 000 internautes par jour.

Le volume d'informations publiées depuis quatre ans (1 700 pages html) et la diversité des thèmes abordés incitent l'internaute à utiliser fréquemment le moteur de recherches. De fait, la page des résultats de la recherche est la plus fréquentée après la page d'accueil.

Les cinq mots clés les plus recherchés sont :
- spam ;
- vidéosurveillance ;
- CNIL ;
- missions ;
- biométrie.

Ces résultats corroborent en partie la répartition moyenne de l'audience des dossiers thématiques. En 2007, les six dossiers les plus consultés sont :
- travail (4 500 visites par mois) ;
- internet (3 300) ;
- correspondants (3 000) ;
- santé (2 600) ;
- banque-crédit (2 300) ;
- spam (1 800).

Les internautes plébiscitent les contenus pratiques et pédagogiques traitant de la problématique de la protection des données appliquée à leur vie quotidienne. À ce titre, la rubrique « Vos traces », enrichie des animations réalisées dans le cadre de la Journée européenne de la protection des données, reste la rubrique la plus consultée du site (48 000 visites par mois). Suivent la rubrique consacrée aux questions les plus fréquemment posées (FAQ, 30 000 visites par mois) et les pages qui explicitent les droits informatique et libertés aux citoyens (20 000 visites par mois).

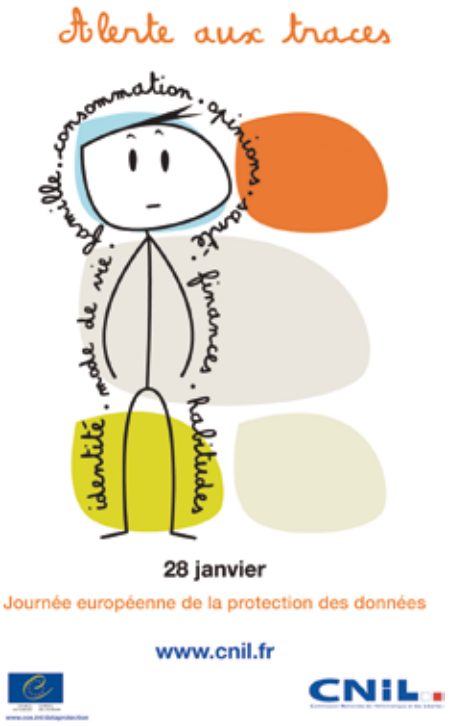
En 2007, la CNIL a amorcé le chantier de la refonte de son site internet. Afin de mieux connaître son public et ses attentes, elle a mis en ligne en novembre 2007 un sondage destiné à recueillir les attentes des internautes. Près de 300 réponses ont été recueillies, le recueil des contributions se poursuit en 2008.

La 1re Journée européenne de la protection des données

Le 28 janvier 2007, le Conseil de l'Europe a célébré la 1re Journée européenne de la protection des données, date anniversaire de l'ouverture à la signature de la Convention 108 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

La CNIL s'est associé à cette journée en proposant sur son site trois animations de sensibilisation intitulées *Alerte aux traces* qui illustrent l'utilisation du GPS, de la télébillétique dans les transports en commun et des moteurs de recherche sur internet. En effet, de nombreux actes de la vie quotidienne (téléphoner, utiliser sa carte bancaire ou surfer sur internet) génèrent des traces porteuses d'informations sur notre identité. L'utilisation anodine de technologies performantes nous conduit naturellement à dévoiler toujours plus d'informations sur nous, sans pour autant savoir qui y aura accès, pour quoi faire et pour combien de temps. Ces informations peuvent être exploitées de plus en plus vite, en plus grand nombre, et sont potentiellement accessibles en tout point du globe. Notre vie privée se réduit ainsi petit à petit avec le risque que ce mouvement soit irréversible.

L'objectif de cette journée, conformément aux missions de la CNIL, est précisément de faire prendre conscience à chacun qu'il est titulaire d'un **droit fondamental à la protection de ses données et de sa vie privée**. La défense de ce droit individuel, aussi important que la liberté de la presse ou la liberté d'aller et venir, appelle une vigilance de tous, à tous les instants.



Les publications

En 2007, la CNIL a édité un guide pratique destiné au grand public intitulé *Banque, crédit : êtes-vous fiché ?* ainsi qu'une plaquette destinée à promouvoir la fonction de correspondant informatique et libertés.

L'image de la CNIL

Comme les années précédentes, une étude portant sur la perception et l'image de la CNIL a été menée en novembre 2007 par TNS SOFRES sur un échantillon de 1 000 personnes représentatives de la population française.

La notoriété de la CNIL

Question :

Connaissez-vous, ne serait-ce que de nom, la CNIL ?

	Juin 2004	Déc. 2005	Déc. 2006	Nov. 2007	Évolution 2006-2007
Oui	32	37	39	50	+ 11
Non	68	63	61	50	– 11
Total	100	100	100	100	

Le niveau d'information sur les droits

Question :

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

Oui, tout à fait	5
Oui, plutôt	21
Sous-total oui	**26**
Non, plutôt pas	35
Non, pas du tout	37
Sous-total non	**72**
Sans opinion	2
Total	100

La perception de l'atteinte à la vie privée

Vous savez que des organismes ont la possibilité de conserver des informations personnelles comme par exemple les coordonnées téléphoniques, le numéro de sécurité sociale, les références bancaires, et de les utiliser dans le cadre d'une réglementation précise.

Question :

Diriez-vous que la constitution de tels fichiers porte atteinte à la vie privée ?

Oui, tout à fait	30
Oui, plutôt	31
Total oui	**61**
Non, plutôt pas	21
Non, pas du tout	15
Total non	**36**
Sans opinion	3
Total	100

L'accroissement très net de la notoriété de la CNIL en 2007 (+ 11 %) s'explique par une exposition médiatique continue. En juillet 2007, la présentation par son président, Alex Türk, du rapport annuel 2006, a été particulièrement médiatisée. En 2007, environ 600 séquences audiovisuelles ont cité la CNIL.

En revanche, en ce qui concerne l'information sur la protection des données personnelles, seulement un Français sur quatre s'estime suffisamment informé. Alors que les personnes interrogées connaissent la CNIL, elles ont du mal à l'associer à la protection de leurs données personnelles, principe qui demeure méconnu de la plupart de nos concitoyens. Afin de mieux faire comprendre quels sont ces droits, la CNIL, au travers de ses publications, de son site internet et de ses interventions médiatiques, s'oriente vers une communication plus pratique (scénarisation de cas concrets, questions/réponses, animations de sensibilisation aux traces).

Cependant, 61 % des personnes interrogées sont conscientes des implications sur leur vie privée de la constitution de fichiers. Elles sont donc, sans vraiment l'énoncer, sensibles à la protection de leurs données personnelles. Pour parvenir à une évolution significative de la connaissance de ces droits, des campagnes d'information grand public devraient être menées. En l'état actuel de ses moyens, de telles initiatives demeurent encore impossibles pour la CNIL.

Informer, conseiller les entreprises

Les pouvoirs de la CNIL à l'égard des entreprises se sont accrus depuis la loi du 6 août 2004. La Commission dispose désormais d'un pouvoir d'autorisation pour les traitements les plus sensibles et peut sanctionner les entreprises qui ne respectent pas la loi.

C'est dire si la mission de conseil et d'information aux entreprises est aujourd'hui fondamentale alors même que les relations entre la CNIL et les entreprises ont longtemps été marquées par l'ignorance et la méfiance.

Faire connaître la loi informatique et libertés demeure un objectif

Ce constat peut sembler paradoxal après bientôt 30 ans d'application de la loi mais si les grandes entreprises ont bien intégré cette problématique, loin s'en faut pour les PME, alors même que les technologies de l'information y ont fait une percée remarquable. La CNIL prend notamment appui sur le réseau des chambres de commerce et d'industrie (CCI) avec lequel elle a signé une convention et qu'elle associe systématiquement aux rencontres régionales qu'elle organise. La Commission a ainsi participé en 2007 à de nombreuses réunions à la demande de la FFSA (Fédération française des sociétés d'assurance), de la FBF (Fédération bancaire française), de l'UDA (Union des annonceurs), du SNCD (Syndicat national de la communication à distance), etc.

La CNIL se rapproche plus systématiquement des sociétés de services informatiques et concepteurs de logiciels pour diffuser les règles applicables et les aider à développer leur technologie en tenant compte de la protection des données personnelles, dans les domaines de la géolocalisation, de la biométrie ou du vote électronique par exemple. La commission a ainsi reçu plus de 450 demandes de conseil émanant d'entreprises en 2007.

Accompagner le développement économique

La CNIL occupe à cet égard un espace privilégié, à la conjonction de l'élaboration des règles juridiques et de la conception des dispositifs techniques sur lesquels elle exerce son contrôle. Les professionnels ont pris conscience de ce rôle charnière de la Commission et n'hésitent plus à venir lui faire part de leurs projets de recherche et développement et de leurs innovations technologiques, ainsi que de leurs interrogations face à l'amoncellement de réglementations dont il convient de décliner concrètement les modalités d'application.

Des contacts ont ainsi été noués avec plusieurs pôles de compétitivité, notamment le pôle « industries du commerce » de la région Nord, le pôle TES de la région Basse-Normandie et le pôle System@tic Paris-Région, afin d'accompagner le déploiement de nouvelles applications RFID, de vidéosurveillance et de gestion d'identité numérique.

Tenir compte de l'évolution de la vie économique et des réalités que sont l'externalisation et la mondialisation

La CNIL est consciente que certaines notions – « responsable de traitement et de sous-traitant » par exemple – sont plus difficiles à appréhender avec le développement du recours à des prestataires offrant clé en mains des services sur lesquels les clients n'ont pas de prise. Les travaux menés par le groupe des CNIL européennes, dit G29, s'avèrent fondamentaux à cet égard, car ils permettent d'avoir une interprétation harmonisée de la directive européenne et d'offrir des réponses plus adaptées aux solutions des multinationales telles que Microsoft, Google ou Hewlett Packard. La mondialisation implique nécessairement de repenser et de développer les relations entre autorités de protection des données et principaux acteurs technologiques afin que la dimension « protection des données » soit prise en compte. Les recommandations, normes simplifiées ou autorisations uniques ne sont adoptées qu'à la suite d'une large concertation menée auprès des entreprises. En 2007, cette pratique a mené à la modification de l'autorisation unique relative à la lutte contre le blanchiment d'argent (AU n° 03).

Les pratiques d'externalisation se développant de plus en plus (1 682 autorisations de transferts de flux transfrontières en 2007), la CNIL a mis en place un groupe de travail sous la présidence de Didier Gasse, chargé de réfléchir à la protection des données dans le cadre de la délocalisation des centres d'appels et de l'externalisation informatique (*cf.* p. 77).

Aider les entreprises à transformer la contrainte légale que représente la loi informatique et libertés en élément de confiance

La CNIL est force de propositions et se tient à l'écoute des besoins exprimés par les entreprises. Cette évolution conduit à s'engager en prenant position pour privilégier les technologies ou les solutions techniques les moins intrusives au regard des droits des personnes. Pour les entreprises, développer et appliquer une véritable politique de protection des données personnelles constitue un avantage concurrentiel décisif en permettant de gagner la confiance des clients et donc une plus grande part de marché.

Cette démarche prendra une ampleur supplémentaire, si la CNIL met en œuvre son pouvoir de labellisation prévu par la loi, mais le décret n'est pas encore paru.

Cette démarche conduit également à nouer des partenariats avec des acteurs privés, comme cela a été le cas en 2007 avec Signal Spam. Par ailleurs, la CNIL poursuit les efforts engagés pour simplifier les formalités par le biais des exonérations de déclaration, de déclaration simplifiée ou unique, d'autorisations uniques (allégement du formulaire de déclaration).

Développer la labellisation

Parmi les priorités de la CNIL, figure la mise en place des procédures de labellisation des produits et procédures tendant à la protection des personnes à l'égard des données à caractère personnel. Pour l'élaboration de ces procédures, qui ne pourront être mises en place que lorsque les décrets d'application seront parus, la CNIL s'appuiera d'une part sur l'expérience acquise dans le projet européen EuroPrise, visant à développer une labellisation européenne, et d'autre part sur une réflexion qu'elle a conduite dès 2005 (en rencontrant notamment certains organismes et administrations ayant déjà développé de telles procédures, tel le COFRAC, la DCSSI ou la DGME) concernant le périmètre et les modalités de mise en œuvre du pouvoir de labellisation.

La politique de labellisation permettra d'agir en amont auprès des entreprises, en fixant un cadre de nature technique à l'attention des éditeurs de logiciel mais aussi des entreprises qui pourraient ainsi disposer de repères quant aux exigences de la CNIL.

Bon à savoir

Depuis la modification de la loi en 2004, la CNIL peut, à la demande notamment des organisations professionnelles, valider des projets de règles professionnelles ainsi que des produits ou procédures tendant à la protection des personnes. La CNIL a d'ores et déjà, dès 2005, reconnu conformes les codes de déontologie des professionnels du marketing direct. D'autres projets de codes sont en cours d'examen, dans le domaine du renseignement commercial et des centres d'appels. La loi lui ayant également conféré un pouvoir de labellisation, la CNIL entend fortement promouvoir, dans l'avenir, les initiatives dès lors qu'elles tendent à la protection des personnes. Elle attend donc avec impatience la parution du décret d'application de la loi en la matière.

La labellisation contribuera également à instaurer une meilleure confiance entre les entreprises et les utilisateurs qui pourront plus aisément identifier et privilégier les produits garantissant un bon niveau de protection de leurs données personnelles.

Informer, conseiller les pouvoirs publics

Chaque année, le président de la CNIL remet son rapport annuel au Président de la République, au Premier ministre et aux présidents des deux Assemblées. Ce temps fort lui permet d'évoquer les principaux sujets de l'année écoulée.

En 2007, la CNIL a décidé de renforcer et de systématiser le dialogue avec le Parlement et les pouvoirs publics. Cette évolution nécessaire correspond à une transformation profonde de ses missions : le développement accéléré des technologies place en effet aujourd'hui la Commission au cœur de problématiques sociétales fortes, comme les titres d'identité biométriques, la mesure de la diversité, les nanotechnologies, la vidéosurveillance, les puces RFID, la géolocalisation, les fichiers de crédit, la délocalisation, la prospection commerciale... C'est pourquoi la Commission a souhaité informer davantage le Parlement sur tous ces sujets, qui posent des enjeux majeurs en matière de protection des données personnelles et de respect de la vie privée.

Informer le Parlement

Les auditions

En 2007, le président de la CNIL a été auditionné par la Commission des lois du Sénat. Il a rencontré les présidents de Commissions Didier Migaud, Jean-Luc Warsmann, Pierre Méhaignerie et Patrick Ollier à l'Assemblée nationale ; Jean-Paul Emorine au Sénat. Il a répondu à des demandes d'auditions émanant de parlementaires, comme le sénateur Claude Saunier, sur le thème des nanotechnologies, et le sénateur Charles Gautier, président du Forum français pour la sécurité urbaine, sur le thème de la vidéosurveillance.

Les services de la Commission ont été auditionnés par : le député Jean-Pierre Door, rapporteur de la mission d'information mise en place par la Commission des affaires sociales, sur le dossier médical personnel ; le député Jean Dionis, du Séjour sur l'application de la loi pour la confiance dans l'économie numérique ; le sénateur Jean Bernard-Reymond, rapporteur sur le projet de décision-cadre relative à la protection des données personnelles traitées dans le cadre de la coopération policière et judiciaire en matière pénale, par les Commissions des lois des deux assemblées, sur la proposition de loi de Jean-Michel Fourgous et Yves Censi visant à permettre la recherche des bénéficiaires des contrats d'assurance-vie non réclamés et en déshérence.

Afin de pérenniser ces relations, la CNIL souhaite organiser des rencontres thématiques avec les parlementaires, sur des sujets d'actualité.

La CNIL, acteur des réformes

La Commission a mis en place de nouvelles méthodes de travail avec le Parlement, de manière à traiter les dossiers davantage en amont et en collaboration avec les parlementaires concernés. Ainsi, au moment de la discussion, en première lecture, à l'Assemblée nationale du projet de loi « Consommation : développement de la concurrence au service des consommateurs » de Luc Châtel à l'automne 2007, le président de la Commission des affaires économiques, Patrick Ollier, a décidé de mettre en place une mission d'information consacrée au surendettement. Il a prévu d'auditionner la CNIL sur les fichiers positifs et de recueillir son expertise pour éclairer les travaux parlementaires.

Des contacts réguliers avec les administrateurs des deux assemblées ainsi qu'avec les attachés parlementaires permettent à la CNIL d'être informée en amont des sujets et facilitent le travail en commun.

Sensibiliser l'exécutif

La CNIL organise des auditions dans ses murs. Michèle Alliot-Marie, ministre de l'Intérieur, de l'Outre-mer et des collectivités locales, a été auditionnée en séance plénière en novembre 2007 et a exposé le programme de travail à venir de son ministère. La dernière venue en audition à la CNIL d'un ministre de l'Intérieur remontait à 1998, lorsque Jean-Jacques Queyranne assurait l'intérim de Jean-Pierre Chevènement. Des auditions devraient avoir lieu en 2008 avec d'autres ministres.

Regards croisés

MICHÈLE TABAROT

Députée des Alpes-Maritimes
Commissaire en charge du secteur «Immigration, intégration»

SÉBASTIEN HUYGHE

Député du Nord
Commissaire en charge du secteur «Affaires sociales»

Deux nouveaux députés, Michèle Tabarot et Sébastien Huyghe, ont été nommés à la CNIL par le président de l'Assemblée nationale, le 6 juillet 2007. La présence de ces parlementaires permet d'établir un lien direct et constant entre la CNIL et l'Assemblée nationale.

Vous êtes arrivée à la CNIL en septembre 2007 : dans quel état d'esprit avez-vous abordé votre fonction de commissaire ?

S. Tabarot : dans un état d'esprit très positif, dans la mesure où cette fonction de commissaire à la CNIL me permet de traiter des sujets nouveaux. En effet, je suis plutôt spécialisée dans les questions d'aménagement du territoire et de développement local. En même temps, ce secteur de l'immigration et de l'intégration revêt une importance particulière au moment où le gouvernement souhaite mettre en œuvre une politique de l'immigration nouvelle et ambitieuse.

Comment articulez-vous votre mandat de député et votre fonction à la CNIL ?

S. Huyghe : j'essaie d'apporter à la Commission mon expérience et mon regard d'élu local. Par ailleurs, je me considère un peu comme un trait d'union entre l'Assemblée et la CNIL : les relations privilégiées que j'entretiens avec les présidents de commissions et les rapporteurs peuvent nous permettre de mieux expliquer et défendre le principe de la protection des données personnelles. Les députés n'ont pas encore une bonne connaissance des compétences et des activités de la Commission, c'est pourquoi il est très important de les informer régulièrement.

Un acteur privilégié : le correspondant informatique et libertés (CIL)

Deux ans après son entrée en vigueur, le CIL est un succès. Ainsi, au 15 décembre 2007, **1 723 organismes** avaient désigné un correspondant. Plusieurs organismes ont opté pour un correspondant mutualisé. En 2007, **plus de 1 050 organismes** ont notifié à la CNIL leur décision de se doter d'un CIL. Ils étaient 650 organismes en 2006 et 73 en 2005.

Qui sont-ils ?

Les CIL sont principalement désignés en interne et la plupart d'entre eux exercent leurs missions en complément de leur fonction principale. Ils sont donc très rarement CIL «à plein temps». Quant à leur profil professionnel, **environ 40 % des CIL sont issus du secteur informatique**. Viennent ensuite les métiers juridiques et d'audit, représentés à 20 %.

Qu'est-ce que c'est ?

LE CIL ET LA LOI

L'article 22 de la loi prévoit qu'en présence d'un «correspondant à la protection des données personnelles», dit correspondant informatique et libertés (CIL), dans l'organisme, celui-ci est dispensé des formalités déclaratives les plus courantes. Ces fichiers sont désormais inscrits dans un registre tenu par le CIL. En revanche, les traitements dits «sensibles», nécessitant une autorisation ou un avis, continuent à être soumis à la CNIL.

Où sont-ils ?

En raisonnant par secteur d'activité, **plus de 80 % des CIL relèvent du secteur privé** et agissent dans les entreprises industrielles, les compagnies d'assurances et les banques. En conséquence, un peu moins de 20 % des correspondants sont présents dans des structures publiques, principalement les organismes de protection sociale, de santé et de retraite, les collectivités locales, les universités, ou encore les services gérant le logement social.

Gros plan sur...

LA CONVENTION DE PARTENARIAT CNIL - CPU

La Conférence des présidents d'université (CPU) et la CNIL ont signé, le 25 janvier 2007, une convention de partenariat pour promouvoir la culture informatique et libertés au sein de la communauté universitaire. Un avenant à cette convention a été conclu le 30 avril 2007 afin de préciser le plan d'action de mise en œuvre de ce partenariat d'enseignement supérieur. La convention poursuit trois objectifs :

– l'assistance de la CNIL à la mise en place des CIL au sein des établissements de l'enseignement supérieur et la création d'un réseau de ces correspondants ;

– la sensibilisation des établissements d'enseignement supérieur à la loi informatique et libertés ;

– un recensement des besoins de formation informatique et libertés dans les cursus d'enseignement supérieur.

La CNIL et la CPU se félicitent du succès de cette convention car, après seulement un an d'existence, environ 20 % des universités se sont dotées d'un CIL. En effet, au 15 décembre 2007, 21 CIL ont pris leurs fonctions au sein des universités. Parmi eux, un CIL exerce ses missions en tant que correspondant mutualisé pour quatre établissements. Ce succès a permis également d'organiser, en commun, une première rencontre annuelle des CIL des universités qui a eu lieu dans les locaux de la CNIL le 5 décembre 2007.

Que font-ils ?

Le rôle principal du CIL est, avant tout, de **veiller à la bonne application de la loi** informatique et libertés, et de s'assurer que les conditions de collecte, d'enregistrement, de communication des données à caractère personnel ne représentent pas un danger pour la vie privée et les libertés des personnes. C'est ce rôle de garant que la loi attribue au correspondant. La confiance qui s'instaure ainsi avec la CNIL se traduit également par **un allégement important des formalités déclaratives**. Cela signifie concrètement que les structures qui optent pour le CIL ne sont plus tenues d'adresser leurs déclarations à la CNIL car c'est désormais le correspondant qui recense ces fichiers.

« Nous sommes conscients des avantages de la technologie mais aussi de son impact sur les libertés des personnes. Nous souhaitons trouver le bon équilibre dans nos procédures internes. »

Laure B., directeur informatique, finance

« Avant d'opter pour cette solution, nous étions toujours dans le doute : Notre projet est-il légal ? Faut-il déclarer ou pas ? Comment ? Qui va le faire ? Qu'en dit la CNIL ? Avec le CIL, tout est plus facile. Nos démarches administratives sont simplifiées, le risque juridique est mieux maîtrisé... Et le temps ainsi dégagé est consacré au développement. »

Gaëlle D., directeur juridique, industrie

En outre, l'accent est mis sur le conseil et la pédagogie en amont, ce qui réduit sensiblement le risque juridique mais également le risque économique, c'est-à-dire le surcoût dû, par exemple, au changement et au développement d'une nouvelle application informatique, ou, de façon moins agréable, une sanction pécuniaire.

Les CIL et la CNIL

La CNIL considère les CIL comme ses interlocuteurs privilégiés et leur réserve un accueil prioritaire dans ses missions de conseil et d'information. À cette fin, la **Cellule correspondants**, véritable guichet unique pour les CIL, mise en place dès la création de la fonction CIL par la loi de 2004, est désormais intégrée à la nouvelle Direction des relations avec les usagers et du contrôle de la CNIL. Dans son fonctionnement, elle s'appuie bien évidemment sur l'expertise de l'ensemble des services de la CNIL afin d'assurer une réponse de qualité aux différentes demandes émanant des CIL. Une messagerie électronique et une ligne téléphonique dédiées sont à la disposition de tous les correspondants dont la désignation a été notifiée à la CNIL.

Par ailleurs, la CNIL développe l'accompagnement des CIL à travers les **ateliers d'information** dont le programme varie.

Les CIL en chiffres

- **17 sessions de formation réalisées en 2007 ; 10 en 2006 ;**
- **650 participants.**

Deux types d'ateliers ont été proposés aux CIL : un atelier sur les **« fondamentaux »**, permettant de présenter la CNIL, ses missions et ses services ainsi que de faire le tour d'horizon de grands principes de la protection des données. Il a pour objectif d'aborder toutes les questions essentielles liées à la fonction du CIL, aux formalités le concernant ainsi qu'à sa relation privilégiée avec la CNIL. Parmi les ateliers **« thématiques »**, l'atelier « RH et nouvelles technologies » aborde les sujets tels que la cybersurveillance, la vidéosurveillance ou la géolocalisation. Dans ce contexte, un coup de projecteur est donné sur les problématiques spécifiques de la gestion des ressources humaines et des transferts hors Union européenne. Un atelier spécifique porte sur les « enjeux technologiques » et tout particulièrement ceux liés à la biométrie, avec une analyse détaillée des enjeux de sécurité des données à caractère personnel et des questions liées à leur anonymisation.

En 2007, deux nouveaux ateliers thématiques ont été créés : **« santé/sécurité sociale/recherche médicale »** et **« collectivités locales ».**

Animés par les experts de la CNIL, tous les ateliers se déroulent dans les locaux de la Commission.

Et demain ?

Sans aucun doute, l'augmentation du nombre de CIL se poursuivra. Pour que la mission du CIL soit un succès, celui-ci a besoin d'une **parfaite collaboration du responsable de traitement** qui doit lui fournir les informations, les moyens et les outils nécessaires pour remplir pleinement sa fonction. Une volonté claire et affirmée de la direction pour l'adhésion de l'ensemble des services à ce projet apparaît essentielle.

CONTRÔLER, SANCTIONNER

Contrôler

2007 a permis de confirmer la place de plus en plus importante des contrôles dans l'activité de la CNIL. Cette année encore, le nombre de contrôles a progressé puisque **164 missions de contrôle** ont été organisées sur l'ensemble du territoire national (**+ 21 %**), qui ont concerné près de 140 organismes. À titre de comparaison, en 2004, seuls 45 contrôles avaient été effectués (une douzaine par an avant 2004).

L'augmentation du nombre de contrôles témoigne de façon significative de la volonté de la Commission de faire respecter les droits reconnus à chaque citoyen par la loi informatique et libertés et de s'assurer, sur place, du respect réel par les responsables de traitements des principes de cette loi.

Les contrôles menés par la Commission sont effectués afin de permettre :

La mise en œuvre du programme annuel adopté par la Commission en séance plénière. Il est défini à partir des thèmes jugés prioritaires par les commissaires : « audits » de fichiers d'importance nationale parfois très sensibles lorsqu'il s'agit de traitements de souveraineté, nécessité d'engager une action visant à améliorer la protection des personnes contre le fichage abusif (60 % des contrôles sont réalisés en application du programme annuel).

La réalisation de besoins identifiés par la CNIL :
– des missions de contrôle peuvent être effectuées dans le cadre du prolongement des formalités préalables, par exemple : le traitement mis en œuvre est-il réellement conforme au dossier de formalités déposé ou à l'autorisation unique visée ? Le refus d'autorisation prononcé par la Commission est-il respecté ? Quelles sont les pratiques des autres responsables de traitement ? Les mesures de sécurité décrites sont-elles effectivement mises en place ? ;
– des missions de contrôle peuvent vérifier le respect d'une mise en demeure adressé par la formation contentieuse en charge du contentieux des contrôles à un responsable de traitement ;
– le service des contrôles réserve une partie de son activité à des vérifications fondées sur des plaintes dont le contenu laisse à penser que le responsable de traitement est en infraction avec la loi (un peu plus de **40 % des contrôles** ont été réalisés dans le cadre de l'instruction de plaintes reçues par la CNIL).

En 2007, les missions de vérification sur place ont porté sur des sujets tels que :
- les dispositifs biométriques des établissements scolaires, des entreprises ou des structures médicales ;
- la prise en compte du droit d'opposition des personnes à être démarchées commercialement par téléphone par des organismes appartenant à des secteurs d'activité très hétérogènes, que ce soit des banques ou des installateurs de fenêtres ;
- les conditions de conservation des données dites « de connexion » (données relatives au trafic des communications électroniques), en particulier au regard des exigences des différentes réglementations prises dans le cadre de la lutte antiterroriste ;
- l'expérimentation du dossier pharmaceutique ;
- les systèmes de vidéosurveillance, que ce soit par des polices municipales ou par des entreprises ;
- les fichiers concernant les salariés : gestion des recrutements et des carrières bien sûr, mais aussi géolocalisation, transfert de données à l'étranger, développement de « lignes éthiques », etc. ;
- l'information des personnes par les opérateurs de communications électroniques (annuaires universels ou services universels de renseignement) ;
- les fichiers dits « de police », d'importance nationale (*cf.* p. 78).

Enfin, on relèvera que **près d'un quart des contrôles a donné lieu à l'examen par les membres de la formation contentieuse** des suites qu'il convenait d'y apporter. Les dossiers transmis à la formation contentieuse sont sélectionnés en fonction de critères définis par la Commission : sensibilité du manquement à la loi, importance de l'organisme mis en cause ou de la publicité donnée par cet organisme au traitement concerné et l'importance du nombre de personnes concernées.

Sanctionner

Une activité accrue

Le renforcement en personnel du service des sanctions a permis de faire croître son activité de plus de 30 %[1] par rapport à 2006.

La formation contentieuse de la CNIL met en exergue le nouveau rôle de contrôle *a posteriori* de la CNIL depuis 2004. Plaintes, contrôles, dossiers de formalités particuliers alimentent cette formation composée de six commissaires qui peut décider, notamment, de mises en demeures, d'avertissements ou de sanctions pécuniaires. Tous les sujets touchant aux données à caractère personnel sont abordés sous un angle quasi juridictionnel. L'année 2007 s'est illustrée par plus d'une centaine de mises en demeure et près d'une dizaine de sanctions pécuniaires ainsi que plusieurs avertissements.

Le rôle de la formation contentieuse est devenu déterminant et s'avère particulièrement efficace, au grand bénéfice des citoyens. La plupart des organismes concernés identifient parfaitement les suites éventuelles d'une mise en demeure et 80 % d'entre eux font d'ailleurs cesser les manquements constatés.

Les dossiers présentés en formation contentieuse concernent, pour plus d'un tiers, le non-respect des obligations de la loi en matière d'information des personnes et de droit d'opposition. On notera également la part importante des atteintes graves à la vie privée, c'est-à-dire le fait de faire figurer dans les fichiers des données sur l'appartenance ethnique, la santé ou des commentaires sur la vie privée des personnes. Les questions de sécurité et d'absence de garantie de la confidentialité des données sont également importantes. Enfin, l'absence d'accomplissement, auprès de la CNIL, des formalités préalables à la mise en œuvre du traitement représente un facteur commun à beaucoup de dossiers.

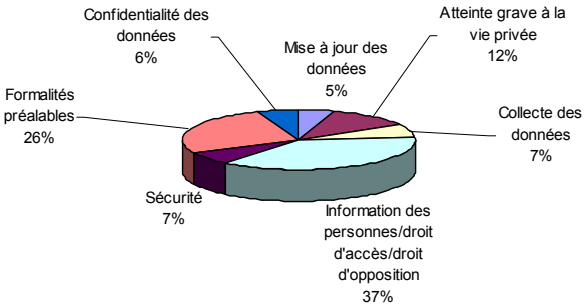
Les chiffres de la formation contentieuse

- **101 mises en demeure ;**
- **5 avertissements ;**
- **9 sanctions financières pour un montant de 175000 euros ;**

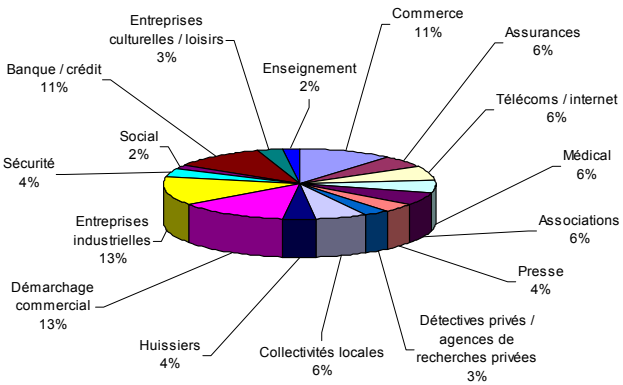
Soit une progression de l'activité du service des sanctions de plus de 30 %.

Les principaux secteurs concernés dans les dossiers de la formation contentieuse sont les organismes bancaires et de crédit ainsi que les sociétés de démarchage commercial, que ce soit par internet, téléphone/télécopie ou courriel. La prospection commerciale (VPC, propositions d'abonnement par courrier, sociétés démarchant pour les aménagements intérieurs…), qui constitue un important vecteur de plaintes à la CNIL, se retrouve logiquement comme le premier secteur visé par les mises en demeure ou sanctions pécuniaires de la CNIL.

Typologie des manquements de fond constatés par la formation contentieuse

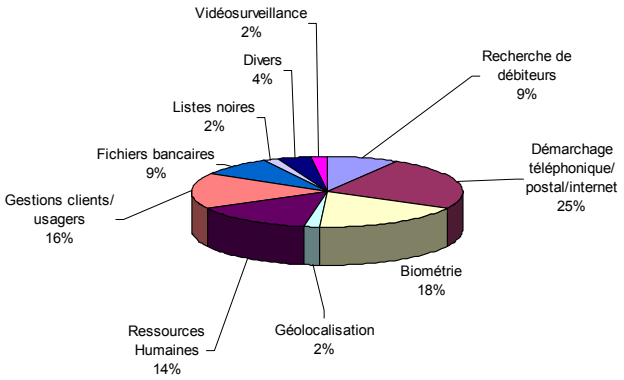


Typologie des secteurs d'activité présentés en formation contentieuse

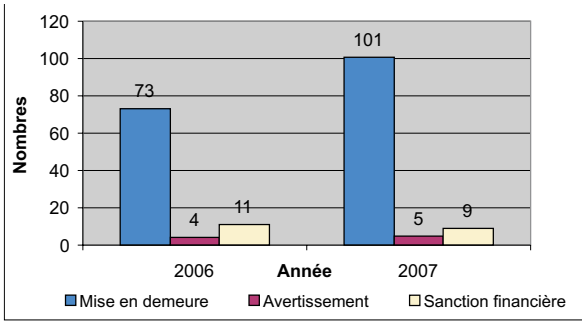


1. Nombre de mises en demeure.

Typologie des dossiers présentés en formation contentieuse



Graphique comparatif des types de sanctions prononcées en 2006 et 2007



Recherche de débiteurs : suite et... fin (ou presque)

▶ Dans son rapport annuel 2006, la CNIL indiquait avoir procédé à la mise en demeure de plusieurs sociétés de recherche de débiteurs en raison, notamment, de l'usurpation de titres ou fonctions pour obtenir de façon détournée des informations sur les personnes recherchées. Le 15 mars 2007, la formation contentieuse a décidé une sanction pécuniaire de 5 000 euros contre l'une de ces sociétés ; le 8 juin 2007, une sanction de 50 000 euros contre une autre de ces sociétés et, le 25 octobre 2007, une sanction pécuniaire de 10 000 euros pour une troisième.

Par ailleurs, plusieurs organismes qui répondaient aux sollicitations de ces sociétés en communiquant des données à caractère personnel sur leurs clients ou usagers viennent de faire l'objet de mises en demeure afin de cesser ces pratiques. L'action de la Commission ne s'arrêtera pas là et plusieurs autres procédures sont en cours d'instruction. Néanmoins, ces sanctions conduisent déjà à des méthodes plus transparentes.

Accéder à son compte sur internet... et à celui de tous les clients !

▶ La formation contentieuse a mis en demeure une société commercialisant sur internet des assurances-vie de revoir ses procédures de sécurité. En effet, l'un de ses clients, en voulant connaître ses encours, s'est aperçu qu'il accédait en réalité à l'ensemble des clients de son conseiller clientèle ainsi qu'à toutes les pièces fournies par ces clients à la banque.

Un fichier de gestion du personnel très particulier

▶ Une importante société spécialisée dans le merchandising et l'animation alimentait son fichier de personnel en commentaires pour le moins subjectifs et assurément non conformes à la loi informatique et libertés qui prévoit que les données des fichiers doivent être adéquates, pertinentes et non excessives. Quelques exemples du florilège constaté : « cas social », « menteuse et pas fiable », « nul », « serait une voleuse », « a disparu suite à une dépression : hospitalisé », « copine de M. – pas fiable ». Ces éléments, ajoutés à des carences en termes de déclaration de fichiers, de durée de conservation des données ou d'information des salariés, ont conduit la formation contentieuse à décider une sanction de 40 000 euros.

Des banques parfois très curieuses...

▶ La Commission a récemment mis en demeure plusieurs établissements bancaires ayant envoyé des questionnaires à des clients qui ne sollicitaient aucune prestation particulière, leur demandant de fournir des informations sur les revenus, la situation familiale, les enfants, l'employeur, etc. Des questionnaires qui n'indiquaient pas le caractère facultatif des réponses ni les mentions relatives aux droits d'accès et de rectification. Affaire à suivre...

Sans commentaire !

PETIT FLORILÈGE DE COMMENTAIRES CONSTATÉS PAR LA CNIL...

« Carence totale, alcoolique profond, au RMI »
« Séropositif depuis 23 ans »
« L'épouse du débiteur a un cancer du pancréas »
« Famille alcoolo »
« Danger ! Madame est malade nerveusement et a tendance à perdre les pédales »
« Bien mais râleuse »
« Cerveau de dinosaure »
« Grosse menteuse »
« Très très très chiante »
« 2 de tension »
« Monsieur je sais tout »
« Madame est odieuse, la taquiner un peu »
« Sal con »
« Bien mais un peu âgée »
« C'est une dame qui pue »
« Personne sans dent et qui boit »
« Branleur ne veut pas sortir de la chambre à 12 h 00, ne plus reprendre »
« Il est comptable et se la pète »
« Ne pas appeler avant 16 heures car mari très con »
« Est en instance de divorce car son mari est en prison pour avoir violé sa fille »
« Se travestit, ne plus prendre »
« Pisse au lit et dans la poubelle »

Les recours devant le Conseil d'État

Le développement de cette activité contentieuse a logiquement suscité en 2007 des recours. Ainsi, trois décisions de sanction prononcées fin 2006 ont fait l'objet d'un recours devant le Conseil d'État. Parmi ces trois décisions, deux concernaient des sociétés effectuant un démarchage téléphonique sans respecter la possibilité pour les personnes appelées d'exercer leur droit d'opposition. La troisième décision avait sanctionné une société pour avoir mis en œuvre un traitement de ressources humaines comportant des flux transfrontières sans avoir fourni à la CNIL tous les renseignements qu'elle avait demandés dans le cadre de l'instruction du dossier de formalités préalables.

Les moyens développés par les requêtes des trois sociétés ont porté tant sur la forme des décisions que sur le fond.

La Commission a précisé le formalisme des contrôles sur place (notification des décisions de contrôle, procès-verbal à l'issue du contrôle, faits reprochés au mis en cause...). Elle a également rappelé le cadre fixé par la loi pour ses missions de contrôle : le juge judiciaire n'intervient, conformément à l'article 44 de la loi du 6 janvier 1978 modifiée en 2004, que dans l'hypothèse d'une opposition du responsable des lieux afin d'ordonner le libre déroulement de la visite de la CNIL.

Les pouvoirs de sanction attribués à la CNIL en 2004 ont conduit la Commission à prévoir un ensemble de procédures destinées à respecter les droits de la défense : ainsi, la Commission a bien rappelé le rôle de régularisation de la mise en demeure. Un rapport de sanction est envoyé plus d'un mois avant l'audience à l'organisme faisant l'objet de la procédure afin qu'il puisse présenter ses observations. Il peut, en outre, être présent ou se faire représenter le jour de l'audience pour faire valoir ses arguments. Enfin, le rapporteur du dossier n'est pas présent au moment du délibéré de la formation contentieuse. Ces règles permettent de conférer à cette dernière un jugement impartial.

Sur le fond, la CNIL a réaffirmé que, lors d'une mission de contrôle, elle s'attachait à vérifier tous les éléments relatifs à la finalité déclarée du traitement, sans se limiter nécessairement à la dénomination de celui-ci. Cette approche matérielle du contenu des applications est indispensable à un bon exercice de ses pouvoirs.

ANTICIPER

Ainsi que cela a été souligné en novembre 2006 lors de la 28e conférence internationale des commissaires à la protection des données à Londres, les autorités souffrent d'une image trop juridique. Or la crédibilité de ces institutions est – et sera – de plus en plus liée à leur capacité à comprendre et anticiper les développements technologiques. Il est donc indispensable que les autorités de protection des données développent leur capacité d'expertise, de prospective et d'intervention dans le domaine technologique.

Pour la CNIL, cet objectif est prioritaire du fait qu'elle est de plus en plus sollicitée sur les sujets technologiques et qu'un nombre croissant de dossiers concerne la mise en œuvre de systèmes d'informations innovants (passeport biométrique, dossier médical personnel). Par conséquent, elle a décidé de développer ses activités d'expertise dès l'année 2007 en recrutant trois ingénieurs experts. Les premiers résultats sont très encourageants, si bien que le renforcement du service se poursuivra en 2008 avec notamment l'arrivée d'un nouvel expert.

Les priorités d'action de la CNIL sont aujourd'hui :
– le développement de l'expertise technique au sujet des applications informatiques complexes (comme la biométrie ou les architectures pour le vote électronique) ;
– l'évaluation approfondie de la sécurité de projets informatiques d'envergure nationale (comme les visas ou le passeport biométriques, le dossier médical personnel ou le bracelet électronique mobile) ;
– la participation, au niveau européen ou international, à des groupes de travail de protection des données (au sein notamment de l'*Internet Task Force* du G29, de l'*International Working Group on Data Protection in Telecommunications*, ou par des travaux internationaux menés avec la Commission européenne au sein du groupe d'experts qui publiera en 2008 une recommandation sur les RFID et un avis sur l'internet des objets) ;
– la veille et la réflexion en amont sur les sujets technologiques majeurs qui vont être amenés à influencer notre société dans le futur, en particulier le domaine des nanotechnologies qui aura un impact certain sur les architectures informatiques et sur leurs relations avec les individus,
– l'anticipation des évolutions technologiques afin qu'elles tiennent compte, dès leur conception, des problématiques informatique et libertés. Ceci requiert le développement de relations bilatérales avec les acteurs industriels majeurs et l'implication, en tant que membre du consortium ou du comité de pilotage, dans des projets de recherche nationaux ou européens (comme le projet eTen EuroPrise sur la labellisation et le projet ANR FC^2 sur la fédération d'identités numériques) ;
– l'information des citoyens ainsi que la participation à des colloques sur les problématiques de la technologie, de la sécurité et de la protection des données ;
– la contribution à des actions de standardisation, en particulier dans le domaine de la sécurité (par exemple en participant au comité du Référentiel général d'interopérabilité, piloté par la Direction générale de la modernisation de l'État).

Il s'agit donc de mieux comprendre et d'appréhender les enjeux technologiques, afin que l'innovation reste compatible avec une protection efficace des données personnelles et de la vie privée.

L'ÉCHELON EUROPÉEN EST DÉTERMINANT

Parce que les données circulent quasiment instantanément à l'échelle européenne, voire mondiale, la CNIL œuvre conjointement avec ses homologues européens dans différents groupes de travail, institutionnels ou informels. Sur le plan communautaire, elle est investie dans les travaux du G29, le groupe des CNIL européennes, dont le président de la CNIL est désormais le président depuis février 2008.

En 2007, les sujets abordés et les documents adoptés par le groupe ont été dominés par des **problématiques transatlantiques**, qu'il s'agisse de l'affaire PNR ou SWIFT[1], qui avaient déjà largement occupé les débats en 2006.

Dans le cadre des négociations avec les pays situés hors de l'Union européenne, et notamment les États-Unis, seule une prise de position harmonisée des autorités de protection des données permet de peser sur les débats, ainsi qu'ont pu le montrer le dossier des alertes professionnelles ou l'affaire SWIFT. Le G29 entend ainsi renforcer sa présence sur le plan international avec des thèmes relatifs aux moteurs de recherche et aux sites communautaires. De nombreux sujets ont été abordés par le G29, dont un avis important adopté le 20 juin 2007 sur la notion de donnée à caractère personnel et un document de travail adopté le 15 février concernant les dossiers médicaux électroniques. En outre, une enquête commune dans le secteur de l'assurance-maladie a été réalisée. Première du genre à être déclinée au niveau de chacun des États membres, elle a donné lieu à l'adoption d'un rapport d'évaluation le 20 juin. Cette action devrait déboucher prochainement sur une série de recommandations.

Dans le domaine du « premier pilier », la CNIL siège au sein de l'organe indépendant de contrôle EURODAC[2] aux côtés de ses homologues et du Contrôleur européen de la protection des données (CEPD). Dans le cadre des réunions de coordination tenues en 2007, plusieurs contrôles prioritaires ont été décidés autour du système EURODAC, qui est dédié à la comparaison des empreintes digitales des demandeurs d'asile sur le territoire de l'Union européenne pour la mise en œuvre de la convention de Dublin. Ces vérifications ont été suivies de recommandations à l'attention de la Commission et des États membres. Elles vont dans le sens d'un fonctionnement amélioré et plus rigoureux d'EURODAC, tant du point de vue de la qualité des données insérées dans la base que de ses conditions d'accès par les autorités de sécurité intérieures.

Dans le domaine du « troisième pilier », la CNIL siège au sein des trois autorités de contrôle communes (ACC) : Europol, Schengen et Douanes.

L'ACC d'Europol s'est réunie quatre fois en 2007, et a adopté son troisième rapport d'activité couvrant la période 2004-2006. Au titre des principales actions engagées, l'ACC a mené une nouvelle inspection auprès d'Europol, portant sur le département de la sécurité du système d'information, les fichiers d'analyse et le service des délits graves, qui a abouti à des recommandations. L'inspection a entraîné des vérifications en cascade auprès des unités nationales d'Europol, au sujet de la présence de certaines fiches individuelles dans l'IS (système d'information Europol). La CNIL a ainsi procédé à la vérification du bien-fondé du fichage de certaines personnes et du respect des délais d'effacement de ces fiches au regard de la convention Europol et du droit national.

Qu'est-ce que c'est ?

LE 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 nationales. Cette organisation réunissant l'ensemble des CNIL européennes 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.

1. Les documents adoptés par le groupe sont disponibles à l'adresse suivante : http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2006_fr.htm
2. En application du règlement EURODAC qui a remplacé en 2005, l'autorité de contrôle commune.

L'ACC Schengen s'est réunie à quatre reprises en 2007. Georges de La Loyère, commissaire de la CNIL en charge des affaires internationales, a été élu président de l'ACC, le 18 décembre 2007. Parmi ses activités marquantes de l'année, il a finalisé l'adoption de son rapport d'inspection suite au contrôle coordonné, mené par chaque autorité de protection des données, dont la CNIL, portant sur les modalités d'inscription de données relatives à des personnes ou à des véhicules aux fins de surveillance discrète et de contrôle spécifique (article 99 de la convention d'application des accords de Schengen).

L'ACC Douanes a engagé un contrôle mené par les autorités nationales de protection des données auprès des autorités douanières nationales en charge de la gestion du système d'information douanier (SID) ainsi qu'un contrôle du système central portant également sur les aspects sécurité. La CNIL a ainsi mené sur la base du questionnaire commun à l'ACC, les vérifications auprès de la Direction générale des douanes et des droits indirects (DGDDI). Un rapport final consolidé a été rédigé et adopté fin 2007.

Le groupe de travail européen Police, qui regroupe les CNIL européennes des États membres de l'Union et du Conseil de l'Europe, a vu ses activités et ses missions sur la protection des données dans le secteur « police/justice » renforcées par la Conférence européenne des commissaires à la protection des données, qui s'est tenue à Larnaca (Chypre) les 10 et 11 mai 2007. C'est en raison de l'accroissement des initiatives législatives prises au niveau européen pour lutter contre le terrorisme et la criminalité organisée qu'il est apparu indispensable aux autorités nationales chargées de la protection des données, d'instaurer une coopération plus étroite entre elles dans le troisième pilier, à l'instar du groupe de l'article 29 du premier pilier.

Ainsi, une résolution adoptée le 11 mai 2007 a structuré les missions et le mode de fonctionnement du groupe Police-Justice et a permis d'élire à sa tête un président (Franco Pizzeti, président de l'autorité italienne de protection des données) et un vice-président pour le représenter (Bart De Schutter, commissaire de la Commission belge).

Ce groupe a aussi adopté une déclaration[1] sur la proposition de décision-cadre relative à la protection des données traitées dans le cadre du troisième pilier, soulignant une fois de plus que l'ensemble de ces dispositions requéraient un niveau élevé de protection des droits fondamentaux et de règles harmonisées.

Qu'est-ce que c'est ?

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.

SCHENGEN

Le système d'information Schengen (SIS) centralise au niveau européen, sur le fondement d'une convention du 19 juin 1990, plus de 17 millions de 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.

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 de la protection des données.

1. Déclaration de Chypre du 11 mai 2007 relative à la décision-cadre de protection des données personnelles dans le troisième pilier, qui fait suite à la déclaration de Londres en novembre 2006, à la déclaration de Budapest en avril 2006 et de Cracovie en 2005 ainsi qu'à l'avis du groupe adopté sur ce même texte en janvier 2006.

LES DÉFIS

L'INTERNAUTE À LA TRACE

La surveillance des réseaux *peer to peer*

En octobre 2005, la CNIL a refusé la mise en œuvre de quatre dispositifs de surveillance des réseaux *peer to peer* présentés par des sociétés de perception et de répartition des droits d'auteurs du secteur musical (SACEM, SDRM, SPPF et SCPP). Ces sociétés ont attaqué les décisions de la Commission devant le Conseil d'État qui les a partiellement annulées le 23 mai 2007. Il a en effet estimé que la CNIL avait commis « une erreur d'appréciation » en considérant que les traitements ayant pour finalité de rechercher et constater la mise à disposition illégale d'œuvres musicales sur les réseaux étaient disproportionnés. En revanche, il a retenu l'analyse de la CNIL concernant le procédé d'envoi de messages pédagogiques ciblés aux internautes. Il a ainsi estimé que ces envois étaient illégaux car ils ne relèvent pas des cas de figure où les fournisseurs d'accès à internet sont autorisés à conserver les données de connexions des internautes.

Regards croisés

ISABELLE FALQUE-PIERROTIN

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

Comment la CNIL a-t-elle participé aux travaux de la mission Olivennes ?

E. de Givry : j'ai été auditionné en octobre 2007, au même titre que d'autres autorités publiques. Notre objectif était de permettre aux membres de la mission d'intégrer au mieux la protection des données dans leurs réflexions et leurs recommandations. Cette audition a été l'occasion de répondre à de nombreuses questions d'ordre technique et juridique en lien avec la protection de la vie privée sur internet.

I. Falque-Pierrotin : étant à la fois membre de la CNIL et de la mission Olivennes, j'ai pu mettre au service de la mission mon expertise en matière de protection des données à caractère personnel. Les membres de la mission ne mesuraient pas nécessairement la richesse du dispositif français et européen de protection des données, ses contraintes mais aussi ses garanties. Cette dimension du problème de la lutte contre le téléchargement illégal devait donc être clairement intégrée à l'analyse de la mission, d'autant que c'est une préoccupation importante des internautes.

EMMANUEL DE GIVRY

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

Quelles réactions suscitent les recommandations de la mission Olivennes au sein de la CNIL ?

I. Falque-Pierrotin : compte tenu des propositions du rapport, le gouvernement puis le Parlement seront amenés à discuter de ces questions et ils feront des choix. Ils devront se prononcer sur la nécessaire conciliation entre la défense des droits des auteurs et celle des libertés individuelles. Ce sont des choix difficiles qui impactent, de façon plus générale, la vision que notre pays a de la régulation d'internet. La CNIL jouera son rôle dans ce processus de décision.

E. de Givry : en tout état de cause, la Commission prend acte que, dans son rapport, la mission Olivennes rappelle à plusieurs reprises que les dispositifs envisagés devront être soumis à la CNIL et que la lutte contre le piratage doit passer par « des réponses proportionnées, pragmatiques, respectueuses des libertés individuelles », ce que la CNIL a toujours affirmé.

À la suite de cette décision, la Commission s'est rapprochée des sociétés de perception et de répartition des droits concernées afin de connaître leurs intentions. Trois d'entre elles (SACEM, SDRM, SCPP) ont renouvelé leurs demandes en les expurgeant du volet pédagogique invalidé. C'est ainsi qu'en novembre 2007, tirant les conséquences de la décision du Conseil d'État, la CNIL a autorisé ces sociétés à mettre en œuvre les traitements de recherche et de constatation d'infractions sur internet. La dernière société concernée (SPPF) a renouvelé sa demande au cours du mois de décembre 2007. La mise en œuvre de ce dispositif, identique aux trois autres, devrait être autorisée début 2008.

En juillet 2007, le ministre de la Culture et de la Communication a créé une mission chargée de trouver des solutions pour « lutter contre le téléchargement illicite et développer des offres légales d'œuvre », menée par Denis Olivennes et à laquelle participait Isabelle Falque-Pierrotin, membre de la CNIL, présidente du conseil d'orientation et déléguée du Forum des droits sur l'internet. Cette mission a présenté, en novembre 2007, plusieurs recommandations ; leur prise en compte par le gouvernement devrait entraîner des aménagements législatifs et techniques sur lesquels la CNIL aura à se prononcer.

Les contrôles de la CNIL

La CNIL a effectué plusieurs missions de contrôle dans les locaux de sociétés prestataires de service procédant à la surveillance des réseaux *peer to peer*. L'examen des éléments collectés lors des missions de vérifications devrait s'achever au cours du premier trimestre 2008.

L'adresse IP : une donnée à caractère personnel pour l'ensemble des autorités de protection européennes

Dans deux arrêts d'avril et mai 2007, la Cour d'appel de Paris a considéré que les adresses IP collectées à l'occasion de la recherche et de la constatation des actes de contrefaçon sur internet ne permettent pas d'identifier, même indirectement, des personnes physiques et que dès lors elles ne constituent pas des données à caractère personnel. La CNIL, inquiète des conséquences d'une telle analyse sur la protection de la vie privée sur internet, s'est rapprochée du Garde des sceaux et du procureur général près la Cour de Cassation afin que soit formé un pourvoi dans l'intérêt de la loi contre ces deux arrêts.

Par un courrier du 8 octobre 2007, le Garde des sceaux s'est engagé à présenter le recours devant la Cour de cassation qui devrait statuer au cours de l'année 2008. Notons que les autorités de protection des données des États membres de l'Union européenne ont rappelé, dans un avis du 20 juin 2007, que l'adresse IP constitue bien une donnée à caractère personnel.

Cybersquatting, typosquatting : l'AFNIC veille

L'Association française pour le nommage internet en coopération (AFNIC), association loi 1901, est l'organisme qui assure la gestion administrative et technique des noms de domaine en « .fr » (France) et « .re » (La Réunion).

Les pratiques dites de *cybersquatting* (utilisation abusive de noms de domaines correspondant à des marques notoires, des sociétés reconnues) et de *typosquatting* (enregistrement d'un nom de domaine proche d'un nom de domaine connu tel que legifrance.fr au lieu de legifrance.gouv.fr) sont en augmentation. Pour lutter contre ces pratiques, l'AFNIC a mis en place un dispositif permettant de tenir à jour une liste des personnes physiques qui recourent à de telles méthodes, contraires à la charte de nommage qu'elle a établie. Cette charte, dont la valeur normative a été reconnue par les tribunaux, précise les règles relatives à l'enregistrement et à la maintenance des noms de domaine administrés par l'AFNIC.

Les personnes inscrites sur cette liste ne pourront donc plus procéder à de nouveaux enregistrements de noms de domaine en « .fr » pendant un an, temps qui correspond à la durée de vie d'un nom de domaine. En cas de nouveau manquement pendant la période de sept ans, l'interdiction sera portée à trois ans. En cas de détournement d'identification pour l'enregistrement des noms de domaine en « .fr » en violation de la décision d'exclusion, l'interdiction sera portée à cinq ans.

Par une délibération du 13 septembre 2007, la CNIL, après avoir pris acte des garanties apportées notamment en ce qui concerne l'information des internautes concernés sur les modalités de mise en œuvre de cette procédure, a autorisé l'AFNIC à mettre en place cette liste.

Les moteurs de recherche et les sites communautaires

Internet fait aujourd'hui partie de notre quotidien : qu'il s'agisse de trouver le lieu de destination idéale pour ses prochaines vacances, la meilleure recette de tiramisu, de savoir ce qui se dit sur le dernier film de Georges Clooney… les moteurs de recherche sont devenus incontournables. Rechercher ses amis d'enfance, développer « ses réseaux » ou tout simplement se faire connaître sur la toile… Autant de raisons qui expliquent le succès actuel des sites communautaires. Pourtant, sous couvert de gratuité, ces services exploitent les données personnelles des internautes à des fins commerciales ou publicitaires, sans que ces derniers en soient clairement informés.

Questions à …

PHILIPPE LEMOINE

Président-directeur général de LaSer
Commissaire en charge du secteur « Technologie »

Pourquoi la CNIL s'intéresse-t-elle aux moteurs de recherche et aux sites communautaires ?

Qu'il s'agisse des moteurs de recherche tels que Google ou Yahoo ! ou des sites communautaires tels que Facebook, MySpace ou LinkedIn, ces services fonctionnent selon le même modèle économique : leur gratuité avec comme contrepartie un financement par la publicité qui, pour être toujours plus ciblée, exploite des gisements de données personnelles fournies par les utilisateurs eux-mêmes, parfois à leur insu.

Dès lors, il est naturel que la CNIL, comme les autres autorités de protection des données, se préoccupe du respect effectif, par ces services, des principes de protection des données et s'intéresse aux conditions dans lesquelles les données sont exploitées et aux modalités selon lesquelles les internautes en sont informés et peuvent exercer leurs droits informatique et libertés.

Ces services sont souvent très utiles. Quels sont les risques pour les citoyens ?

En dévoilant, à son moteur ou à son réseau, des données personnelles sur ses habitudes de vie, ses réseaux d'amis, ses loisirs, voire ses opinions politiques ou religieuses, l'internaute rend sa vie privée visible par chacun sur la toile et permet aux sites de se constituer de formidables mines d'informations susceptibles ainsi de multiples exploitations commerciales. La conscience de tout cela est imparfaite. Par moments, il y a des réactions de rejet face à une invasion maladroite de la publicité. Mais la sensibilité aux enjeux de libertés privées et publiques est insuffisante, notamment chez les jeunes.

Le risque est bien réel et accru du fait que l'internaute ne maîtrise pas toujours suffisamment ces nouveaux outils. Par exemple, même quand le service est paramétrable, la configuration par défaut favorise souvent une diffusion très large des données, si bien que des informations devant rester dans la sphère privée se retrouvent souvent exposées à tous sur internet.

Quelles actions sont en cours ou vont être menées par la CNIL ?

La CNIL s'est rapprochée des acteurs majeurs dans ces domaines, afin qu'ils prennent mieux en compte les problématiques informatique et libertés, qu'il s'agisse de la protection des données sensibles, de l'information des personnes et de l'exercice effectif de leur droit de refuser l'exploitation commerciale de leurs données, ou encore de la durée de conservation des données. Mais nos actions ne doivent pas se limiter à l'échelle nationale. C'est pourquoi le groupe des CNIL européennes (groupe dit de l'article 29) rendra public un avis sur les moteurs de recherche début 2008. Cet avis devrait rappeler les règles de protection des données applicables aux moteurs de recherche et formuler un certain nombre de recommandations pratiques. Le groupe entend adopter une démarche identique à l'égard des sites communautaires.

En parallèle, les utilisateurs doivent élever leur niveau de connaissance de base en matière de protection des données personnelles. Des actions d'information et de sensibilisation du public doivent donc être conduites par la CNIL, en particulier à destination des plus jeunes.

QUELLES TRACES PERSONNELLES GARDE UN MOTEUR DE RECHERCHE ?

Lors de chaque recherche, les moteurs collectent généralement de nombreuses informations sur vous : un cookie personnel, l'adresse IP de la machine et le contenu de la requête. Ces données sont souvent conservées pour de longues durées, c'est-à-dire excédant une année pour tous les acteurs majeurs du secteur. Ensuite, elles peuvent être effacées ou anonymisées. Cela signifie qu'un moteur de recherche connaît précisément toutes les recherches que vous lui avez soumises sur plus d'une année ainsi que toutes les publicités auxquelles vous avez été sensible.

Bon à savoir

FAIRE SUPPRIMER UNE PAGE WEB CONTENANT DES INFORMATIONS PERSONNELLES

Lorsqu'un internaute demande la suppression de la diffusion de données le concernant auprès de l'éditeur d'un site web, ce dernier déréférence la page en question mais l'information peut rester un certain temps disponible sur internet, ce qui suscite parfois réactions et plaintes auprès de la CNIL de l'internaute, estimant que ses demandes n'ont pas été prises en compte.

Qu'en est-il ? Les moteurs de recherche conservent temporairement une copie de toutes les pages que leurs moteurs d'indexation visitent. Interrogé sur ce point par la CNIL, Google a précisé que lorsqu'une page est supprimée par l'éditeur du site, cette page est également supprimée des résultats de recherche, y compris sa version cache lors de la prochaine indexation du site par le robot du moteur de recherche. Or, le délai de réindexation d'un site varie en fonction de différents critères tels que la popularité ou la fréquence d'actualisation du site, mais intervient en moyenne toutes les deux à trois semaines (certains sites, d'actualité par exemple, pouvant faire l'objet d'une mise à jour quasi quotidienne). C'est durant cet intervalle de temps que la version cache d'une page peut encore potentiellement être consultée alors que cette page n'est plus diffusée sur son site d'origine.

AUTOMOBILISTES, PIÉTONS, CYCLISTES, PASSAGERS : CIRCULEZ, VOUS ÊTES PISTÉS !

Le « *pay as you drive* » sous contrôle de la CNIL

L'assurance automobile s'intéresse à des dispositifs de télématique embarquée sur les véhicules dits *pay as you drive*, permettant de connaître l'usage réel du véhicule afin d'adapter la prime d'assurance. La CNIL a refusé en 2005 d'autoriser un assureur à tracer de façon systématique les déplacements des jeunes conducteurs et à enregistrer les dépassements de vitesses maximales autorisées, du fait de l'interdiction légale, pour les assureurs, de tenir un fichier d'infractions. Que tous les déplacements du véhicule puissent être enregistrés était apparu disproportionné par rapport à l'objectif poursuivi.

En 2007, de nombreux échanges ont eu lieu avec les assureurs, préalablement au lancement de nouvelles offres, afin de déterminer les conditions de mise en œuvre de tels systèmes respectant la protection des données et la liberté d'aller et venir.

Ainsi, pour l'assurance automobile des flottes de véhicules d'entreprises, la CNIL n'est pas opposée au développement de dispositifs transmettant aux assureurs des données statistiques anonymisées sous forme agrégée (pas de données de localisation), dès lors qu'aucune donnée ne permet de géolocaliser le véhicule ou de détecter d'éventuels excès de vitesse. Une étude d'ensemble est actuellement menée par la Commission sur ce sujet et sera rendue publique au cours de l'année 2008.

LAPI, système de lecture des plaques d'immatriculation

En application de la loi de lutte contre le terrorisme de janvier 2006, le ministère de l'Intérieur a soumis à l'avis de la CNIL un **système de lecture des plaques d'immatriculation**. Six véhicules de police sérigraphiés ou banalisés ont ainsi été équipés de caméras permettant de :
– lire automatiquement la plaque d'immatriculation des véhicules ;
– comparer ces données au fichier des véhicules volés et au fichier Schengen ;
– prendre la photographie des occupants des véhicules.

Ces dispositifs sont mis en œuvre à titre expérimental pour une période de deux ans et ont pour objet de :
– prévenir, réprimer et faciliter la constatation des actes de terrorisme ;
– faciliter la constatation des infractions de vol et de recel de véhicules volés ainsi que des infractions criminelles ou liées à la criminalité organisée.

Sans remettre en cause la légitimité de la lutte contre le terrorisme et la criminalité, la CNIL avait considéré en 2005 lors de l'examen du projet de loi de lutte contre le terrorisme que :
– la surveillance automatique des déplacements des personnes utilisant le réseau routier apparaissait de nature à porter atteinte à la liberté d'aller et venir ;
– la collecte systématique des photographies des passagers pouvait aboutir à un contrôle d'identité à l'insu des personnes.

Le projet d'arrêté concrétisant la mise en œuvre de cette expérimentation a été soumis à la CNIL qui a rendu, le 8 février 2007, un avis très réservé dans lequel elle souligne notamment que :
– de tels dispositifs peuvent être utilisés pour surveiller « des événements particuliers » sans que cette notion soit définie, ni la durée de leur installation ;

– des procédures de contrôle *a posteriori* de l'utilisation des données doivent être mises en œuvre aux fins de prévenir et empêcher tout détournement de finalité.

La Commission a demandé qu'un rapport d'évaluation comportant notamment des éléments permettant d'apprécier et de justifier les durées de conservation retenues lui soit transmis.

Consulter son solde de points du permis de conduire sur internet avec Télépoints

Le 21 juin 2007, la CNIL a donné un avis favorable à la création du téléservice Télépoints permettant la consultation directe par internet du solde des points affectés au permis de conduire. Ce site internet permettra aux titulaires du permis de conduire, et à eux seuls, de connaître leur solde de points, à l'exclusion de toute autre information.

Dans son avis, la Commission a estimé que ce nouveau téléservice comportait des mesures de sécurité satisfaisantes, notamment :
– la connexion au site internet est sécurisée ;
– l'accès au service nécessite un code d'accès confidentiel et sécurisé de huit caractères ;
– la confidentialité des informations de la base est assurée par leur chiffrement.

Vélib' : « les vélos en toute liberté » respectent-ils vos libertés ?

La CNIL a été consultée par la Ville de Paris et par la Société des mobiliers urbains pour la publicité et l'information (SOMUPI) sur la mise en place du système de location de vélos dénommé Vélib'. Ce système repose sur un abonnement à la journée ou à la semaine (« courte durée »), ou à l'année (« longue durée »). Une tarification supplémentaire est appliquée en fonction du temps de la location, la première demi-heure étant gratuite.

Dans le cadre d'abonnements de courte durée, ni SOMUPI ni la Ville de Paris ne disposent d'informations personnelles sur les usagers. En revanche, dans le cadre d'abonnements de longue durée, les données de validation (lieu de prise et de restitution du vélo) sont collectées et rattachées à l'identité de l'abonné. C'est pourquoi, dans un souci de protection de la liberté d'aller et venir anonymement, une discussion est engagée actuellement entre la CNIL, SOMUPI et la Ville de Paris sur la durée de conservation de ces données afin de limiter celle-ci au temps strictement nécessaire pour le traitement des réclamations clients concernant la tarification des locations.

Questions à …

GUY ROSIER

Conseiller maître honoraire
à la Cour des comptes
Vice-président délégué en charge
du secteur « Affaires économiques »

Qu'est-ce que le fichier central des automobiles (FCA) ? Pour quelles raisons la CNIL a-t-elle décidé de contrôler ce fichier ?

Dans le FCA, géré par l'Association auxiliaire de l'automobile (AAA), sont enregistrés les renseignements concernant l'ensemble des véhicules immatriculés en France et les données à caractère personnel de leurs propriétaires. Ces informations, collectées lors des procédures d'immatriculation, sont utilisées à des fins statistiques et commerciales par les constructeurs et concessionnaires automobiles agréés annuellement par le ministère de l'Intérieur.

La CNIL, régulièrement saisie de plaintes de particuliers, qui, sollicités à des fins commerciales, s'interrogent sur l'origine des informations utilisées par les constructeurs et concessionnaires, a décidé de mener des missions de contrôle auprès de ces derniers afin de vérifier les modalités d'utilisation du FCA et la qualité de l'information délivrée aux propriétaires de véhicules concernant le droit d'opposition dont ils disposent.

Comment se sont déroulés les contrôles ? Quels résultats ont été obtenus ?

La CNIL a effectué 15 contrôles auprès des principaux constructeurs et concessionnaires automobiles. Au regard des constatations effectuées, elle leur a prescrit de corriger certaines de leurs pratiques et, surtout, d'améliorer l'information qu'ils délivrent à leurs clients (en particulier, la possibilité de s'opposer à l'utilisation de leurs données). Elle a demandé en outre au gestionnaire du FCA de rappeler aux utilisateurs des données issues de ce fichier leurs obligations en matière de données personnelles.

Il faut souligner qu'un nouveau système d'immatriculation sera mis en place en 2009 : il est prévu, à cette occasion, d'améliorer l'information des automobilistes dès les formalités d'immatriculation, de manière à ce qu'ils puissent, le cas échéant, s'opposer à l'utilisation commerciale des informations ainsi collectées.

Le « passe découverte » : un passe Navigo enfin anonyme !

Aller et venir librement, anonymement, est l'une des libertés fondamentales dans nos démocraties. C'est pourquoi, à l'occasion du lancement des abonnements hebdomadaires et mensuels sur passe Navigo, la CNIL a réinterrogé le Syndicat des transports d'Île-de-France (STIF) sur la possibilité pour les usagers d'utiliser des titres de transport anonymes sans qu'il en résulte de surcoût. Cette demande de la Commission figurait déjà dans son avis du 8 avril 2004 relatif à l'exploitation des données de validation des passes Navigo par la RATP. Dans le passe Navigo actuel, les données de validation (date, heure et lieu de passage) sont associées au numéro d'abonné durant 48 heures, uniquement à des fins de lutte contre la fraude.

Depuis le 1er septembre 2007, le STIF commercialise un nouveau passe appelé « passe découverte » pour lequel les données de validation ne seront pas associées à un numéro d'abonné (ce qui les rend anonymes). Ce nouveau passe se compose à la fois d'une carte à puce anonyme et d'une carte nominative de transport qui, pour les besoins de contrôles des sociétés de transport, comporte au recto une photographie (collée par l'usager) et ses nom et prénoms (*via* une inscription manuscrite). La carte nominative de transport et la carte à puce doivent être présentées ensemble lors d'éventuels contrôles. Les données de validation inscrites sur la puce n'étant pas associées à un numéro d'abonné ou à un nom de client, elles ne sont conservées qu'à des fins purement statistiques

En cas de perte, de vol, de détérioration ou d'erreur technique, le remplacement du passe s'effectue moyennant finance, à charge pour l'abonné de fournir une nouvelle photographie et de réinscrire ses nom et prénoms au recto du nouveau passe.

Malgré la mise en service tardive et payante de ce passe Navigo « anonyme », la CNIL se réjouit de voir ses recommandations enfin appliquées. Elle a demandé au STIF d'assurer une large information des usagers sur le développement de ce passe anonyme.

PARAFES prend son envol... avec vos empreintes

La CNIL s'est prononcée le 3 mai 2007 sur le traitement PARAFES (Passage automatisé rapide aux frontières extérieures Schengen) qui pérennise les expérimentations menées depuis 2005 par le ministère de l'Intérieur dans le cadre du programme Pégase. Ce fichier permet de collecter et conserver dans une base centrale les empreintes digitales des passagers aériens qui le souhaitent, afin de leur permettre d'emprunter un dispositif de passage rapide des frontières extérieures de l'espace Schengen, dans tous les aéroports français internationaux qui mettront en place ce dispositif. Ce traitement concernerait environ 100 000 voyageurs aériens fréquents.

La Commission a déploré de ne pas avoir été destinataire d'une évaluation globale, reposant sur des critères et des objectifs bien identifiés, des expérimentations menées en 2005 et 2006. Elle a ainsi rappelé que si ce passage plus rapide des personnes souscrivant au programme PARAFES doit se faire dans le respect des règles de fiabilité et de sécurité des contrôles aux frontières, la mise en place d'une base centrale de données biométriques ne peut être admise que « dans la mesure où des exigences impérieuses en matière de sécurité ou d'ordre public le justifient ». L'inscription des empreintes digitales du voyageur dans une carte à puce individuelle et son utilisation comme moyen d'authentification biométrique présenteraient de moindres risques pour la protection des données personnelles que la création d'une base centrale.

La CNIL a également estimé que l'enregistrement dans une base centrale des empreintes digitales de huit doigts était excessif au regard de la finalité principale du traitement et non justifié techniquement. S'agissant de l'interconnexion du fichier PARAFES avec le Fichier des personnes recherchées (FPR) et le système d'information Schengen (SIS), qui constitue une nouveauté par rapport au dispositif expérimenté depuis 2005, si son intérêt ne peut être mis en cause, la Commission a demandé que cette interconnexion soit techniquement limitée à certaines informations.

Nouvel accord PNR Europe-États-Unis

En juillet 2007, l'Union européenne a conclu un nouvel accord avec les États-Unis sur le traitement et le transfert de données des données PNR par les transporteurs aériens au ministère américain de la sécurité intérieure (*United States Department of Homeland Security* – DHS). Ce nouvel accord remplace l'ancien accord PNR intérimaire signé avec les États-Unis le 19 octobre 2006 et qui arrivait à échéance le 31 juillet 2007. Ce nouvel accord, prévu pour une durée de sept ans, met un terme à la période d'incertitudes ouverte par la décision de la Cour de justice des communautés européennes du 30 mai 2006 annulant le précédent accord conclu le 28 mai 2004.

Qu'est-ce que c'est ?

LES DONNÉES PNR (*Passenger Name Record*)

Il s'agit des informations collectées auprès des passagers aériens au stade de la réservation commerciale. Elles permettent d'identifier, entre autres : l'itinéraire du déplacement, les vols concernés, le contact à terre du passager (numéro de téléphone au domicile, professionnel, etc.), les tarifs accordés, l'état du paiement effectué, le numéro de carte bancaire du passager, ainsi que les services demandés à bord tels que des préférences alimentaires spécifiques (végétarien, asiatique, kasher, etc.) ou des services liés à l'état de santé du passager. Des informations du type « tarif pèlerin », « missionnaire » ou « clergé » figurent dans les champs « libres » des rubriques « remarques générales ». Étant susceptibles de faire apparaître indirectement une origine raciale ou ethnique supposée, des convictions religieuses ou philosophiques, ou l'état de santé des personnes, ces données sont considérées par la directive européenne comme sensibles, à exclure ou à protéger.

Pourtant, si le résultat de ces négociations fournit désormais une base juridique à long terme pour le transfert de données passagers, il fait droit à des exigences américaines toujours croissantes.

Le nouvel arrangement est accompagné d'une lettre du DHS donnant des « assurances » censées garantir la manière dont il compte protéger les données PNR des passagers européens. Cependant, le groupe des CNIL européennes (G29), le Parlement européen, le Contrôleur européen de la protection des données de même que la CNIL ont estimé que le niveau global des engagements marquait un net recul au regard des normes européennes de protection des données. Ils ont souligné que cet accord ne garantissait pas un niveau de protection adéquat.

Dans son avis, le G29 souligne tout particulièrement que :
– le nombre d'autorités américaines pouvant accéder aux données PNR a été étendu ;
– les finalités d'utilisation des données PNR pourront varier en cas de modification unilatérale de leur législation par les États-Unis ;
– la décision éventuelle de transférer des données PNR européennes vers d'autres pays tiers sera prise de manière unilatérale par les États-Unis, sans consultation préalable des autorités européennes ;
– il est désormais possible aux autorités américaines, « dans des cas exceptionnels », d'avoir accès à des données dites sensibles, pouvant révéler l'origine raciale et ethnique, les opinions politiques, l'état de santé, malgré un filtrage initialement prévu ;
– les données seront conservées non plus 3 ans et demi mais 15 ans, sous forme active pendant sept ans et passive pendant 8 ans, sans garantie que les fichiers non consultés soient définitivement détruits ;
– le passage du mode *pull* actuellement en vigueur (accès direct par les autorités américaines aux données détenues par les compagnies aériennes) au mode *push* (envoi des données par les compagnies aériennes ne permettant plus d'accès direct aux autorités américaines) ne sera réalisé au 1er janvier 2008 que si les conditions techniques de ce passage paraissent acceptables aux États-Unis ;
– l'évaluation de l'application de l'accord (*review*) perd son caractère annuel obligatoire ; seul le commissaire européen de la Direction générale justice-liberté-sécurité sera en charge de cette inspection, sans que les autorités nationales de protection des données soient clairement associées ;
– les autorités américaines auront la faculté de décider de manière unilatérale s'il sera répondu favorablement aux demandes des passagers européens d'accès et de rectification aux données les concernant détenues par les autorités américaines.

Projet de PNR européen : quel modèle pour l'Europe ?

Le 6 novembre 2007, la Commission européenne a dévoilé son projet de décision-cadre visant à instaurer un régime PNR pour l'Europe. Son objectif est d'harmoniser les modalités de transmission par les transporteurs aériens assurant **des vols vers le territoire d'au moins un État membre ou à partir de celui-ci**, des renseignements relatifs aux passagers aux fins de prévenir et de combattre les infractions terroristes et la criminalité organisée.

Cette proposition reproduit, sur bien des points, le modèle de l'accord PNR EU-États-Unis de juillet 2007, qui constitue un recul pour l'ensemble du niveau de protection des données : ce dispositif prévoit ainsi la collecte de 19 catégories de données, une période de conservation de 13 ans (données accessibles pendant 5 ans puis conservées 8 ans dans une base de données passive), le transfert à des autorités de pays tiers, une clause de réciprocité avec des pays tiers utilisant déjà un système de PNR, une clause d'évaluation sans précision sur sa régularité ni sur la participation effective des autorités indépendantes de protection des données.

La CNIL et ses homologues du G29 on fait part, dès janvier 2007, de leurs fortes réserves sur l'opportunité de créer un tel dispositif. Le groupe a adopté un avis dès le 5 décembre 2007, qui recommande la prise en

compte de ses propres règles européennes de protection des données, et en particulier, une approche plus proportionnée du nombre de données à collecter ainsi que de leur durée de conservation.

Le G29 insiste sur l'obtention de garanties concernant le filtrage des données sensibles, les conditions de transferts de ces données à des pays tiers, de leur contrôle ou encore des conditions d'exercice du droit des personnes. Il est soucieux du niveau de garanties concernant la surveillance régulière du système par nos autorités indépendantes de protection des données.

Les initiatives du G29 associées à celles des mêmes autorités de protection des données réunies au sein du groupe Police-Justice du troisième pilier, ont débuté très en amont en réaction à l'initiative législative du PNR Europe afin d'aboutir très clairement à l'application d'un régime PNR exemplaire pour l'Europe. Comptant également sur le soutien actif du Parlement européen, fort critique à nouveau dans sa dernière résolution sur les termes de l'accord PNR EU-États-Unis [1], les autorités de protection des données n'auront de cesse d'affirmer ensemble dans le processus de négociation en 2008, auprès du Conseil et de la Commission européenne, que **le schéma de PNR américain ne peut et ne doit pas constituer un modèle pour l'Europe**.

La CNIL et ses homologues ne cachent pas leurs inquiétudes également sur la base légale de ce futur PNR Europe. En effet, les règles de protection des données, en l'état du texte, renvoient à l'application de la future décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, dont le trop faible niveau des garanties obtenues a été dénoncé sans relâche par la CNIL et ses homologues européens, le Contrôleur européen de la protection des données, le Parlement européen, jusqu'à l'adoption politique de ce texte en cette fin d'année.

1. Résolution du Parlement européen du 12 juillet 2007 sur l'accord avec les États-Unis concernant l'utilisation de données PNR.

LA SANTÉ NUMÉRIQUE À L'HEURE DES CHOIX

SESAM Vitale 2 entre en vigueur

Le dispositif SESAM Vitale comprend la carte Vitale, la carte de professionnel de santé (CPS) qui assure l'identification et l'authentification du professionnel de santé ainsi que le dispositif de signature électronique des feuilles de soins électroniques (FSE). Comme en témoignent les nombreux avis rendus sur le sujet depuis 1998, la CNIL suit avec constance ce dispositif et est très attentive aux mesures prises pour assurer la confidentialité tant des télétransmissions que des fichiers.

Début 2007, le gouvernement a décidé de diffuser la nouvelle carte Vitale qui comporte :
– la photographie couleur de l'assuré sur et dans la carte ;
– l'adresse de l'assuré, son médecin traitant, éventuellement les données relatives à la protection complémentaire ;
– la situation du titulaire en matière d'accident du travail ou de maladies professionnelles ;
– les données relatives à l'accès aux soins dans un autre État membre de l'Union européenne ;
– les coordonnées d'une personne à prévenir en cas de nécessité ;
– la mention indiquant que le titulaire a eu connaissance des dispositions de la réglementation sur le don d'organe.

À l'occasion des avis rendus le 10 juillet 2007 sur le système SESAM Vitale, la Commission a rappelé la nécessité d'un chiffrement fort des données de santé. Le dispositif SESAM Vitale 2 permet précisément un renforcement du chiffrement des données issues du codage des actes, prestations et produits, et un chiffrement de transport à condition d'avoir un logiciel métier SESAM Vitale 1.40 et un lecteur de carte adapté.

Les nouveaux dossiers DMP, DP et Web médecin : concurrence ou convergence ?

Qu'est-ce que c'est ?

LE DOSSIER MÉDICAL PERSONNEL (DMP)

Le DMP, dossier du patient, permettra aux professionnels de santé désignés par lui d'avoir accès à toute information médicale relative à ce patient pouvant être utile à la coordination des soins. Une réflexion est en cours sur la stratégie à adopter pour la poursuite de ce projet.

LE DOSSIER PHARMACEUTIQUE (DP)

Le DP permettra aux pharmaciens d'avoir accès à l'historique des médicaments délivrés à une même personne dans l'ensemble des officines au cours des quatre derniers mois, afin d'éviter les interactions médicamenteuses. Le DP, conduit et financé par l'Ordre des pharmaciens, est en cours d'expérimentation dans six départements.

LE WEB MÉDECIN

Le Web Médecin (ou historique des remboursements) permettra aux médecins conventionnés d'avoir accès, à l'occasion d'une consultation médicale, à l'historique des soins, médicaments et examens remboursés au patient au cours des 12 derniers mois. Le Web médecin, mis en place par l'assurance-maladie, est en cours de déploiement après avoir été expérimenté.

Questions à …

JEAN-PIERRE DE LONGEVIALLE

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

Ces projets ne risquent-ils pas de se concurrencer ?

C'est la question que se sont posée les membres de la Commission lorsqu'ils ont eu à délibérer en 2007 à la fois sur le DMP, sur une demande d'autorisation d'expérimentation du DP, enfin sur la généralisation progressive du Web médecin. Qui dit multiplication des bases de données médicales personnelles, dit multiplication des risques. Elle ne peut donc être envisagée qu'au prix de garanties renforcées et à la condition que chaque dispositif ait, pour la santé publique, une utilité spécifique indiscutable.

Par ailleurs, le fait que ces différents projets soient expérimentés ou arrivent en phase opérationnelle de façon plus ou moins concomitante risque, si un bon accompagnement n'est pas assuré, de faire naître auprès du public, et même des professionnels, des difficultés de compréhension ou d'adaptation.

En quoi ces différents projets se distinguent-ils les uns des autres ?

Les différences sont très nettes :
– le DMP est sous le contrôle du patient ; le DP et le Web médecin sont sous le contrôle, respectivement, des pharmaciens et de l'assurance-maladie ;
– le DMP est accessible d'abord au patient, ensuite aux professionnels de santé auxquels le patient attribue des droits d'accès ; le DP et le Web médecin sont accessibles (en présence du patient) respectivement aux pharmaciens et aux médecins conventionnés ;
– sur les historiques de remboursement fournis par le DP et le Web médecin, ne figurent que les codes détaillés des médicaments (avec les quantités) et des actes (par exemple, le numéro codant une analyse de sang et non la numération sanguine obtenue) ; dans le DMP, il s'agit de rendre accessibles les données médicales elles-mêmes de la façon la plus ergonomique possible ;
– les historiques de remboursement fournis sont limités à 4 mois pour le DP et à 12 mois pour le Web médecin ; le DMP, en régime de croisière, a vocation à accompagner la personne sa vie durant ;
– enfin, ces projets n'en sont pas au même point de maturité. Le DP est en cours d'expérimentation ; le Web médecin, après des expérimentations qui avaient été autorisées par la Commission, est désormais en phase de déploiement ; pour ce qui est du DMP, la ministre en charge de la santé, peu après sa prise de fonction, a souhaité confier une « revue de projet » à une mission conjointe des Inspections générales des finances, des affaires sociales et des télécommunications.

Où en est-on aujourd'hui sur le DMP ?

La mission d'inspection a remis un rapport approfondi. Les difficultés rencontrées dans la conduite du projet sont clairement analysées, en particulier celles tenant à des problèmes de gouvernance et surtout le fait que le modèle économique du DMP reste insuffisamment déterminé. Cependant, la mission estime qu'un abandon du projet serait vécu comme une régression, notamment du point de vue des droits du malade.

Elle recommande plutôt un recentrage stratégique, la reprise des expérimentations et l'adoption d'un calendrier de déploiement plus réaliste que celui initialement retenu. La ministre vient de charger un groupe d'experts de lui faire des propositions sur la base de ce rapport. Quelles seront-elles ? Une simple correction de trajectoire ou une révision de plus grande ampleur ? L'avenir reste, à cette heure, ouvert.

Quel est le rôle exact de la CNIL dans la mise en œuvre de ces projets ?

La CNIL a été associée dès le départ à leur mise en place. Elle a accompagné toutes les phases de définition et de réalisation du DMP et devrait prochainement se prononcer sur l'extension de l'expérimentation du DP qu'elle a autorisée le 15 mai dernier. Elle a également autorisé la généralisation du Web médecin le 10 juillet après en avoir validé les déploiements successifs.

Le développement de ces différents projets qui poursuivent des finalités en partie communes mais obéissent à des régimes juridiques distincts n'est pas sans poser des problèmes d'articulation et de lisibilité pour le grand public. C'est pourquoi la CNIL a attiré l'attention des pouvoirs publics sur la nécessité de clarifier les finalités et fonctionnalités de ces projets. Elle a également rappelé la nécessité, pour mener à bien ces projets, de définir un cadre juridique stable, de déployer des solutions de sécurité effectives et de haut niveau et de construire ces projets en informant les patients et en impliquant les professionnels de santé.

Les contrôles de l'expérimentation du DMP

La CNIL a procédé à près de 18 contrôles sur place auprès des principaux acteurs de l'expérimentation du DMP : hébergeurs, centres hospitaliers, réseaux de santé, médecins libéraux et centres d'appels. À l'issue de ces contrôles, elle a établi un constat dont beaucoup d'éléments restent d'actualité.

Sur les conditions d'ouverture du DMP

La CNIL a constaté que certains hébergeurs transféraient les identifiants de patients aux établissements de soins par voie électronique sans protection particulière. Certains centres d'appels, en cas de perte des identifiants permettant la consultation ou l'alimentation des DMP, envoyaient un mot de passe par courrier électronique non crypté au patient, ou lui communiquaient ce mot de passe par téléphone. Ces pratiques sont de nature à compromettre la confidentialité de ces informations.

Les modalités pratiques retenues pour permettre au patient de désigner nominativement les professionnels de santé autorisés à consulter et à alimenter le DMP se sont parfois traduites par des désignations collectives d'établissements ou de cabinets médicaux.

La CNIL a également relevé que les patients n'étaient pas tous parfaitement informés que l'accès aux données médicales contenues dans leur DMP nécessitait une connexion internet. De plus, il leur a été parfois indiqué que l'accès à ces données était possible par l'intermédiaire du centre d'appels de l'hébergeur, alors que ce dernier a pour seule fonction d'assister techniquement les patients ou de leur permettre de modifier les données administratives les concernant, leur mot de passe ou la composition de leur cercle de confiance.

Sur le fonctionnement du DMP

Une insuffisance des mesures d'identification et d'authentification mises en œuvre dans les centres d'appels a été relevée puisque l'authentification des patients ne s'opérait pas systématiquement par une interrogation à partir des questions défis renseignées par les patients lors de leur inscription (par exemple : « le nom de votre belle-mère ? La marque de votre première voiture ? ») .

De plus, des hébergeurs proposent, pour les établissements de soins n'ayant pas équipé leurs professionnels de santé de CPS (carte de professionnel de santé), un accès aux DMP depuis leur site internet sur la base d'un simple identifiant et d'un mot de passe. Cette solution, peu satisfaisante sur le plan des sécurités, ne saurait être pérennisée.

Il a toutefois été vérifié que les personnels administratifs et techniques, tant de l'hébergeur que des centres d'appels, n'ont pas accès aux données de santé contenues dans les DMP.

S'agissant du nouveau droit de masquage qui permet au patient de rendre inaccessibles à certains professionnels de santé des données présentes dans son DMP, la CNIL n'a pu mesurer son application effective, dans la mesure où il n'a pas été mis en œuvre dans le cadre de l'expérimentation.

Sur la sécurité et la protection des données

L'appréciation des dispositifs de sécurité proposés par chaque hébergeur était l'un des points essentiels des avis rendus par la Commission le 21 mars 2006. C'est pourquoi elle constituait un des aspects principaux des contrôles de la CNIL.

S'agissant du chiffrement complet des bases de données mises en œuvre, et non pas uniquement celui des canaux de communication des données, les missions de contrôle montrent que cette recommandation de la CNIL n'a pas été systématiquement mise en œuvre.

En outre, l'expérimentation a révélé une importante faille de sécurité sur le site internet d'un hébergeur, où l'accès au DMP par les patients reposait sur des identifiants et mots de passe identiques et facilement déductibles. Bien que résolue dans de brefs délais, cette faille a démontré l'intérêt qui s'attache à la définition d'un mot de passe « robuste ».

Au total, les contrôles effectués par la CNIL ont mis en évidence des niveaux de sécurité disparates et parfois insuffisants, en particulier à l'hôpital. La mission d'inspection de l'Inspection générale des affaires sociales (IGAS), des finances (IGF) et le Conseil général des technologies de l'information (CGTI) ont fait le même constat.

Bon à savoir

QUELS DROITS POUR LES PATIENTS ?

Alors que le DMP est rendu obligatoire puisque le niveau de prise en charge des actes et prescriptions par l'assurance-maladie sera subordonné à l'accès par le professionnel de santé au DMP, l'ouverture du DP est facultative et subordonnée à l'accord du patient qui a la faculté de fermer son dossier à tout moment dans l'officine de son choix.

La consultation du DMP, du DP et du Web médecin est subordonnée à l'accord préalable du patient qui se matérialise par la remise au praticien de sa carte Vitale. Toutefois, si le patient refuse l'accès de son DMP à son médecin, il sera moins bien remboursé, ce qui n'est pas le cas pour le DP et le Web médecin.

Le titulaire d'un DMP se voit reconnaître le droit de « masquer » les informations qui y sont portées, c'est-à-dire de les rendre inaccessibles à tous les professionnels, hormis le praticien auteur du document. Le titulaire d'un DP, quant à lui, ne peut pas rendre inaccessible une donnée inscrite, mais il a la possibilité de s'opposer à son inscription s'il ne souhaite pas qu'un médicament figure dans son DP ; l'exercice de ce droit sera signalé par l'indication du caractère incomplet du DP.

Le patient aura la possibilité d'accéder directement depuis son ordinateur à son DMP, alors qu'il ne pourra avoir accès à son DP et au Web médecin que par l'intermédiaire du professionnel de santé de son choix (pharmacien dans un cas, médecin dans l'autre).

LE SALARIÉ... MONDIALISÉ MALGRÉ LUI

Dans le cadre du programme annuel des contrôles 2007, la Commission avait souhaité que soient effectuées des missions de contrôle sur les conditions de mise en œuvre des fichiers relatifs à la gestion des ressources humaines. Près d'**une cinquantaine de contrôles** ont ainsi été diligentés afin de vérifier des dispositifs concernant des données à caractère personnel se rapportant à des employés : fichiers de gestion du personnel, de recrutement, mais aussi dispositifs biométriques, dispositifs de géolocalisation, alertes professionnelles, etc.

Les principaux constats qui peuvent être faits à l'issue de ces contrôles sont les suivants.

L'évaluation des conditions de mise en œuvre des dispositifs « d'alerte professionnelle »

Imposés par la loi américaine dite Sarbanes-Oxley aux entreprises cotées en bourse aux États-Unis, les dispositifs d'alerte professionnelle permettent aux salariés de ces entreprises de signaler, en dehors de la voie hiérarchique classique, des comportements contraires à la loi ou aux règles fixées par leur société.

Premier constat : **l'absence d'utilisation, par les salariés français, de ces dispositifs**. En effet, ces instruments, créés par les maisons mères situées à l'étranger, ne correspondent pas aux pratiques observées au sein des sociétés françaises. Il semblerait que ces dispositifs ne présentent guère d'utilité au regard des dispositions prévues par le Code du travail ou au regard de l'utilisation, classique, de la voie hiérarchique, afin de rapporter des dysfonctionnements.

Deuxième constat : **la mauvaise appréhension des contraintes issues de la loi informatique et libertés** lors de la mise en œuvre de ces dispositifs. Tel est le cas des entreprises qui ont procédé à un engagement de conformité à l'autorisation unique n° 4, alors même que très peu des dispositifs sont limités aux domaines « financier, comptable, bancaire et de lutte contre la corruption », comme le prévoit pourtant son article 1er. Dans les faits, les entreprises adossent leur dispositif d'alerte professionnelle à leur code de conduite, généralement rédigé par leur société mère, dont l'objet est plus vaste que le champ de l'autorisation unique de la CNIL.

Le développement important des flux transfrontières de données

En 2007, la CNIL a autorisé **1 682 transferts de flux transfrontières** et a toujours en attente d'instruction **538 demandes**. Dans le secteur des ressources humaines, deux cas peuvent être observés :

– les transferts sont réalisés à la demande de la société mère, située par exemple aux États-Unis, dans le cadre d'une rationalisation des outils de gestion des ressources humaines : toutes les filiales utilisent le même logiciel et les données sont hébergées dans les serveurs de la maison mère. Une absence totale de prise en compte des obligations issues de la loi informatique et libertés a parfois été constatée : absence d'information des personnes, ignorance quant à la durée de conservation des données une fois transférées, absence d'autorisation de la CNIL qui constitue un délit puni de cinq ans d'emprisonnement et de 300 000 euros d'amende en application de l'article 226-16 du Code pénal ;

– les données sont transférées à l'étranger dans le cadre de contrats de sous-traitance. L'entreprise décide de confier la gestion de sa paie ou de ses opérations de recrutement à un prestataire externe, situé à l'étranger ou qui héberge ses bases de données à l'étranger.

Questions à …

HUBERT BOUCHET

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

Pourquoi avoir choisi de porter un intérêt tout particulier aux dispositifs d'alerte professionnelle ?

La CNIL s'est mobilisée dès l'apparition des premiers projets d'application en France d'une de la loi Sarbanes-Oxley. Elle a mené un travail de fond, en coopération avec certaines autorités nord-américaines, afin de définir un cadre dans lequel ces dispositifs pouvaient être mis en place tout en respectant les exigences françaises en matière de protection des données à caractère personnel. La CNIL a ainsi adopté un document d'orientation le 10 novembre 2005 et une autorisation unique le 8 décembre de la même année (autorisation unique n° 4). Il est donc apparu nécessaire, dans un second temps, d'apprécier au sein même des entreprises les conditions de mise en œuvre de ces dispositifs qui excluent tout l'univers social de leurs champs.

Quels sont les principaux enseignements à retirer de ces contrôles ?

Manifestement, ces dispositifs apparaissent comme des instruments « importés » ne correspondant pas à la réalité sociale des entreprises françaises. Ils ne correspondent ni à la réalité des pratiques des entreprises françaises, ni à la mentalité des salariés français. La CNIL a même constaté que bon nombre de responsables chargés dans les entreprises concernées d'installer ces dispositifs sont eux-mêmes assez réticents à la mise en place de ces mécanismes. D'un point de vue informatique et libertés, ces dispositifs sont délicats à installer, notamment au regard de leur champ d'application et de l'information des salariés concernés.

Quels autres constats ces missions de contrôle ont-elles permis d'établir en matière de gestion des ressources humaines ?

Le recours à l'informatique en matière de gestion des ressources humaines – au sens large – n'est plus à démontrer : biométrie, gestion informatisée des carrières et des recrutements, vidéosurveillance, gestion automatisée des accès et du contrôle des présences, etc. Tous ces traitements sont soumis à la loi informatique et libertés. Pour autant, l'ensemble des obligations de loi est parfois mal appréhendé par les responsables de ressources humaines, notamment en matière de déclaration des traitements, de durée de conservation des données ou d'information des salariés. Ce constat est particulièrement vrai en matière de flux de données vers des États n'appartenant pas à la Communauté européenne, qui sont soumis à des règles précises parfois ignorées par les entreprises françaises qui encourent, de ce fait, de sérieux risques juridiques, y compris pénaux.

Bien souvent, l'entreprise responsable du traitement des données ignore la localisation effective des données dont elle est pourtant responsable.

Cette situation est de nature à méconnaître les dispositions de la loi qui prévoient **l'information des personnes** dont les données font l'objet d'un transfert à destination d'un État non membre de la Communauté européenne, mais aussi celles qui imposent au responsable de traitement de « maîtriser » la sécurité des données dont il est responsable. En effet, cette maîtrise implique de savoir où se situent physiquement les bases de données et de veiller à ce que leur transfert se fasse de manière à garantir leur confidentialité.

Les dispositifs de géolocalisation des véhicules de salariés

Ces dispositifs permettent à un employeur de connaître à tout moment la localisation d'un salarié utilisant un véhicule équipé d'un dispositif GPS. Les finalités pouvant conduire à la mise en place de tels outils sont parfois mal appréhendées par les sociétés qui peuvent avoir tendance à ne pas bien définir les objectifs présidant à la mise en œuvre de ces dispositifs. Dès lors, elles s'exposent à ne pas être en mesure de justifier d'une finalité légitime, notamment au regard de la recommandation adoptée sur ce sujet par la CNIL le 16 mars 2006.

La dizaine de contrôles effectuée a largement démontré un **manque d'information des salariés à propos de leurs droits** (droit d'accès, de rectification et d'opposition) et une absence de définition de la durée de conservation pour les données collectées par les employeurs.

LES INITIATIVES DE LA FRANCOPHONIE

Les parlementaires de la francophonie et le Gabon s'intéressent à la protection des données

En juillet 2007, Alex Türk, président de la CNIL, a été invité à Libreville à introduire le débat d'actualité de la 33e session de l'assemblée parlementaire de la francophonie consacrée à la protection des données personnelles et à la vie privée. À cette occasion, il a proposé deux lignes d'action :
– tout d'abord, il a évoqué le projet visant à doter chaque pays francophone d'une législation consacrant le droit à la protection des données et instituant une autorité indépendante chargée de son application ;
– ensuite, dans un monde où 4/5e des pays ne reconnaissent pas encore ce droit, il a indiqué que le principe d'une convention internationale devait être reconnu.

Lors de ce déplacement au Gabon, la délégation de la CNIL a rencontré plusieurs élus nationaux, des membres de la Cour constitutionnelle du Gabon, le ministre de la Justice et le président de l'Autorité de régulation des télécommunications. Une demande de coopération future a été évoquée par ces interlocuteurs.

Création de l'Association francophone des autorités de protection des données personnelles (AFAPDP)

L'AFAPDP a été créée à l'occasion de la première conférence des autorités francophones de protection des données personnelles qui s'est tenue à Montréal le 25 septembre 2007. Elle a pour mission de favoriser la coopération et les actions de formation entre les pays de la francophonie dans le domaine de la protection des libertés, des données personnelles et de la vie privée. Elle réunit 27 représentants d'État francophones.

LA FRANCOPHONIE

55 pays membres, 13 observateurs, 800 millions d'habitants, sur les 5 continents : tel est l'espace de la francophonie.

L'Organisation internationale de la francophonie (OIF) œuvre en particulier pour la paix, la démocratie et le développement, en apportant notamment son soutien à l'État de droit et aux droits de l'Homme. Elle agit pour que les pays du Sud en transition acquièrent les moyens de maîtriser le processus de leur développement. Elle entend contribuer à l'humanisation de la mondialisation, selon les termes d'Abdou Diouf, le secrétaire général de l'organisation.

Ont été élus :
– en qualité de président de l'association, le président de la commission d'accès à l'information du Québec ;
– en qualité de vice-présidents, la présidente de l'autorité du Burkina Faso récemment désignée et le préposé adjoint de l'autorité de la Suisse ;
– en qualité de secrétaire général, Alex Türk.

Le siège de l'association est à Paris, dans les locaux de la CNIL.

Questions à …

ALEX TÜRK

Sénateur du Nord
Président de la CNIL

Pourquoi avez-vous choisi de faire du partage d'expérience avec les pays francophones une priorité de votre mandat ?

Il y a au moins trois raisons à cela :
– dans un domaine marqué par l'accélération des progrès technologiques et par l'usage sans frontière des technologies de l'information, nous nous devions de développer nos coopérations au-delà de celles déjà mises en place avec les pays membres de l'Union européenne ; c'était également un souhait de nos homologues, en particulier du Canada et de la Suisse ;
– surtout, la chute des prix des technologies de l'information et de l'accès aux réseaux de télécommunications permet aux pays du Sud de moderniser leurs administrations et leur économie, mais aussi d'offrir des prestations informatiques ou télécoms aux entreprises de pays étrangers francophones (externalisation des centres d'appels ou de la gestion de base de données). Dès lors, pour s'assurer du niveau satisfaisant de protection des données de nos concitoyens, notre intérêt mutuel était de mettre à la disposition des pays du Sud notre expérience ;
– enfin, mon souhait est que nous puissions contribuer à déclencher, avec nos collègues des réseaux européen, francophone, ibéro-américain et de la région Asie-Pacifique, une initiative mondiale pour l'adoption d'une charte mondiale sur la protection des données personnelles.

Quels sont les résultats de l'action menée jusqu'à maintenant ?

Tout d'abord, nous avons obtenu une impulsion politique majeure grâce à l'engagement pris par les chefs d'État et de gouvernements de la francophonie en 2004 lors du sommet de Ouagadougou, et plus encore lors de celui de Bucarest en 2006, d'intensifier les travaux législatifs et institutionnels nécessaires à la reconnaissance du droit à la protection des données. Les institutions de la francophonie sont de plus en plus sensibilisées. C'est le cas de la délégation à la paix, à la démocratie et aux droits de l'Homme et de l'assemblée parlementaire. Plusieurs pays du Sud entament ou ont achevé les travaux législatifs auxquels nous avons été associés.

Le Burkina Faso a installé en décembre 2007 son autorité indépendante. Le Sénégal adopte actuellement sa législation informatique et libertés. La CNIL est sollicitée par les autorités du Gabon et de Madagascar. Le gouvernement français a fait de l'adoption d'une législation informatique et libertés la condition d'une aide apportée au Bénin en matière d'automatisation des fichiers de sécurité (police, gendarmerie, douanes). Avec le lancement de l'association des CNIL francophones (AFAPDP), nous renforçons nos capacités grâce à un échange de réflexion, d'information et de bonnes pratiques. Nous pourrons mesurer les progrès accomplis lors de la 2e conférence francophone dont la CNIL sera l'hôte en octobre 2008, à Strasbourg, à l'occasion de la conférence mondiale informatique et libertés.

AU PROGRAMME 2008

TRENTE ANS APRÈS, FAUT-IL (ENCORE) MODIFIER LA LOI INFORMATIQUE ET LIBERTÉS ?

Trente ans après la promulgation de la loi informatique et libertés, quatre ans après sa refonte, l'heure est au bilan : notre loi « tient-elle toujours la route » ? Est-elle toujours adaptée compte tenu des profondes mutations technologiques intervenues depuis les années 70, de la mondialisation croissante des traitements et des échanges de données, de l'évolution même des esprits ? La vie privée revêt-elle encore une signification à l'heure où chacun se dévoile sans complexe sur internet, révèle ses goûts, ses opinions politiques, sa religion, ses préférences sexuelles, son réseau d'amis… ?

Notre loi informatique et libertés est une bonne loi : robuste, elle a su jusqu'à présent résister à l'assaut des vagues technologiques et sécuritaires successives. Imaginative, elle a inspiré, et inspire, bien des législations étrangères de protection des données. Protectrice des droits des personnes, elle constitue un garde-fou indispensable face à un développement incontrôlé de l'informatique.

La loi du 6 août 2004, en confortant les missions d'expertise technique, en introduisant un pouvoir de contrôle et de sanction de la CNIL, un pouvoir d'autorisation *a priori* pour les fichiers les plus sensibles tout en instituant les correspondants informatique et libertés, véritables relais locaux de la CNIL, a incontestablement redynamisé la protection des données en France et donné à la CNIL une légitimité nouvelle grâce à ces pouvoirs accrus.

Pour autant, la loi doit encore être améliorée sur certains points : les formalités de déclaration restent mal comprises car trop complexes ; la réalité des transferts internationaux de données n'est pas vraiment prise en compte dans la loi ; l'information des personnes sur leurs droits mérite d'être précisée ; les modalités de fonctionnement de l'institution doivent être revues pour permettre une action plus efficace et rapide…

C'est la raison pour laquelle le président de la Commission a décidé de créer un groupe de travail qui, présidé par Jean Massot et Philippe Nogrix, aura pour mission d'évaluer l'application de la loi et de proposer le cas échéant une révision de celle-ci.

Questions à …

JEAN MASSOT

Président de section honoraire au Conseil d'État
Commissaire en charge du secteur « Finances publiques »

Pourquoi la CNIL a-t-elle décidé de créer un groupe de travail sur la révision de la loi informatique et libertés ?

Même si la refonte de la loi intervenue en 2004 a permis à la CNIL de disposer enfin de véritables pouvoirs de contrôle, de sanction et d'autorisation, nous sommes conscients que pour assurer pleinement les missions que nous a confiées le Législateur, il est nécessaire de parfaire sur certains points la loi, pour la rendre plus compréhensible et, de ce fait, en permettre une meilleure application.

Comment allez-vous procéder ?

Philippe Nogrix et moi-même allons d'abord dresser, avec le concours des autres membres de la Commission et des services de la CNIL, un premier inventaire des dispositions de la loi posant des problèmes d'application pratique ou des difficultés d'interprétation. Nous souhaitons aussi rencontrer un certain nombre d'acteurs économiques et institutionnels afin de recueillir leur point de vue et leurs éventuelles suggestions d'amélioration. Ensuite, des propositions de modifications de la loi seront le cas échéant formulées et bien sûr débattues par la collégialité.

Quand rendrez-vous vos conclusions ?

Le groupe de travail devrait en principe rendre ses conclusions à l'été 2008.

LA FRANCE ET L'ALLEMAGNE COORGANISATRICES DE LA 30e CONFÉRENCE MONDIALE

Pour la première fois depuis sa création en 1978, la conférence sera organisée conjointement par la CNIL et l'Autorité fédérale allemande de protection des données (*Bundesbeauftragte für den Datenschutz und Informationsfreiheit*, BfDI). Cette coorganisation, symbole de l'amitié franco-allemande, donne à l'événement une envergure particulière, résolument européenne et internationale. Le thème de la conférence est : « **Protéger la vie privée dans un monde sans frontières.** »

La conférence de 2008 se déroulera dans l'hémicycle de l'Assemblée parlementaire du Conseil de l'Europe, à Strasbourg, du 15 au 17 octobre 2008. Elle se tiendra dans un cadre et un contexte exceptionnels. Elle sera l'occasion de célébrer le 30e anniversaire des lois et des autorités française et allemande de protection des données. Ces deux lois fondamentales ont, quelques années plus tard, constitué la base des travaux du Conseil de l'Europe et de l'Union européenne en la matière. La Conférence se déroulera pendant la présidence française de l'Union européenne, qui fera de la défense des libertés et droits fondamentaux un de ses axes d'action.

La Conférence a pour objectif d'aider à identifier les grands enjeux, actuels ou en devenir, pour la vie privée des personnes, au regard des grands développements technologiques, politiques ou juridiques internationaux. En permettant d'exposer clairement les défis mondiaux auxquels font face les libertés individuelles, la Conférence a l'ambition de contribuer à améliorer l'effectivité de la protection des données dans le monde. Elle permet aux associations de consommateurs et de défense des libertés, aux entreprises, aux acteurs du secteur public et aux autorités de contrôle de débattre sur leurs préoccupations et leurs visions de la protection de la vie privée, dans un esprit de collaboration et de concertation. La Conférence a également vocation à susciter l'intérêt du grand public afin de le sensibiliser aux enjeux de la protection de la vie privée dans un monde marqué à la fois par un recours accru à la technologie et par la mondialisation.

Qu'est-ce que c'est ?

LA CONFÉRENCE MONDIALE DES COMMISSAIRES À LA PROTECTION DES DONNÉES ET À LA VIE PRIVÉE

Cette conférence se tient chaque année à l'automne. Elle réunit l'ensemble des 81 autorités et commissaires à la protection des données et à la vie privée de tous les continents. Elle est ouverte aux intervenants et participants du monde économique, des autorités publiques et de la société civile. Une partie de la conférence est réservée aux représentants des autorités accréditées par la conférence, durant laquelle sont adoptées les résolutions et déclarations.

EXTERNALISATION INFORMATIQUE : COMMENT ASSURER LA PROTECTION DES DONNÉES ?

À la suite des orientations publiées dans le rapport d'activité 2006 (p. 74), la Commission a décidé de mettre en place un groupe de travail sur la délocalisation des centres d'appels ainsi que sur l'externalisation informatique.

La problématique relative aux centres d'appels est double :
– il peut s'agir d'externaliser auprès d'un centre d'appels les contacts avec les clients qui appellent afin d'obtenir une aide technique dite *hot line*, une commande de biens ou de services, ou encore une simple information
– les centres d'appels peuvent aussi être utilisés par l'entreprise dans le cadre de son activité de prospection de nouveaux produits et services.

Dans les deux cas, des fichiers sont mis en œuvre et doivent donc respecter les règles de protection des données.

Par ailleurs, la tendance à l'externalisation en dehors de l'Union européenne des moyens informatiques des entreprises s'accentue, en particulier dans des pays qui, le plus souvent, ne disposent pas de législation protectrice des données personnelles. Selon le syndicat professionnel Syntec informatique, la part des services informatiques délocalisés à l'étranger (*offshore*) par les entreprises françaises passerait de 1,6 % à 5 % en 2009, soit une croissance plus élevée que celle des services eux-mêmes.

L'impact important de l'externalisation informatique et des centres d'appels sur les emplois tant en France que dans les pays prestataires inscrit la dimension économique et sociale au premier rang des problématiques soulevées par *l'offshore*.Or quel que soit le type de traitement effectué, de la simple *hot line* au transfert de données médicales, la prise en compte de la loi informatique et libertés dans les opérations d'externalisation s'impose.

Se pose également la question de savoir comment de tels transferts de données vers ces pays peuvent avoir lieu en assurant le respect des droits des personnes concernées. En créant ce groupe de travail sous la présidence de Didier Gasse, la Commission souhaite dresser un état des lieux de la situation, identifier les risques selon le type de situation rencontrée, faire le point sur les formalités applicables en matière de flux de traitement de données.

Le groupe de travail a vocation à proposer des solutions pour inciter les entreprises à un meilleur respect des règles de protection de données, qu'il s'agisse d'élaborer des codes de déontologie, des règles internes d'entreprise, voire d'alléger les formalités préalables.

Les travaux du groupe de travail ont débuté au dernier trimestre 2007. Les premières auditions ont permis de rencontrer notamment l'Association française des centres de relation clientèle (AFRC) et le Syndicat professionnel des centres de contact (SP2C), d'identifier le Maroc comme le premier pays francophone de destination sur le marché des centres d'appels *offshore*.

Ces actions s'inscrivent dans la démarche que la CNIL mène actuellement, en concertation avec ses homologues européens, visant à démontrer l'intérêt pour les pays tiers de se doter d'une loi spécifique de protection des données. Il s'agit ainsi de sécuriser le cadre juridique dans lequel les entreprises françaises externalisent hors de l'Union européenne, tout en favorisant le développement économique des pays en question, dans des secteurs à fort potentiel de développement.

LE CONTRÔLE DES FICHIERS DE POLICE STIC, FNAEG ET RG

Le contrôle du STIC

Pour la première fois de son histoire, la CNIL a engagé au mois de juin 2007, conformément à son programme annuel de contrôles, une vérification d'ensemble du Système de traitement des infractions constatées (STIC), « le grand fichier de la police », sous la responsabilité du ministère de l'Intérieur. Ce fichier regroupe toutes les informations concernant des personnes qui sont soit mises en cause dans des enquêtes ouvertes pour crimes, délits ou contraventions de 5e classe, soit victimes de ces mêmes infractions. C'est donc un fichier qui **recense des faits et non des condamnations**.

La mission a débuté en juin 2007 au ministère de l'Intérieur, et plusieurs contrôles ont déjà eu lieu à Paris, en région parisienne, en Champagne-Ardenne et en Normandie. Ils devraient se poursuivre dans d'autres régions au début de l'année 2008. Ces contrôles se déroulent auprès de commissariats de police, de services régionaux de police judiciaire, de directions régionales des renseignements généraux.

Dans la mesure où ces vérifications sur place ont également pour objet de s'assurer des conditions d'interrogation du fichier à des fins d'enquête administrative – quand celle-ci est rendue obligatoire pour l'exercice de certaines professions réglementées – , les représentants de la CNIL se sont également rendus dans des préfectures. En outre, la question de la mise à jour du STIC étant essentielle au regard de la protection des données personnelles, compte tenu notamment des conséquences qu'elle peut emporter sur le recrutement des personnes, les représentants de la CNIL sont aussi conduits à vérifier auprès des procureurs de la République les modalités de transmission aux services de police des suites judiciaires (par exemple un classement sans suite), surtout quand celles-ci sont susceptibles d'entraîner des modifications du STIC ou une consultation limitée à des fins administratives des informations qui y sont enregistrées.

D'ores et déjà, quelques constats peuvent être faits concernant les profils d'habilitations utilisés pour interroger le STIC, les relations entre les services de police et les préfets à qui il appartient de délivrer des décisions d'agrément et les tribunaux qui, de façon très inégale, répondent ou non aux services de police pour connaître les suites judiciaires des faits.

À l'issue de ces contrôles, la CNIL rendra publiques ses conclusions et proposera des mesures pratiques de nature à améliorer pour le citoyen tant **l'accès aux informations contenues dans ce fichier que les modalités de son fonctionnement.**

Les professions pour lesquelles la CNIL est le plus souvent saisie de demandes de droit d'accès indirect aux fichiers de police STIC et JUDEX sont :
– agents de surveillance et de gardiennage, de transport de fonds ;
– agents de recherches privées ;
– agents de sûreté procédant à de contrôles, notamment en zones aéroportuaires ;
– agents de sécurité de la SNCF et de la RATP ;
– fonctionnaires et agents de la police nationale, de la police municipale, des douanes.

Pour connaître la liste exhaustive des professions concernées, se référer au décret n° 2005-1124 du 6 septembre 2005 fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 21 de la loi n° 2003-239 du 18 mars 2003.

Le contrôle du FNAEG

Qu'est-ce que c'est ?

LE FICHIER NATIONAL DES EMPREINTES GÉNÉTIQUES (FNAEG)

Le FNAEG sert à faciliter l'identification et la recherche :
– des auteurs d'infractions à l'aide de leur profil génétique ;
– des personnes disparues à l'aide du profil génétique de leurs descendants ou de leurs ascendants.

Le FNAEG est placé sous la responsabilité de la Direction centrale de la police judiciaire au ministère de l'Intérieur, sous le contrôle d'un magistrat.

Le contrôle du FNAEG, qui était inscrit au programme annuel des contrôles de l'année 2007, s'est déroulé au mois de novembre dans les locaux de la police technique et scientifique d'Écully dans le Rhône. Ce contrôle, qui était aussi une première, a permis à la délégation de la CNIL de mesurer la place désormais prise par ce fichier en tant qu'outil quotidien de travail de la police.

Près de **616000 profils génétiques** sont aujourd'hui enregistrés dans la base et sa croissance est exponentielle depuis l'élargissement par les lois de sécurité successives intervenues en 2001 et 2003 de son champ d'application et de la nature des infractions susceptibles de justifier un enregistrement.

Ce contrôle a permis de vérifier les conditions d'enregistrement dans la base des informations, les modalités de mise à jour du fichier et d'effacement des données, ainsi que les différentes hypothèses de consultation des informations, notamment lorsqu'il est nécessaire de les rapprocher d'un profil génétique trouvé sur le lieu d'un délit ou d'un crime. Lorsque les conclusions de ce contrôle seront arrêtées par la Commission, elles seront également rendues publiques.

Le contrôle des fichiers des Renseignements généraux

Le contrôle de ces fichiers, inscrit initialement au programme de contrôle de la CNIL pour 2007, se déroulera en pratique en début d'année 2008. Son principe est prévu par l'article 6 du décret du décret du 14 octobre 1991 selon un rythme quinquennal. Or, le précédent contrôle date du deuxième semestre 1998. En effet, cette opération, qui nécessite une mobilisation importante des commissaires chargés du droit d'accès indirect et des services de la CNIL, n'a pu être réalisée plus tôt compte tenu de la charge de travail de la Commission et de l'insuffisance de ses moyens.

Les conséquences du rapprochement annoncé au sein d'une même Direction centrale du renseignement intérieur des services des renseignements généraux et de la Direction de la surveillance du territoire sont importantes, notamment du point de vue des méthodes de travail mises en œuvre et des éventuels nouveaux fichiers créés pour ce faire.

Ce contrôle permettra plus particulièrement de vérifier les points suivants :
– tout d'abord, s'assurer que lorsqu'une direction départementale des renseignements généraux indique à la CNIL qu'une personne est inconnue, elle l'est réellement ;
– ensuite, vérifier que les dossiers transmis par la DCRG correspondent bien à ceux détenus par les directions départementales des renseignements généraux ;
– enfin, s'assurer qu'en cas de demande par la CNIL de suppression partielle ou totale d'un dossier, celle-ci est effectivement réalisée par la direction départementale des renseignements généraux concernée.

AFFAIRE *DISCOVERY* : UN NOUVEAU DOSSIER SENSIBLE AVEC LES ÉTATS-UNIS

Qu'est-ce que c'est ?

DISCOVERY

Nom donné à la procédure américaine permettant, dans le cadre de la recherche de preuves pouvant être utilisées dans un procès, de demander à une partie tous les éléments d'information (faits, actes, documents...) pertinents pour le règlement du litige dont elle dispose quand bien même ces éléments lui seraient défavorables.

La CNIL constate un accroissement récent des exigences de communication de données personnelles détenues, entre autres, par les filiales françaises de sociétés américaines faisant l'objet de procédures de *Discovery* devant les juridictions civiles américaines, ou *Pre-trial discovery*. Il est devenu fréquent que les sociétés soumises à ces exigences, ou leurs filiales étrangères, se voient obligées de communiquer les copies de l'intégralité des disques durs ou des messageries électroniques de certains salariés, voire de l'ensemble de leur personnel.

Par ailleurs, dans un cadre juridique différent, certaines autorités étrangères, telles que la *Securities and Exchange Commission* (SEC) ou la *Federal Trade Commission* (FTC), peuvent également exiger de sociétés étrangères la production de documents ou pièces, en vertu de pouvoirs d'enquêtes qui leur sont propres.

Ces injonctions peuvent concerner des sociétés françaises, selon qu'elles sont filiales de sociétés américaines cotées sur le marché américain, ou qu'elles agissent directement sur le marché américain.

De nombreuses questions au regard de la loi informatique et libertés

Ces demandes de communication contreviennent aux dispositions relatives à la protection des données, tout particulièrement en ce qui concerne l'information et le consentement des personnes, la proportionnalité du traitement effectué et les conditions du transfert de données hors de l'Union européenne.

De telles situations soulèvent en outre des difficultés relevant d'autres domaines que celui de la loi informatique et libertés, notamment en matière d'entraide judiciaire internationale, de protection des intérêts économiques nationaux, de secrets industriels et commerciaux, voire de souveraineté nationale.

L'existence de procédures protectrices des intérêts des sociétés françaises

Toute injonction émise par les autorités judiciaires et administratives américaines, en application de la convention de La Haye de 1970, doit faire l'objet d'une demande d'entraide judiciaire auprès du bureau qui en est chargé au ministère de la Justice. Après examen, cette demande est soit rejetée, soit transmise à la juridiction dans le ressort de laquelle elle doit être exécutée.

La loi du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique prévoit que, sous réserve d'accords internationaux, il est interdit à toute personne de demander ou de communiquer des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives ou dans le cadre de celles-ci. Seule l'existence d'un accord ou traité international peut donc permettre de faire droit aux demandes d'autorités administratives étrangères.

Ainsi, un accord d'assistance mutuelle a-t-il été conclu entre la Commission des opérations de bourse (COB), devenue Autorité des marchés financiers (AMF) et la *Securities and Exchange Commission* (SEC). Seule une demande d'information relayée par l'AMF peut permettre aux entreprises françaises, sollicitées pour répondre à des demandes de la SEC, de se mettre à l'abri d'un risque de condamnation pénale.

Questions à …

BERNARD PEYRAT

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

Pourquoi avoir créé un groupe de travail et comment fonctionne-t-il ?

La CNIL a été approchée par des entreprises françaises et des cabinets d'avocats sollicitant ses conseils sur l'encadrement juridique devant être respecté quant à la communication d'informations à des autorités judiciaires ou administratives étrangères. Ces demandes, adressées par des administrations étrangères, mais aussi par des sociétés mères à leurs filiales, voire par des partenaires commerciaux, soulèvent des problèmes juridiques multiples qui intéressent aussi bien le secret des affaires que la protection des brevets, les mécanismes d'entraide judiciaires internationale, d'intelligence économique… domaines qui ne sont pas de la compétence de la CNIL.

En revanche, la CNIL est directement concernée par les conditions dans lesquelles sont transférées les données personnelles. Qu'en est-il de l'information et du consentement des salariés, des clients ou prospects, des avocats intéressés ? Des modalités de transferts de données hors Union européenne ? Et surtout de la proportionnalité des traitements mis en œuvre ?

La question est extrêmement délicate car il est souvent difficile pour une filiale de s'opposer ou même simplement de résister à la demande de sa maison mère ou à la demande d'une autorité administrative, en particulier des États-Unis, en raison d'une législation et d'une jurisprudence qui donnent des pouvoirs considérables à ces administrations ou au juge chargé d'apprécier la légitimité des demandes faites par une partie dans un procès.

Avec Georges de La Loyère, Philippe Nogrix et les services de la Commission, nous avons entrepris d'auditionner toutes les parties intéressées : pouvoirs publics, avocats, entreprises… Ce large échange permettra de nourrir la réflexion afin de déboucher sur des recommandations dans un domaine dans lequel c'est à peine forcer le trait que de souligner qu'il y a des enjeux tout à la fois de « guerre économique » et de « guerre de culture juridique », où s'opposent les systèmes romano-germanique et anglo-saxon.

Quels sont vos objectifs ?

Nos objectifs sont doubles.

Il est d'abord nécessaire de rappeler la nécessité de respecter le cadre juridique tel qu'il a été fixé, soit par notre législation de protection des données, soit par les conventions internationales, à défaut duquel les injonctions émises directement par des autorités étrangères seraient irrégulières, ce que beaucoup d'entreprises ignorent.

Par ailleurs, des travaux sont engagés au plan de l'Union européenne pour adopter une position commune. C'est la raison pour laquelle les réflexions nationales menées par la CNIL ont leur prolongement dans le cadre du G29. Ces travaux, renforcés par l'analyse des droits nationaux des pays de l'Union européenne, sont réalisés en concertation avec les institutions européennes, et en particulier la Commission, afin d'initier des négociations avec, entre autres, les États-Unis.

CRÉATION D'UN PRIX DE THÈSE INFORMATIQUE ET LIBERTÉS

Questions à ...

ANNE DEBET

Professeur des universités
Commissaire en charge du secteur «Affaires culturelles, enseignement»

La CNIL a décidé de créer un prix de thèse informatiques et libertés qui sera attribué pour la première fois en 2008.

Pourquoi créer un prix de thèse informatique et libertés ?

Il est essentiel, dans le monde d'aujourd'hui, de susciter et d'encourager la réflexion éthique et juridique sur les nouveaux enjeux de société induits par l'avènement du tout numérique. Force est de constater que les travaux de recherche universitaires manquent en ce domaine ; lorsqu'ils existent, ils se limitent trop souvent à une vision «très classique» des enjeux de la protection des données par exemple autour du numéro de sécurité sociale et des interconnexions. Or, ces enjeux doivent être réévalués à l'aune de ces nouvelles technologies d'identification et de traçage que sont la biométrie, les puces RFID, internet, les nanotechnologies.

La création de ce prix permettra, nous l'espérons, de développer les recherches et études en ces domaines. Ce sera aussi bien sûr, pour la CNIL, une occasion supplémentaire de sensibiliser le monde universitaire – enseignants comme étudiants – aux problématiques informatiques et libertés.

À qui ce prix est-il destiné ?

Ce prix s'adresse en priorité aux doctorants de 3e cycle en sciences humaines, droit, histoire, sciences politiques, sociologie, économie, qui ont soutenu depuis 2006, pour la première année, puis dans l'année universitaire précédant la remise du prix pour les années suivantes. Il concerne une thèse sur un sujet intéressant la protection des données personnelles ayant obtenu la mention très honorable avec les félicitations du jury.

Concrètement, quel sera son montant et les modalités de son attribution ?

Ce prix sera de 7 000 euros, ce qui constitue, je pense, un montant attractif. Notre Commission devrait prochainement définir la composition du jury dont j'assurerai la présidence ainsi que le calendrier pour la remise des travaux.

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

Décret d'application de la loi n° 2006-1640 du 21 décembre 2006 de financement de la sécurité sociale pour 2007

Création d'un répertoire national commun aux organismes chargés de la gestion d'un régime obligatoire de sécurité sociale, aux caisses assurant le service des congés payés, ainsi qu'aux organismes mentionnés à l'article L. 351-21 du Code du travail, relatif aux bénéficiaires des prestations et avantages de toute nature qu'ils servent.

Décret d'application de la loi n° 2007-1786 du 19 décembre 2007 de financement de la sécurité sociale pour 2008

Conditions d'application de l'article 161-36-4-2 du Code de la sécurité sociale relatif au dossier pharmaceutique.

Décrets d'application de la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance

Conditions d'application du nouvel article 6-I de la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité.

Décret d'application de la loi n° 2007-131 du 31 janvier 2007 relative à l'accès au crédit des personnes présentant un risque aggravé de santé

Conditions de collecte et d'utilisation des données à caractère personnel de nature médicale.

Décret d'application de la loi relative à l'informatique, aux fichiers et aux libertés

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

Décrets d'application de la loi n° 2007-127 du 30 janvier 2007 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions

Modalités d'élection par voie électronique.

Choix et modalités d'utilisation de l'identifiant de santé.

Décret d'application de la loi n° 2006-872 du 13 juillet 2006 portant engagement national pour le logement

Modalités de fonctionnement et nature des informations recueillies par l'Observatoire nominatif des logements et locaux.

Décret d'application de l'ordonnance n° 2007-329 du 12 mars 2007 relative au Code du travail

Conditions d'application des articles L. 5427-1 à L. 5427-5 du Code du travail.

Décret d'application de l'ordonnance n° 2006-596 du 23 mai 2006 relative au Code du sport

Mise en place d'un traitement automatisé portant sur les données relatives à la localisation individuelle des sportifs.

Décret d'application de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information

Conditions de sélection et de consultation des informations collectées par les organismes dépositaires mentionnés à l'article L. 132-3 du Code du patrimoine.

Décret d'application de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Modalités de mise en œuvre et d'exploitation d'un service public mettant à disposition de l'usager un espace de stockage accessible en ligne.

LES PROPOSITIONS DE LA CNIL aux pouvoirs publics

Aménager le régime du droit d'accès pour les traitements de lutte contre le blanchiment

Lors de l'adoption, le 1er décembre 2005, de l'autorisation unique portant sur les traitements mis en œuvre par les organismes financiers au titre de la lutte contre le blanchiment de capitaux et le financement du terrorisme, la question des modalités d'exercice du droit d'accès a été tout particulièrement examinée par la CNIL.

La difficulté de distinguer, parmi les données enregistrées dans ces traitements, celles qui sont soumises au secret professionnel le plus strict, a souligné l'utilité qu'il y aurait à introduire une disposition légale définissant, de manière spécifique, les règles d'accès à ce type de fichiers et instaurant une procédure équivalant à celle du droit d'accès indirect.

L'attention a été appelée sur la nécessité de remédier à cette lacune de notre droit à l'occasion de la refonte du Code monétaire et financier qu'entraînera la transposition de la troisième directive adoptée le 26 octobre 2005 sur la lutte antiblanchiment. Le projet de loi de transposition de cette directive est actuellement en cours de préparation et la Commission pourrait être consultée sur cet aspect du projet de loi au début de l'année 2008.

Assurer un développement encadré des études et recherches menées dans le domaine de la diversité, de l'intégration et de la lutte contre les discriminations

La France doit améliorer son appareil statistique et des réponses peuvent d'ores et déjà être apportées pour faire progresser la connaissance de notre société et, par là même, mieux lutter contre les discriminations.

Ainsi, au titre des recommandations sur la mesure de la diversité adoptées en mai 2007, la CNIL a notamment souhaité appeler l'attention des pouvoirs publics sur la nécessité d'ouvrir plus largement aux chercheurs, mais dans des conditions encadrées, l'accès aux fichiers de gestion et aux bases de données statistiques. À cet égard, la création de centres d'accès sécurisés, qui existent déjà à l'étranger, constitue une piste qui doit être approfondie. Il existe déjà, en France, un centre, « le réseau Quételet » (dénommé Comité de concertation pour les données en sciences humaines et sociales).

Il convient aussi de développer les études sur le « ressenti » des discriminations.

Sur un plan technique, la CNIL recommande aux pouvoirs publics d'encourager un recours beaucoup plus systématique aux techniques de chiffrement et d'anonymisation.

Revoir le régime d'encadrement des dispositifs de vidéosurveillance

Dès le développement des premiers systèmes de vidéosurveillance, la CNIL s'est reconnue compétente pour connaître des enregistrements visuels de vidéosurveillance sur la base de la loi du 6 janvier 1978.

La loi du 21 janvier 1995 d'orientation et de programmation pour la sécurité (LOPS), modifiée par la suite par la loi du 6 août 2004, a restreint la compétence de la CNIL en encadrant la vidéosurveillance sur les lieux publics par une procédure d'autorisation préfectorale (article 10).

Ainsi, seuls les enregistrements visuels de vidéosurveillance « utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques », sont soumis à la loi du 6 janvier 1978 modifiée en août 2004.

La loi du 23 janvier 2006 relative à la lutte contre le terrorisme a étendu les cas justifiant l'installation de systèmes de vidéosurveillance de lieux publics à la prévention d'actes de terrorisme

La CNIL, confrontée à un accroissement très net du nombre des déclarations et des plaintes relatives à la vidéosurveillance (chiffres 2007), mais aussi à de nombreuses demandes téléphoniques, constate de la part du public une grande incompréhension des règles applicables à la vidéosurveillance.

La complexité des dispositions applicables et leur manque de clarté rendent la bonne compréhension de ces règles difficile pour les citoyens.

Il apparaît souhaitable de clarifier le régime juridique applicable aux systèmes de vidéosurveillance, en particulier sur l'étendue de la compétence de la CNIL s'agissant des dispositifs de vidéosurveillance de voie publique et des lieux ouverts au public.

Compte tenu des évolutions technologiques et en particulier des possibilités de traitement des images, tout système numérique de vidéosurveillance installé dans un lieu public ou ouvert au public ne devrait-il pas relever de la compétence de la CNIL ?

L'enregistrement numérique de séquences de vidéosurveillance de personnes physiques ne constitue-t-il pas nécessairement aujourd'hui un traitement automatisé de données à caractère personnel au sens de la loi informatique et libertés ?

La loi du 21 janvier 1995 a été adoptée à une époque où la vidéosurveillance s'effectuait essentiellement avec des enregistrements analogiques sur bande magnétique. Elle doit aujourd'hui être revue à l'aune des évolutions technologiques.

La question du contrôle indépendant

Les récentes annonces gouvernementales (triplement du nombre de caméras de surveillance en France, relance du plan 1 000 caméras à Paris, projet d'interconnexion des images des réseaux de vidéosurveillance de la RATP, de la SNCF, mais aussi de lieux de cultes, de certaines entreprises et grands magasins), ont renforcé la nécessité d'une réflexion sur les moyens accordés aux organismes de contrôle.

À cet égard, l'attribution à la CNIL d'un pouvoir de contrôle unique sur les systèmes de vidéosurveillance, qu'ils soient installés dans des lieux publics ou dans des locaux privés serait une solution. Si le citoyen peut être amené à considérer que la mise en œuvre de dispositifs de systèmes de vidéosurveillance améliore le niveau de sécurité collective et individuelle, il ne veut pas renoncer pour autant à la garantie de ses droits. Apparaît ici la vocation de la CNIL à intervenir dans le contrôle de ces dispositifs.

D'ores et déjà, des préfectures ont sollicité la CNIL pour effectuer des contrôles sur place de systèmes de vidéosurveillance qu'elles avaient pourtant elles-mêmes autorisés et pour lesquels elles bénéficient, en théorie, d'un pouvoir de contrôle.

ANNEXES

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 contentieuse chargée de prononcer des sanctions. Il a été élu président du G29 en février 2008.

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 contentieuse.

Vice-président

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

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 contentieuse.

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

Anne DEBET, professeur des universités
Secteur : Affaires culturelles, enseignement
Anne Debet est membre de la CNIL depuis janvier 2004. Elle est membre élu de la formation contentieuse.

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

Georges de LA LOYÈRE, membre du Conseil économique et social
Secteur : Affaires internationales
Georges de La Loyère est membre de la CNIL depuis octobre 2004. Il est président de l'autorité de contrôle Schengen depuis le 18 décembre 2007 et représente la CNIL au sein du groupe de l'article 29 et de l'autorité de contrôle Europol.

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.

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.

Sébastien HUYGHE, député du Nord
Secteur : Affaires sociales
Sébastien Huyghe est membre de la CNIL depuis juillet 2007.

Philippe LEMOINE, président-directeur général de LaSer
Secteur : Technologie
Philippe Lemoine a été commissaire du gouvernement auprès de la CNIL de 1982 à 1984. Il est membre de la CNIL depuis janvier 1999.

Jean MASSOT, président de section honoraire au Conseil d'État
Secteur : Finances publiques
Jean Massot est membre de la CNIL depuis avril 2005.

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 contentieuse.

Michèle TABAROT, députée des Alpes-Maritimes
Secteur : Immigration, intégration
Michèle Tabarot est membre de la CNIL depuis juillet 2007.

Commissaires du gouvernement

Pascale COMPAGNIE

Catherine POZZO DI BORGO, adjointe

LES SERVICES AU 1er MARS 2008

Président

Alex TÜRK

Secrétaire général

Yann PADOVA

DIRECTION DES AFFAIRES JURIDIQUES, INTERNATIONALES ET DE L'EXPERTISE

DIRECTION DES RELATIONS AVEC LES USAGERS ET DU CONTRÔLE

DIRECTION DES RESSOURCES HUMAINES, FINANCIÈRES ET INFORMATIQUES

LA CNIL EN CHIFFRES

395 délibérations

En 2007, la CNIL a siégé 40 fois au cours de 25 séances plénières, 12 formations contentieuses et 3 bureaux. Ces réunions ont conduit à l'adoption de 395 délibérations (+ 30 % par rapport à 2006).

Au titre du conseil et de l'expertise

6 avis sur projet de loi ou de décret

Au titre des sanctions

9 sanctions pécuniaires correspondant à des amendes allant de 5000 à 50000 euros

5 avertissements

101 mises en demeure

Au titre de la simplification

4 autorisations uniques

2 avis sur un acte réglementaire unique

Au titre des formalités déclaratives

214 autorisations

26 refus d'autorisation

22 avis sur des traitements sensibles ou à risques

7115 saisines

En 2007, la CNIL a reçu 7115 saisines qui correspondent à **4455 plaintes** (+ 25 % par rapport à 2006) et **2660 demandes d'accès aux fichiers de police et de gendarmerie** (+ 67 % par rapport à 2006).

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

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

56404 déclarations de fichiers

En 2007, la CNIL a enregistré 56404 nouveaux traitements de données personnelles. Depuis 1978, ce sont au total 1216404 fichiers qui ont été déclarés à la CNIL.

Les chiffres à la loupe

En 2007, la CNIL a :

- **enregistré 56404 nouveaux traitements de données personnelles ;**
- **comptabilisé 685 CIL ;**
- **reçu 4455 plaintes ;**
- **adopté 395 délibérations ;**
- **autorisé 1682 transferts de flux transfrontières ;**
- **mené 164 missions de contrôle ;**
- **adressé 101 mises en demeure ;**
- **adressé 5 avertissements ;**
- **prononcé 9 sanctions financières ;**
- **effectué 5 dénonciations au parquet.**

LES MOYENS DE LA CNIL

Le personnel

La CNIL dispose de **105 postes budgétaires en 2007**, suite aux 10 créations obtenues en loi de finances 2007. Grâce aux 15 postes supplémentaires obtenus au budget 2008, la CNIL comptera **120 postes fin 2008 ;** l'effort engagé depuis 2005 est donc conforté et amplifié de façon significative sur 2007-2008.

Cependant, au regard des missions dévolues à la CNIL et des comparaisons internationales avec ses homologues notamment européens, cet effort devra être soutenu et poursuivi. À titre de comparaison, le ratio nombre d'agents par million d'habitants est de 1,6 pour la CNIL contre (par exemple) 11,5 pour l'autorité tchèque qui, avec seulement 10 millions d'habitants, bénéficie d'autant d'agents que la CNIL. À cette aune, cette dernière se situe au dernier rang de l'Union européenne.

En termes d'effectifs globaux, l'autorité anglaise comprend 260 agents et l'autorité allemande près de 400 ; l'autorité canadienne dispose quant à elle de 300 agents (pour une population totale de 30 millions d'habitants).

L'accroissement de l'activité est en effet plus rapide que ce qui avait été envisagé en 2004 et 2005. Les nouvelles missions de contrôles, de sanctions, de coordination du réseau des correspondants informatique et libertés et d'information du public ainsi que les fonctions supports (budget, comptabilité, gestion des ressources humaines…) associées au développement des activités « métiers » de la CNIL, impliquent des ressources humaines suffisantes, seul moyen de répondre efficacement aux attentes légitimes d'écoute et de proximité de nos concitoyens.

Pour illustrer cette activité en forte expansion, on constate notamment une augmentation :
– des demandes de droit d'accès indirect (environ 400 en 2002 ; 2 660 en 2007) ;
– du nombre de plaintes reçues (environ 240 chaque mois au cours du dernier trimestre 2006 contre 360 désormais) ;
– du nombre de délibérations rendues (395 en 2007, soit plus de cinq fois plus qu'en 2003).

Les crédits

Le budget 2007 a augmenté de 10 % par rapport à 2006, sous l'effet principal de l'augmentation évoquée des effectifs [1].

S'agissant du budget de fonctionnement, si l'augmentation du budget en 2006 a permis la concrétisation du projet de déménagement de la CNIL sur un site unique, plus vaste et plus fonctionnel, lui permettant de disposer d'espaces nécessaires à l'accueil du public et à la formation des correspondants informatique et libertés, la progression en 2007 a été trop faible pour répondre aux besoins induits par le fonctionnement courant de l'institution et à la montée en charge de projets notamment informatiques indispensables au bon rendement des activités de la CNIL. Elle ne dispose pas non plus des ressources suffisantes pour engager une véritable politique d'information des citoyens et de communication sur l'importance des enjeux auxquels elle doit répondre.

L'augmentation obtenue en loi de finances initiale 2008 de **400 000 euros** va certes offrir quelques marges de manœuvre nouvelles, mais cette progression reste bien en deçà des niveaux nécessaires, d'autant plus qu'en application de la LOLF [2], elle est **amputée en gestion de 249 000 euros** dès le 1er janvier 2008.

En matière de fonctionnement aussi, les comparaisons internationales sont souvent défavorables à la CNIL. À titre de meilleur exemple, l'autorité anglaise dispose d'un budget de communication 30 fois supérieur à celui de la CNIL, soit environ 3 millions d'euros (10 % du budget total) contre 100 000 euros (0, 9 % du budget total) pour la CNIL.

1. La masse salariale correspondante étant inscrite au budget de la CNIL.
2. Loi organique relative aux lois de finances du 1er août 2001.

Évolution des moyens de la CNIL (lois de finances initiales)

	2004	2005	2006	2007	2008	Évolution (en nombre) 2004-2008	Évolution (en %)
Postes	**80**	**85**	**95**	**105**	**120**	**40**	**50,0**
Crédits (en M€)	**6,5**	**7,2**	**9,0**	**9,9**	**11,4**	**4,9**	**75,4**
Personnels	*4,2*	*4,7*	*5,3*	*6,1*	*7,2*	*3,0*	*71,4*
Fonctionnement	*2,3*	*2,5*	*3,7*	*3,8*	*4,2*	*1,9*	*82,6*

LISTE DES DÉLIBÉRATIONS ADOPTÉES PAR LA CNIL EN 2007

Les délibérations de la CNIL sont consultables sur le site de Légifrance – www.legifrance.gouv.fr

NUMÉRO DATE	OBJET
2007-001 11 janvier 2007	Délibération portant avis sur le projet de décret pris pour l'application du dernier alinéa du I de l'article 30 de la loi du 6 janvier 1978
2007-002 11 janvier 2007	Délibération portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion d'infractions à la police des services publics de transports terrestres
2007-003 11 janvier 2007	Délibération portant avis sur un projet de décret simple portant création du système national d'information prévu à l'article L. 247-2 du Code de l'action sociale et des familles, organisant la transmission des données destinées à l'alimenter
2007-004 11 janvier 2007	Délibération autorisant l'Institut national de la statistique et des études économiques (INSEE) à mettre en œuvre les traitements automatisés de données à caractère personnel nécessaires à la réalisation d'une enquête statistique obligatoire de victimation
2007-005 11 janvier 2007	Délibération autorisant la mise en œuvre par la CPAM de Montbéliard d'un traitement automatisé de données à caractère personnel ayant pour finalité le suivi des fraudes
2007-006 18 janvier 2007	Délibération autorisant la mise en œuvre par l'université d'Évry-Val d'Essonne d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance du visage et de l'iris
2007-007 18 janvier 2007	Délibération autorisant la mise en œuvre par la société Sagem Défense Sécurité d'un traitement automatisé de données à caractère personnel ayant pour finalité principale le développement d'algorithmes de reconnaissance du visage en trois dimensions
2007-008 18 janvier 2007	Délibération portant avis sur le projet de décret pris pour l'application des articles L. 611-3 à L. 611-5 du Code de l'entrée et du séjour des étrangers et du droit d'asile et portant création du Fichier des non-admis (FNAD)
2007-009 18 janvier 2007	Délibération autorisant la mise en œuvre par la société Crédit Logement d'un traitement automatisé d'aide à la décision en matière d'octroi de garantie
2007-010 18 janvier 2007	Délibération portant avis sur un projet de décret en Conseil d'État relatif aux traitements de données à caractère personnel mis en œuvre au sein des maisons départementales des personnes handicapées
2007-011 25 janvier 2007	Délibération portant avertissement
2007-012 25 janvier 2007	Délibération portant mise en demeure
2007-013 25 janvier 2007	Délibération portant mise en demeure

2007-014 25 janvier 2007	Délibération portant mise en demeure
2007-015 25 janvier 2007	Délibération portant mise en demeure
2007-016 25 janvier 2007	Délibération portant mise en demeure
2007-017 25 janvier 2007	Délibération portant mise en demeure
2007-018 25 janvier 2007	Délibération portant mise en demeure
2007-019 25 janvier 2007	Délibération portant mise en demeure
2007-020 25 janvier 2007	Délibération portant habilitation d'agents de la CNIL
2007-021 8 février 2007	Délibération autorisant à titre expérimental, pendant un an, la mise en œuvre par la société RIA France d'un traitement automatisé des ordres de transferts internationaux de fonds, ayant notamment pour finalité la lutte contre le blanchiment de capitaux et le financement du terrorisme
2007-022 8 février 2007	Délibération autorisant l'INSEE à mettre en œuvre les traitements automatisés de données à caractère personnel nécessaires à la réalisation et à l'exploitation des résultats d'une enquête statistique obligatoire concernant la santé des jeunes
2007-023 8 février 2007	Délibération autorisant la mairie de Toulouse à mettre en œuvre un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2007-024 8 février 2007	Délibération autorisant la mise en œuvre par la communauté d'agglomération Salon-Étang de Berre-Durance d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2007-025 8 février 2007	Délibération autorisant la mise en œuvre par l'établissement public du musée du Louvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux clés de certains locaux du musée du Louvre
2007-026 8 février 2007	Délibération autorisant la mise en œuvre par l'Institut national des hautes études de sécurité d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données issues du Système de traitement des infractions constatées
2007-027 8 février 2007	Délibération portant avis sur le projet d'arrêté pris pour l'application de l'article 8 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers
2007-028 13 février 2007	Délibération portant avis sur le projet d'arrêté portant création d'un traitement automatisé de données à caractère personnel dénommé Centre de gestion des interceptions judiciaires (CGIJ)
2007-029 13 février 2007	Délibération portant avis sur un projet de décret en Conseil d'État fixant le contenu et les modalités de transmission à la direction générale des impôts, aux fins de pré-impression sur leur déclaration de revenus, des revenus perçus par les personnes employées à domicile et payées par chèque emploi-service ou dans le cadre de la prestation d'accueil du jeune enfant
2007-030 15 février 2007	Délibération portant mise en demeure

2007-031 15 février 2007	Délibération portant mise en demeure
2007-032 15 février 2007	Délibération portant mise en demeure
2007-033 15 février 2007	Délibération portant mise en demeure
2007-034 15 février 2007	Délibération portant mise en demeure
2007-035 15 février 2007	Délibération portant mise en demeure
2007-036 20 février 2007	Délibération portant avis sur deux projets d'arrêtés relatifs d'une part aux spécifications physiques et logiques de la carte d'assurance-maladie et aux données contenues dans cette carte et d'autre part aux conditions d'émission et de gestion des cartes d'assurance-maladie
2007-037 20 février 2007	Délibération autorisant la mise en œuvre par la caisse primaire d'assurance-maladie Pau-Pyrénées d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des activités contentieuses et le traitement des litiges
2007-038 20 février 2007	Délibération autorisant la mise en œuvre par la fondation Les orphelins apprentis d'Auteuil d'un traitement de données à caractère personnel ayant pour finalité le suivi des incidents concernant les personnes accueillies dans ses établissements afin d'assurer la prévention des incidents et la protection des jeunes
2007-039 20 février 2007	Délibération portant refus d'autorisation de la mise en œuvre par la société Crown Worldwide SAS d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle
2007-040 20 février 2007	Délibération portant refus d'autorisation de la mise en œuvre par la société Kimberly-Clark SNC d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle
2007-041 8 mars 2007	Délibération autorisant de la mise en œuvre par Aéroports de Paris d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au sein de la zone réservée du satellite S3 de l'aéroport de Paris-Charles-de-Gaulle
2007-042 8 mars 2007	Délibération autorisant le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche à réaliser et à exploiter les résultats d'une enquête statistique réalisée auprès d'un panel d'élèves entrés en classe de 6e en 1995 concernant leur santé
2007-043 8 mars 2007	Délibération autorisant la mise en œuvre de deux traitements de données à caractère personnel de la Commission nationale des comptes de campagne et des financements politiques permettant la gestion des reçus délivrés aux personnes ayant apporté leur soutien financier à un candidat aux élections ou à un parti ou groupement politique, d'une part, et celle de l'examen des comptes de campagne des candidats aux élections et des partis politiques, d'autre part
2007-044 8 mars 2007	Délibération refusant la création par la société Experian d'un traitement automatisé ayant pour finalité la mise en place d'une « centrale de crédit »
2007-045 15 mars 2007	Délibération portant mise en demeure
2007-046 15 mars 2007	Délibération portant sanction

2007-047 15 mars 2007	Délibération portant sanction
2007-048	Délibération annulée
2007-049 15 mars 2007	Délibération portant sanction
2007-050 21 mars 2007	Délibération portant autorisation de la mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles à l'entreprise François-Charles Oberthur Fiduciaire
2007-051 21 mars 2007	Délibération portant autorisation de la mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles au Millennium Chemicals Thann SAS
2007-052 21 mars 2007	Délibération portant autorisation de la mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité contrôle d'accès au bâtiment du service interacadémique des examens et concours (SIEC)
2007-053 21 mars 2007	Délibération autorisant la direction départementale de l'équipement de la Martinique à mettre en œuvre un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2007-054 21 mars 2007	Délibération portant autorisation de la mise en œuvre par la société Brevalex d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-055 21 mars 2007	Délibération portant refus d'autorisation de la mise en œuvre par la société Gestion Location Intervention Exploitation (GLIE) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-056 21 mars 2007	Délibération portant autorisation de la mise en œuvre par le port autonome de Bordeaux d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à un appontement pétrolier et gazier
2007-057 21 mars 2007	Délibération portant autorisation de la mise en œuvre par le Commissariat à l'énergie atomique d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au centre d'étude de Valduc
2007-058 25 avril 2007	Délibération portant avis sur un projet de décret en Conseil d'État relatif au groupement d'intérêt public pour la reconstitution des titres de propriété en Corse
2007-059 25 avril 2007	Délibération autorisant la mise en œuvre par la société Coinstar Money Transfert SAS d'un traitement automatisé ayant pour finalités la gestion des transferts internationaux d'argent, la lutte contre le blanchiment de capitaux et la gestion d'opérations de prospection commerciale
2007-060 25 avril 2007	Délibération modifiant l'autorisation unique n° AU-003 concernant 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
2007-061 25 avril 2007	Délibération autorisant la mise en œuvre par la société Connex Chambéry d'un traitement automatisé de données à caractère personnel AMARILIS pour la gestion des abonnements au service de transport en commun de Chambéry
2007-062 25 avril 2007	Délibération portant avis sur un projet de délibération de l'Agence française de lutte contre le dopage autorisant le traitement automatisé des données relatives à la localisation des sportifs soumis à des contrôles individualisés

2007-063 25 avril 2007	Délibération portant autorisation de mise en œuvre par le réseau Handident d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un dossier odontologique partagé
2007-064 25 avril 2007	Délibération portant autorisation de mise en œuvre par le centre hospitalier de Villefranche d'un partage d'informations médicales au travers du portail internet régional SIS Rhône-Alpes
2007-065 25 avril 2007	Délibération portant autorisation de mise en œuvre par le centre médical de Bayère d'un partage d'informations médicales au travers du portail internet régional SIS Rhône-Alpes
2007-066 25 avril 2007	Délibération portant autorisation de mise en œuvre par ACCOMIP-REPOP d'un système d'échange de données de santé dans le cadre d'un réseau de santé ville-hôpital de prévention et de prise en charge de l'obésité pédiatrique en Midi-Pyrénées
2007-067 25 avril 2007	Délibération portant autorisation de mise en œuvre par l'Association DIABÈTE 49 d'un système d'échange de données de santé dans le cadre d'un réseau de santé ville-hôpital
2007-068 25 avril 2007	Délibération portant autorisation de mise en œuvre par l'association Vie l'âge d'un dossier médical informatisé et partagé dans le cadre d'un réseau de santé
2007-069 25 avril 2007	Délibération portant autorisation de mise en œuvre par l'association Géronto-assistance d'un dossier médical informatisé et partagé dans le cadre d'un réseau de santé
2007-070 25 avril 2007	Délibération portant autorisation de mise en œuvre par le centre Eugène Marquis d'un système d'échange de données de santé dans le cadre de comités de concertation pluridisciplinaires pour la prise en charge de patients atteints d'un cancer
2007-071 25 avril 2007	Délibération portant autorisation de mise en œuvre par le CHU de Besançon d'un dossier médical informatisé et partagé en cancérologie dans le cadre du réseau régional de cancérologie ONCOLIE
2007-072 25 avril 2007	Délibération portant autorisation de mise en œuvre par le CHU de Rennes d'un dossier médical partagé pour chaque greffé dans le cadre du réseau de surveillance des transplantés hépatiques dénommé Prométhée
2007-073 25 avril 2007	Délibération portant autorisation de mise en œuvre par l'association pour le développement des prises en charge des troubles chroniques du sommeil d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un dossier médical partagé entre les professionnels de santé dans le cadre du réseau ville-hôpital Morphée
2007-074 25 avril 2007	Délibération portant autorisation de mise en œuvre par REUCARE d'un système d'échange de données de santé dans le cadre de comités de concertation pluridisciplinaires
2007-075 25 avril 2007	Délibération portant autorisation de mise en œuvre par l'association unité de concertation pluridisciplinaire en oncologie de la Vienne (UCPO 86) d'un dossier médical informatise et partage de suivi post-thérapeutique alterne en cancérologie
2007-076 25 avril 2007	Délibération portant autorisation de mise en œuvre par UNI-K d'un système d'échange de données de santé dans le cadre d'un dossier médical partagé et de réunions de concertation pluridisciplinaires
2007-077 25 avril 2007	Délibération portant autorisation de mise en œuvre par l'hôpital intercommunal de Neuville Fontaines d'un partage d'informations médicales au travers du portail internet régional SIS Rhône-Alpes
2007-078 25 avril 2007	Délibération portant autorisation de mise en œuvre par l'établissement hospitalisation à domicile soins et santé d'un partage d'informations médicales au travers du portail internet régional SIS Rhône-Alpes
2007-079 25 avril 2007	Délibération habilitant des agents de la CNIL à procéder à des vérifications

2007-080 25 avril 2007	Délibération autorisant la mise en œuvre par les hôpitaux universitaires de Strasbourg d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux blocs opératoires
2007-081 25 avril 2007	Délibération autorisant la mise en œuvre par la société Fenwick d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux chariots élévateurs
2007-082 25 avril 2007	Délibération autorisant la mise en œuvre par la SCP Regnard – Beder – Denfer & Bodet, titulaire de l'office de greffier du tribunal de commerce de Paris, à mettre en œuvre un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à la salle informatique
2007-083 25 avril 2007	Délibération refusant la mise en œuvre par la mairie de Metz d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à la salle informatique
2007-084 25 avril 2007	Délibération autorisant la mise en œuvre par la société Sanofi Pasteur d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au poste de pilotage des automates de production
2007-085 25 avril 2007	Délibération refusant la mise en œuvre par la société Solymatic France d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-086 25 avril 2007	Délibération autorisant la mise en œuvre par la société TNT Express France d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au centre de contrôle
2007-087 25 avril 2007	Délibération autorisant la mise en œuvre par la société Sogeti Infrastructure Services d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles
2007-088 25 avril 2007	Délibération autorisant la mise en œuvre par le Casino de la Baule d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles
2007-089 25 avril 2007	Délibération autorisant la mise en œuvre par la société Maguin SAS d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles
2007-090 25 avril 2007	Délibération autorisant la mise en œuvre par le service départemental d'incendie et de secours du Maine-et-Loire d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles
2007-091 25 avril 2007	Délibération refusant la mise en œuvre par l'Autorité de contrôle des assurances et des mutuelles (ACAM) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au réseau informatique (postes de travail fixes et portables)
2007-092 25 avril 2007	Délibération autorisant la mise en œuvre par le Casino du Nivernais d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles
2007-093 25 avril 2007	Délibération refusant la mise en œuvre par la société la société CSV International d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-094 3 mai 2007	Délibération portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel relatives à des passagers des aéroports français franchissant les frontières extérieures des États parties à la convention signée à Schengen le 19 juin 1990

2007-095 3 mai 2007	Délibération portant mise en demeure
2007-096 3 mai 2007	Délibération portant mise en demeure
2007-097 3 mai 2007	Délibération portant mise en demeure
2007-098 3 mai 2007	Délibération portant mise en demeure
2007-099 3 mai 2007	Délibération portant mise en demeure
2007-100 3 mai 2007	Délibération portant mise en demeure
2007-101 3 mai 2007	Délibération portant mise en demeure
2007-102 3 mai 2007	Délibération portant mise en demeure
2007-103 3 mai 2007	Délibération portant mise en demeure
2007-104 15 mai 2007	Délibération autorisant la mise en œuvre par la mairie de Roissy-en-France d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à la déchetterie
2007-105 15 mai 2007	Délibération autorisant la mise en œuvre par la société Bristish American Tobacco France d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux données stockées sur des clés USB
2007-106 15 mai 2007	Délibération portant autorisation des applications informatiques nécessaires à la mise en œuvre à titre expérimental du dossier pharmaceutique
2 007-107 24 mai 2007	Délibération portant avis sur un projet de décret en Conseil d'État portant création de deux traitements automatisés de données à caractère personnel pour l'expérimentation et l'exploitation de la constitution des listes électorales prud'homales en vue du scrutin du 3 décembre 2008.
2 007-108 24 mai 2007	Délibération portant avis sur un projet de décret en Conseil d'État relatif à certaines obligations d'information et de formation des travailleurs susceptibles d'être exposés aux rayonnements ionisants et à la prise en compte des compétences dévolues à l'autorité de sûreté nucléaire
2 007-109 24 mai 2007	Délibération portant avis sur le projet de décret en Conseil d'État présenté par le ministère de la justice relatif au placement sous surveillance électronique mobile pris en application des articles 763-13 et 763-14 du Code de procédure pénale
2 007-110 24 mai 2007	Délibération portant avis sur un projet de décret pris pour l'application du deuxième alinéa de l'article L. 611-3 du Code de l'entrée et du séjour des étrangers et du droit d'asile, portant création d'un traitement automatisé de données à caractère personnel des ressortissants étrangers qui font l'objet d'une mesure d'éloignement et modifiant la partie réglementaire de ce même code
2007-111 30 mai 2007	Délibération portant sanction
2007-112 30 mai 2007	Délibération portant sanction

2007-113 30 mai 2007	Délibération portant mise en demeure
2007-114 30 mai 2007	Délibération portant mise en demeure
2007-115 30 mai 2007	Délibération portant mise en demeure
2007-116 30 mai 2007	Délibération portant mise en demeure
2007-117 30 mai 2007	Délibération portant mise en demeure
2007-118 30 mai 2007	Délibération portant mise en demeure
2007-119 30 mai 2007	Délibération portant mise en demeure
2007-120 30 mai 2007	Délibération portant mise en demeure
2007-121 30 mai 2007	Délibération portant mise en demeure
2007-122 30 mai 2007	Délibération portant mise en demeure
2007-123 30 mai 2007	Délibération portant mise en demeure
2007-124 30 mai 2007	Délibération portant mise en demeure
2007-125 30 mai 2007	Délibération portant mise en demeure
2007-126 14 juin 2007	Délibération portant mise en demeure
2007-127 14 juin 2007	Délibération portant mise en demeure
2007-128 14 juin 2007	Délibération portant mise en demeure
2 007-129 14 juin 2007	Délibération portant mise en demeure
2007-130 14 juin 2007	Délibération portant mise en demeure
2007-131 14 juin 2007	Délibération portant mise en demeure
2007-132 14 juin 2007	Délibération portant mise en demeure
2007-133 14 juin 2007	Délibération portant mise en demeure

2007-134 14 juin 2007	Délibération portant mise en demeure
2007-135 14 juin 2007	Délibération portant mise en demeure
2007-136 14 juin 2007	Délibération portant avertissement
2007-137 21 juin 2007	Délibération autorisant la mise en œuvre par la société EMI France d'un traitement automatisé de données à caractère personnel ayant pour finalité le suivi des œuvres remises aux employés et à des tiers
2007-138 21 juin 2007	Délibération autorisant la mise en œuvre par la SARL Magic Form d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à un club de sport
2007-139 21 juin 2007	Délibération autorisant la mise en œuvre par la société Sanofi Aventis d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux données stockées sur des clés USB
2007-140 21 juin 2007	Délibération autorisant la mise en œuvre par la compagnie financière Edmond de Rothschild Banque d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux postes de travail informatiques
2007-141 21 juin 2007	Délibération autorisant la mise en œuvre par la CPAM de Sélestat d'un traitement automatisé de données à caractère personnel ayant pour finalité le suivi des signalements concernant les assurés, employeurs ou professionnels de santé dans le cadre du suivi des fraudes et anomalies
2007-142 21 juin 2007	Délibération autorisant la mise en œuvre par la caisse régionale d'assurance-maladie de Rhône-Alpes d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des dossiers des personnes victimes d'accidents du travail ou de maladies professionnelles dans lesquels la faute inexcusable de l'employeur a été retenue
2007-143 21 juin 2007	Délibération autorisant la mise en œuvre par la caisse régionale d'assurance-maladie de Rhône-Alpes d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des recours des assurés sociaux contre les décisions de rejet de leur demande de reconnaissance d'inaptitude au travail, dans le cadre du contentieux technique de la sécurité sociale
2007-144 21 juin 2007	Délibération autorisant la mise en œuvre par la SNCF d'un nouvel abonnement intitulé « e-forfait » pour le traitement automatisé de données à caractère personnel ayant pour finalité la gestion de la clientèle
2007-145 21 juin 2007	Délibération autorisant la communauté d'agglomération de la région nazairienne et de l'estuaire (CARENE) à mettre en œuvre un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2007-146 21 juin 2007	Délibération autorisant la mise en œuvre d'un dispositif biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès au Casino du Cap d'Agde
2007-147 21 juin 2007	Délibération portant avis sur un projet d'arrêté du ministère de l'Intérieur, de l'Outre-Mer et des Collectivités territoriales relatif à la création du téléservice Télépoints permettant la consultation par internet du solde des points affectés au permis de conduire et relatif à la modification du Système National des Permis de Conduire (SNPC)

2007-148 21 juin 2007	Délibération autorisant la mise en œuvre par la société Citibank International PLC d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des droits d'accès des employés aux différentes applications métier internes à l'établissement (autorisation n° 1215076)
2007-149 21 juin 2007	Délibération autorisant la mise en œuvre par la société Citibank International PLC d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion du recrutement externe et interne au sein de Citigroup (autorisation n° 1227075)
2007-150 21 juin 2007	Délibération autorisant la mise en œuvre par la société Citibank International PLC d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des rémunérations fixes et variables du personnel de Citibank en France (autorisation n° 1226654)
2007-151 21 juin 2007	Délibération autorisant la mise en œuvre par la société Citibank International PLC d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des dossiers des employés de l'établissement (autorisation n° 1215071)
2007-152 21 juin 2007	Délibération autorisant la mise en œuvre par la société Citigroup Global Markets Limited d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des droits d'accès accordés aux employés à différentes applications métier internes à l'établissement (autorisation n° 1206399)
2007-153 21 juin 2007	Délibération autorisant la mise en œuvre par la société Compagnie IBM France d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion de la paie et celle du personnel (autorisation n° 780791)
2007-154 21 juin 2007	Délibération autorisant la mise en œuvre par la société Netcentrex d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des ressources humaines (autorisation n° 1231531)
2007-155 21 juin 2007	Délibération autorisant la mise en œuvre par la société Parker Hanninfin France SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité le suivi des entretiens annuels et des objectifs pour le personnel cadre (autorisation n° 1202833)
2007-156 21 juin 2007	Délibération autorisant la mise en œuvre par la société Pionner Genetique SARL d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des achats et des relations avec les fournisseurs et prestataires de services (autorisation n° 1224501)
2007-157 21 juin 2007	Délibération autorisant la mise en œuvre par la société Pionner Genetique SARL d'un transfert de données à caractère personnel hors de l'Union européenne pour finalité la gestion de la paie et des ressources humaines relatives aux salariés et au personnel intérimaire (autorisation n° 1221497)
2007-158 21 juin 2007	Délibération autorisant la mise en œuvre par la société Pioneer Semences SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion de la paie et des ressources humaines relatives aux salariés et personnel intérimaire (autorisation n° 1221503)
2007-159 21 juin 2007	Délibération autorisant la mise en œuvre par la société Pioneer Semences SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des achats et des relations avec les fournisseurs (autorisation n° 1224498)
2007-160 21 juin 2007	Délibération autorisant la mise en œuvre par la société Sun Microsystems France SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion du personnel (autorisation n° 1224746)
2007-161 21 juin 2007	Délibération autorisation la mise en œuvre par la société Sun Microsystems France SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité le recensement des collaborateurs cocontractants, présents dans les locaux de Sun Microsystems mais non rémunérés par Sun Microsystems (autorisation n° 1224771)

2007-162 21 juin 2007	Délibération autorisant la mise en œuvre par la société Texas Instruments France d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité le remboursement des notes de frais (autorisation n° 1217905)
2007-163 21 juin 2007	Délibération autorisant la mise en œuvre par la société Texas Instruments France d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des tâches des personnels, la comptabilité et la gestion des projets (autorisation n° 1219090)
2007-164 21 juin 2007	Délibération autorisant la mise en œuvre par la société UNILEVER FRANCE SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalités l'externalisation de la gestion des ressources humaines, ainsi que le traitement de la paie, à la société prestataire Accenture (autorisation n° 1212123)
2007-165 21 juin 2007	Délibération autorisant la mise en œuvre par la société ABN AMRO BANK N.V. d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité de fournir un outil permettant de gérer le helpdesk (autorisation n° 1038036)
2007-166 21 juin 2007	Délibération autorisant la mise en œuvre par la société ABN AMRO Corporate Finance France d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité de fournir un outil central permettant de gérer le *helpdesk* (autorisation n° 1038038)
2007-167 21 juin 2007	Délibération autorisant la mise en œuvre par la société BNP PARIBAS d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1203604)
2007-168 21 juin 2007	Délibération autorisant la mise en œuvre par la société Compagnie financière ALCATEL d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité le *reporting* sur des données administratives liées aux ressources humaines (autorisation n° 1204047)
2007-169 21 juin 2007	Délibération autorisant la mise en œuvre par la société ESSO SA française d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des contacts clients et prospects (autorisation n° 1144850)
2007-170 21 juin 2007	Délibération autorisant la mise en œuvre par la société GIE ABN AMRO Rothschild d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité de fournir un outil central permettant de gérer le *helpdesk* (autorisation n° 1039691)
2007-171 21 juin 2007	Délibération autorisant la mise en œuvre par la société Sealed Air Packaging SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité le calcul des rémunérations et de leurs accessoires (autorisation n° 1141000)
2007-172 21 juin 2007	Délibération autorisant la mise en œuvre par la société Sealed Air SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité l'hébergement des informations (autorisation n° 1140999)
2007-173 21 juin 2007	Délibération autorisant la mise en œuvre par la société ARIBA France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1221251)
2007-174 21 juin 2007	Délibération autorisant la mise en œuvre par la société AXON' CABLE SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des clients et des prospects (autorisation n° 1183578)
2007-175 21 juin 2007	Délibération autorisant la mise en œuvre par la société Pioneer Semences SAS d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité de permettre la gestion des relations commerciales avec les clients directs (distributeurs), les utilisateurs finaux (agriculteurs), et les prospects (autorisation n° 1221484)
2007-176 21 juin 2007	Délibération autorisant la mise en œuvre au sein du groupe CETELEM de transferts d'informations hors de l'Union européenne et ayant pour finalité la gestion électronique de documents et de courriers (autorisation n° 1232789)

2007-177 21 juin 2007	Délibération autorisant la mise en œuvre par la société Hosta SA d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion de l'assurance-maladie complémentaire et le remboursement des prestations aux assurés (autorisation n° 834195)
2007-178 21 juin 2007	Délibération autorisant la mise en œuvre par la société Chubb Insurance Company of Europe SA (succursale française) d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la souscription et la gestion des contrats ainsi que le traitement du dossier en cas de sinistre (autorisation n° 1217340)
2007-179 21 juin 2007	Délibération autorisant la mise en œuvre par la société Chubb Insurance Company of Europe SA (succursale française) d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité le suivi et la gestion des paiements et des encaissements (autorisation n° 1217309)
2007-180 21 juin 2007	Délibération autorisant la mise en œuvre par la société Chubb Insurance Company of Europe SA (succursale française) d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité de centraliser et répertorier les informations relatives aux employés (autorisation n° 1217339)
2007-181 21 juin 2007	Délibération autorisant la mise en œuvre par la société Chubb Insurance Company of Europe SA (succursale française) d'un transfert de données à caractère personnel hors de l'Union européenne et ayant pour finalité la gestion des risques étudiés, déclinés, résiliés (autorisation n° 1217338)
2007-182	Délibération annulée
2007-183 28 juin 2007	Délibération portant mise en demeure
2007-184 28 juin 2007	Délibération portant mise en demeure
2007-185 28 juin 2007	Délibération portant mise en demeure
2007-186 28 juin 2007	Délibération portant sanction
2007-187 10 juillet 2007	Délibération relative à une proposition d'avertissement
2007-188 10 juillet 2007	Délibération autorisant la mise en œuvre par Mutuosportsanté d'un dossier médical partagé pour les joueurs, les entraîneurs, les accompagnants et les arbitres de la coupe du monde de rugby 2007
2007-189 10 juillet 2007	Délibération autorisant la 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 la constitution d'un répertoire partagé des professionnels de santé (RPPS)
2007-190 10 juillet 2007	Délibération modifiant la délibération n° 04-074 du 21 septembre 2004 et la délibération n° 2006-257 du 5 décembre 2006 relatives aux traitements de données à caractère personnel mis en œuvre par les collectivités locales à partir des données cadastrales
2007-191 10 juillet 2007	Délibération refusant la mise en œuvre par la société Infobail d'un traitement automatisé de données à caractère personnel intitulé « le fichier des impayés locatifs » pour la gestion des impayés par les locataires d'immeubles d'habitation
2007-192 10 juillet 2007	Délibération refusant la mise en œuvre par la société Infobail d'un traitement automatisé de données à caractère personnel intitulé « le fichier des locataires confiance » pour le recensement des locataires d'immeubles d'habitation respectant leurs obligations de paiement

2007-193 10 juillet 2007	Délibération portant avis sur le projet d'arrêté du directeur général des douanes et des droits indirects du ministère de l'Économie, des Finances et de l'Industrie relatif au fichier d'identification des dossiers d'enquêtes douanières (FIDE)
2007-194 10 juillet 2007	Délibération autorisant la mise en place généralisée par la Caisse nationale d'assurance-maladie des travailleurs salariés d'un traitement permettant aux médecins d'accéder aux données relatives aux prestations servies aux bénéficiaires de l'assurance-maladie
2007-195 10 juillet 2007	Délibération portant avis sur le projet de décret pris pour l'application de l'article L. 611-6 du Code de l'entrée et du séjour des étrangers et du droit d'asile, portant création d'un traitement automatisé de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa et modifiant la partie réglementaire de ce même code
2007-196 10 juillet 2007	Délibération portant avis sur un projet d'arrêté interministériel portant création d'un dispositif dénommé « système de pesée en marche (SPM) » permettant de contrôler en marche certains véhicules de transports routiers
2007-197 10 juillet 2007	Délibération portant avis sur le projet d'arrêté du ministère de l'intérieur créant le fichier national des interdits de stade (FNIS)
2007-198 10 juillet 2007	Délibération portant avis sur un projet de décret en Conseil d'État pris pour l'application de l'article L. 131-6 du Code de l'éducation et portant sur le traitement automatisé de données à caractère personnel relatif au recensement des enfants soumis à l'obligation scolaire et à l'amélioration du suivi de l'obligation d'assiduité scolaire
2007-199 10 juillet 2007	Délibération autorisant la mise en œuvre par le groupe des fromageries Bel d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation des empreintes digitales des employés dans le cadre d'une opération de sponsoring
2007-200 10 juillet 2007	Délibération autorisant la direction départementale de l'équipement de la Loire-Atlantique à mettre en œuvre un système d'information géographique à partir des données cadastrales
2007-201 10 juillet 2007	Délibération autorisant la direction départementale de l'équipement du Maine-et-Loire à mettre en œuvre un système d'information géographique à partir des données cadastrales
2007-202 10 juillet 2007	Délibération autorisant la direction départementale de l'équipement de la Mayenne à mettre en œuvre un système d'information géographique à partir des données cadastrales
2007-203 10 juillet 2007	Délibération autorisant la direction départementale de l'équipement de la Sarthe à mettre en œuvre un système d'information géographique à partir des données cadastrales
2007-204 10 juillet 2007	Délibération autorisant la direction départementale de l'équipement de la Vendée à mettre en œuvre un système d'information géographique à partir des données cadastrales
2007-205 10 juillet 2007	Délibération autorisant la mise en œuvre par le réseau ONCAZUR d'un système d'échange de données de santé dans le cadre de comités de concertation pluridisciplinaires
2007-206 10 juillet 2007	Délibération autorisant la mise en œuvre par le réseau ONCO 92 SUD d'un système d'échange de données de santé dans le cadre de comités de concertation pluridisciplinaires
2007-207 10 juillet 2007	Délibération autorisant la mise en œuvre par le Centre hospitalier universitaire de Dijon d'un système d'évaluation de la qualité, l'efficacité et du coût de la prise en charge des nouveau-nés à risque de déficience et de handicap nés en région périnatale de Bourgogne
2007-208 10 juillet 2007	Délibération autorisant la mise en œuvre par le centre René Huguenin de lutte contre le cancer d'un système de partage de données de santé entre dans le cadre d'un réseau ville-hôpital
2007-209 10 juillet 2007	Délibération autorisant la mise en œuvre par le Centre hospitalier Pierre Nouveau de Cannes d'un système de partage de données de santé dans le cadre d'un réseau ville-hôpital

2007-210 10 juillet 2007	Délibération autorisant la mise en œuvre par le réseau de génétique Île-de-France Ouest d'un traitement de données à caractère personnel ayant pour finalité l'amélioration du diagnostic des maladies génétiques par la création de dossiers médicogénétiques partagés
2007-211 10 juillet 2007	Délibération autorisant la mise en œuvre par l'association RESOPAL Dieppe d'un traitement de données à caractère personnel ayant pour finalité la coordination des soins palliatifs à domicile
2007-212 10 juillet 2007	Délibération autorisant la mise en œuvre par l'hôpital local d'Amplepuis d'un partage d'informations médicales au travers du portail internet régional SIS Rhône-Alpes
2007-213 10 juillet 2007	Délibération autorisant la mise en œuvre par le centre hospitalier de Saint Joseph-Saint Luc d'un partage d'informations médicales au travers du portail internet régional SIS Rhône-Alpes
2007-214 10 juillet 2007	Délibération autorisant la mise en œuvre par l'Institut d'histopathologie d'une transmission des comptes rendus d'anatomopathologie des patients pris en charge dans le cadre du réseau ONCO Pays de la Loire au travers d'un dossier de cancérologie partagé
2007-215 10 juillet 2007	Délibération autorisant la mise en œuvre par la Haute Autorité de lutte contre les discriminations et pour l'égalité d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des réclamations qui lui sont adressées
2007-216 10 juillet 2007	Délibération autorisant la mise en œuvre, par le ministère de l'Économie, des Finances et de l'Industrie, d'un traitement automatisé de données à caractère personnel ayant pour objet l'identification des contribuables, dénommé PERS
2007-217 10 juillet 2007	Délibération autorisant la mise en œuvre par la société Pitney Bowes Management Services SAS d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1115318)
2007-218 10 juillet 2007	Délibération autorisant la mise en œuvre par la société SECAP – groupe Pitney Bowes d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1093110)
2007-219 10 juillet 2007	Délibération autorisant la mise en œuvre par la société Technopli SARL d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1105323)
2007-220 10 juillet 2007	Délibération autorisant la mise en œuvre par la société Debevoise & Plimpton LLP de transferts de données à caractère personnel hors de l'Union européenne (autorisation n° 1238276)
2007-221 10 juillet 2007	Délibération autorisant la mise en œuvre par la Société française du radiotéléphone (SFR) d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1238736)
2007-222 10 juillet 2007	Délibération autorisant la mise en œuvre par AXA Assistance France d'un transfert d'informations hors de l'Union européenne (autorisation n° 1217876)
2007-223 10 juillet 2007	Délibération autorisant la mise en œuvre par AXA Assurances IARD Mutuelle d'un transfert d'informations hors de l'Union européenne (autorisation n° 1231077)
2007-224 10 juillet 2007	Délibération autorisant la mise en œuvre par AXA France IARD d'un transfert d'informations hors de l'Union européenne (autorisation n° 1231082)
2007-225 10 juillet 2007	Délibération autorisant la mise en œuvre par AXA Assurance Vie Mutuelle d'un transfert d'informations hors de l'Union européenne (autorisation n° 1231085)
2007-226 10 juillet 2007	Délibération autorisant la mise en œuvre par AXA France Vie d'un transfert d'informations hors de l'Union européenne (autorisation n° 1231100)
2007-227 10 juillet 2007	Délibération autorisant la mise en œuvre au sein du GE Money Outre-mer d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1238266)
2007-228 10 juillet 2007	Délibération portant mise en demeure

2007-229 10 juillet 2007	Délibération portant mise en demeure
2007-230 10 juillet 2007	Délibération portant mise en demeure
2007-231 10 juillet 2007	Délibération portant mise en demeure
2007-232 10 juillet 2007	Délibération portant mise en demeure
2007-233 14 juin 2007	Délibération portant avertissement
2007-234 13 septembre 2007	Délibération autorisant la mise en œuvre par le CHU de Grenoble d'un système d'échange de données de santé
2007-235 13 septembre 2007	Délibération autorisant la mise en œuvre par l'Association soins de suite 45 d'un dossier médical partagé afin d'améliorer l'orientation des patients dans le système de soins
2007-236 13 septembre 2007	Délibération autorisant la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES) du ministère de la Santé, de la Jeunesse et des Sports à mettre en œuvre les traitements automatisés de données à caractère personnel nécessaires à la réalisation d'une enquête statistique sur le recours aux spécialistes en médecine de ville
2007-237 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Philipp Morris France SAS d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation 831679)
2007-238 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Hewlett Packard France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation 1240356)
2007-239 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Hewlett Packard France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation 1241293)
2007-240 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Sybase France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation)
2007-241 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Sybase France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation)
2007-242 13 septembre 2007	Délibération autorisant la mise en œuvre par le centre régional des moyens techniques de la Lyonnaise des Eaux de Bordeaux d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2007-243 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Fleet Logistics France SAS d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1224004)
2007-244 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Fleet Logistics France SAS d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1224007)
2007-245 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Fleet Logistics France SAS d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1224545)
2007-246 13 septembre 2007	Délibération autorisant la mise en œuvre par l'Association française pour le nommage internet en coopération (AFNIC) d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'une liste d'exclusion afin de lutter contre les violations de la Charte de nommage du « .fr » de l'AFNIC
2007-247 13 septembre 2007	Délibération portant autorisation de la mise en œuvre par la société Glaces Thiriet SAS d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux postes informatiques

2007-248 13 septembre 2007	Délibération relatif à la mise en œuvre par la manufacture française de pneumatique Michelin d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance vocale et ayant pour finalité la gestion des mots de passe
2007-249 13 septembre 2007	Délibération refusant la mise en œuvre par la société d'économie mixte des transports urbains de la Sambre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de la prise de service par les agents de conduite
2007-250 13 septembre 2007	Délibération refusant la mise en œuvre par la SBP Audit & Expertise d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-251 13 septembre 2007	Délibération autorisant la mise en œuvre par la société Sanofi-Aventis Recherche & Développement d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-252 13 septembre 2007	Délibération autorisant la mise en œuvre par le Réseau de transport d'électricité d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au centre régional de conduite Est
2007-253 13 septembre 2007	Délibération refusant la mise en œuvre par le centre médical de Forcilles d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-254 13 septembre 2007	Délibération refusant la mise en œuvre par la société Écureuil Lease d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-255 13 septembre 2007	Délibération refusant la mise en œuvre par la société Delami SAS d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-256 13 septembre 2007	Délibération autorisant la mise en œuvre par le centre interrégional du traitement de l'information de Lyon d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au centre informatique
2007-257 13 septembre 2007	Délibération refusant la mise en œuvre par la chambre départementale d'agriculture des Pyrénées-Orientales d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-258 13 septembre 2007	Délibération refusant la mise en œuvre par la société Beuralia d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-259 13 septembre 2007	Délibération refusant la mise en œuvre par la société AKDEV d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité la gestion des horaires de travail
2007-260 13 septembre 2007	Délibération refusant la mise en œuvre par la société Atlas Copco France Holding d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles
2007-261 13 septembre 2007	Délibération refusant la mise en œuvre par la société CCV Beaumanoir d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-262 13 septembre 2007	Délibération refusant la mise en œuvre par la CPAM d'Armentières d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles

2007-263 13 septembre 2007	Délibération refusant la mise en œuvre par la société Kreek's France Arachides d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des horaires
2007-264 13 septembre 2007	Délibération refusant la mise en œuvre par la société Serare (enseigne Courtepaille) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux caisses
2007-265 13 septembre 2007	Délibération refusant la mise en œuvre par la société Synergie Cad d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles
2007-266 13 septembre 2007	Délibération refusant la mise en œuvre par la Société nouvelle des Galeries Lafayette d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-267 13 septembre 2007	Délibération autorisant la mise en œuvre par la mairie de Le Cannet d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles
2007-268 20 septembre 2007	Délibération refusant la mise en œuvre par la société CCI Conseils d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-269 20 septembre 2007	Délibération autorisant la mise en œuvre par la société Laboratoire Renaudin d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-270 20 septembre 2007	Délibération autorisant la mise en œuvre par la communauté d'agglomération de la vallée de Montmorency d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-271 20 septembre 2007	Délibération autorisant la mise en œuvre par la Caisse nationale militaire de sécurité sociale d'un traitement automatisé de données à caractère personnel ayant pour finalité de permettre aux médecins d'accéder à l'historique des remboursements des ressortissants de la Caisse
2007-272 20 septembre 2007	Délibération autorisant la mise en œuvre par la société AXA Assurance Vie Mutuelle d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1246212)
2007-273 20 septembre 2007	Délibération autorisant la mise en œuvre par la société AXA France Vie d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1246215)
2007-274 20 septembre 2007	Délibération autorisant la mise en œuvre par la société GE Energy Products France SNC d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1248208)
2007-275 20 septembre 2007	Délibération portant habilitation d'agents de la CNIL à procéder à des vérifications
2007-276 20 septembre 2007	Délibération autorisant la mise en œuvre par la société General Motors Strasbourg SAS d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1220559)
2007-277 20 septembre 2007	Délibération autorisant la mise en œuvre par la société Chevron France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1237044)
2007-278 20 septembre 2007	Délibération autorisant la mise en œuvre par la société Fuel and Marine Marketing France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1238977)
2007-279 20 septembre 2007	Délibération autorisant la mise en œuvre par la société Chevron Antilles Guyane Française d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1238976)
2007-280 20 septembre 2007	Délibération autorisant la mise en œuvre par la société Antillaise des Pétroles Chevron d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1238974)

2007-281 20 septembre 2007	Délibération autorisant la mise en œuvre par la société Chevron Réunion Ltd d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1245990)
2007-282 20 septembre 2007	Délibération autorisant la mise en œuvre par la Société de Transport Macé – Hydrotrans d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1245992)
2007-283 20 septembre 2007	Délibération autorisant la mise en œuvre par la société de transport Texaco – Sorotex d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1245995)
2007-284 20 septembre 2007	Délibération autorisant la mise en œuvre par la Société de Transport de Gaz d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1245998)
2007-285 20 septembre 2007	Délibération autorisant la mise en œuvre par la mutuelle d'épargne, de retraite et de prévoyance CARAC d'un traitement de données à caractère personnel ayant pour finalité la lutte contre le blanchiment de capitaux et le financement du terrorisme (autorisation n° 1134399)
2007-286 20 septembre 2007	Délibération portant mise en demeure
2007-287 20 septembre 2007	Délibération portant mise en demeure
2007-288 20 septembre 2007	Délibération portant mise en demeure
2007-289 20 septembre 2007	Délibération portant mise en demeure
2007-290 20 septembre 2007	Délibération portant mise en demeure
2007-291 20 septembre 2007	Délibération portant mise en demeure
2007-292 20 septembre 2007	Délibération portant mise en demeure
2007-293 20 septembre 2007	Délibération portant mise en demeure
2007-294 20 septembre 2007	Délibération portant avertissement
2007-295 4 octobre 2007	Délibération portant avis sur un projet d'arrêté du ministre de l'Économie, des Finances et de l'Industrie modifiant l'arrêté du 14 juin 1982 relatif à l'extension d'un système automatisé de gestion du fichier des comptes bancaires (FICOBA)
2007-296 4 octobre 2007	Délibération autorisant la mise en œuvre par le Groupe des écoles des télécommunications (GET) (société INT Évry) d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance de diverses données biométriques
2007-297 4 octobre 2007	Délibération autorisant la mise en œuvre par la société Stäubli Technology & Services d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2007-298 11 octobre 2007	Délibération autorisant la mise en œuvre par l'Association de lutte contre la piraterie audiovisuelle d'un traitement automatisé de données à caractère personnel ayant pour finalité la réalisation de statistiques concernant la circulation des œuvres audiovisuelles sur les réseaux d'échanges de fichiers dits de « pair à pair »

2007-299 11 octobre 2007	Délibération autorisant la mise en œuvre par l'établissement français du sang de traitements automatisés de données à caractère personnel ayant pour finalité la gestion des processus métiers et notamment la gestion des donneurs et receveurs de sang
2007-300 11 octobre 2007	Délibération portant avis sur un projet de décret en Conseil d'État présenté par le ministre délégué à l'énergie et aux matières premières relatif à la procédure applicable en cas d'impayés des factures d'électricité, de gaz, de chaleur ou d'eau
2007-301 11 octobre 2007	Délibération portant avis sur un projet d'arrêté relatif à la mise en place d'un traitement de données à caractère personnel dénommé « Service de consultation du plan cadastral – SCPC »
2007-302 25 octobre 2007	Délibération portant avertissement
2007-303 25 octobre 2007	Délibération portant mise en demeure
2007-304 25 octobre 2007	Délibération portant mise en demeure
2007-305 25 octobre 2007	Délibération portant mise en demeure
2007-306 25 octobre 2007	Délibération portant mise en demeure
2007-307 25 octobre 2007	Délibération portant mise en demeure
2007-308 25 octobre 2007	Délibération portant mise en demeure
2007-309 25 octobre 2007	Délibération portant mise en demeure
2007-310 25 octobre 2007	Délibération portant mise en demeure
2007-311 25 octobre 2007	Délibération portant mise en demeure
2007-312 25 octobre 2007	Délibération portant mise en demeure
2007-313 25 octobre 2007	Délibération portant mise en demeure
2007-314 25 octobre 2007	Délibération autorisant la mise en œuvre par la société Orange Réunion d'un traitement de données à caractère personnel ayant pour finalité la prévention des impayés
2007-315 25 octobre 2007	Délibération autorisant la mise en œuvre par la société Réunionnaise du Radiotéléphone d'un traitement de données à caractère personnel ayant pour finalité la prévention des impayés
2007-316 25 octobre 2007	Délibération autorisant la mise en œuvre par la société AXA France Vie d'un transfert de données à caractère personnel hors de l'Union européenne
2007-317 25 octobre 2007	Délibération autorisant la mise en œuvre par la société AXA France IARD d'un transfert de données à caractère personne hors de l'Union européenne
2007-318 25 octobre 2007	Délibération portant autorisation unique des traitements de données à caractère personnel mis en œuvre par les sociétés d'assurance du groupe GMF dont la finalité est la lutte contre le blanchiment de capitaux et le financement du terrorisme

2007-319 25 octobre 2007	Délibération autorisant la mise en œuvre par HSBC France d'un transfert de données à caractère personnel hors de l'Union européenne
2007-320 25 octobre 2007	Délibération autorisant la mise en œuvre par la société AXA France IARD d'un transfert de données à caractère personnel hors de l'Union européenne
2007-321 25 octobre 2007	Délibération autorisant la mise en œuvre par la société AXA France Vie d'un transfert de données à caractère personnel hors de l'Union européenne
2007-322 25 octobre 2007	Délibération portant sanction
2007-323 25 octobre 2007	Délibération portant mise en demeure
2007-324 25 octobre 2007	Délibération autorisant la mise en œuvre par la fédération du crédit mutuel d'Île-de-France d'un traitement automatisé de données à caractère personnel dénommé DIANE au titre de la lutte contre la Fraude à la Carte Bancaire
2007-325 25 octobre 2007	Délibération autorisant la mise en œuvre par le crédit Industriel et Commercial d'un traitement automatise de données à caractère personnel dénommé DIANE au titre de la lutte contre la fraude à la carte bancaire
2007-326 8 novembre 2007	Délibération portant avis sur un projet de décret modificatif relatif au Fichier judiciaire automatisé des auteurs d'infractions sexuelles (FIJAIS)
2007-327 8 novembre 2007	Délibération autorisant la mise en œuvre par la société NRJ Mobile d'un traitement de données à caractère personnel ayant pour finalité la prévention des impayés
2007-328 8 novembre 2007	Délibération autorisant la mise en œuvre par le centre Jean Perrin d'un partage d'informations relatives à la transfusion sanguine en Auvergne – Loire, réseau EDITAL
2007-329 8 novembre 2007	Délibération autorisant la mise en œuvre par la Caisse nationale du régime social des indépendants d'un traitement automatisé de données à caractère personne ayant pour finalité de permettre aux médecins d'accéder à l'historique des remboursements de leurs adhérents
2007-330 8 novembre 2007	Délibération autorisant la mise en œuvre par la Caisse centrale de mutualité sociale Agricole d'un traitement automatisé de données à caractère personnel ayant pour finalité de permettre aux médecins d'accéder à l'historique des remboursements des adhérents de la Mutualité sociale agricole
2007-331 8 novembre 2007	Projet de délibération autorisant la mise en œuvre par la Mutualité Fonction Publique Service d'un traitement automatisé de données à caractère personnel permettant aux médecins d'accéder à l'historique des remboursements des adhérents de la mutualité Fonction publique
2007-332 8 novembre 2007	Délibération autorisant le transfert hors de l'Union européenne par HSBC France de données à caractère personnel au titre de la sous-traitance de la gestion administrative des confirmations de transactions (demande d'autorisation n° 1260218)
2007-333 8 novembre 2007	Délibération autorisant la mise en œuvre par la cité des Télécoms Fondation d'entreprise d'un traitement de données à caractère personnel ayant pour finalité l'expérimentation de dispositifs biométriques dans le cadre d'une exposition pédagogique
2007-334 8 novembre 2007	Délibération autorisant la mise en œuvre par la Société civile des producteurs phonographiques d'un traitement de données à caractère personnel ayant pour finalité la recherche et la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés *peer to peer* (autorisation n° 1090042)
2007-335 8 novembre 2007	Délibération autorisant la mise en œuvre par la société Hitachi Europe SAS d'un traitement de données à caractère reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès au système d'information (autorisation n° 1242571)

2007-336 8 novembre 2007	Délibération autorisant la mise en œuvre par la société Hitachi Software Engineering France SAS d'un traitement de données à caractère reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux (autorisation n° 1243325)
2007-337 8 novembre 2007	Délibération autorisant la mise en œuvre par la société Horanet Services & Diffusion d'un traitement de données à caractère reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux (autorisation n° 1245435)
2007-338 8 novembre 2007	Délibération autorisant la mise en œuvre par la société Études et développement en électronique numérique (EDEN) d'un traitement de données à caractère reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux
2007-339 8 novembre 2007	Délibération autorisant la mise en œuvre par la société Hitachi Data Systems d'un traitement de données à caractère reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès au système d'information (autorisation n° 1248197)
2007-340 22 novembre 2007	Délibération autorisant la société INITIAL BTB à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle
2007-341 22 novembre 2007	Délibération autorisant le groupement d'intérêt économique ELIS (GIE ELIS) à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle
2007-342 22 novembre 2007	Délibération autorisant la mise en œuvre par la société Téléroute France d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux postes informatiques (autorisation n° 1176947)
2007-343 22 novembre 2007	Délibération autorisant la mise en œuvre par la société Wolters Kluwer France d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux postes informatiques (autorisation n° 1176668)
2007-344 22 novembre 2007	Délibération autorisant la mise en œuvre par le centre hospitalier de Sainte Foy-lès-Lyon d'un partage d'informations médicales au travers du portail internet régional SIS Rhône-Alpes
2007-345 22 novembre 2007	Délibération autorisant la mise en œuvre par la société AXA Assistance France d'un transfert de données à caractère personnel hors de l'Union européenne à des fins de sous-traitance de la communication des coordonnées de prestataires à ses clients
2007-346 22 novembre 2007	Délibération autorisant la direction de l'agriculture et de la forêt de Guadeloupe à mettre en œuvre un système d'information géographique à partir des données cadastrales
2007-347 22 novembre 2007	Délibération autorisant la mise en œuvre par le réseau de cancérologie de Champagne-Ardenne ONCOCHA d'un dossier médical informatisé et partagé en cancérologie (DCC)
2007-348 22 novembre 2007	Délibération autorisant 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 finalité la recherche et la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés *peer to peer* (autorisation n° 1091623)
2007-349 22 novembre 2007	Délibération autorisant 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 la recherche et la constatation des délits de contrefaçon commis *via* les réseaux d'échanges de fichiers dénommés *peer to peer* (autorisation n° 1091622)
2007-350 22 novembre 2007	Délibération autorisant la mise en œuvre par la société BP France SA d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1061420)
2007-351 22 novembre 2007	Délibération autorisant la mise en œuvre par la société ADP GSI France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1180050)

2007-352 22 novembre 2007	Délibération portant sanction
2007-353 22 novembre 2007	Délibération portant mise en demeure
2007-354 22 novembre 2007	Délibération portant mise en demeure
2007-355 22 novembre 2007	Délibération portant mise en demeure
2007-356 22 novembre 2007	Délibération portant mise en demeure
2007-357 22 novembre 2007	Délibération portant mise en demeure
2007-358 22 novembre 2007	Délibération portant mise en demeure
2007-359 22 novembre 2007	Délibération portant mise en demeure
2007-360 22 novembre 2007	Délibération portant mise en demeure
2007-361 22 novembre 2007	Délibération portant mise en demeure
2007-362 22 novembre 2007	Délibération portant mise en demeure
2007-363 22 novembre 2007	Délibération portant mise en demeure
2007-364 29 novembre 2007	Délibération autorisant la mise en œuvre par LG Electronics France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1194761)
2007-365 29 novembre 2007	Délibération autorisant la mise en œuvre par LG Electronics Mobilecomm France d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1190581)
2007-366 29 novembre 2007	Délibération autorisant la mise en œuvre par le centre hospitalier de Tourcoing d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un réseau régional E-NADIS pour la prise en charge des patients infectés par le VIH et/ou par les hépatites B et C dans le Nord-Pas-de-Calais (autorisation n° 1251720)
2007-367 29 novembre 2007	Délibération portant prorogation de la phase expérimentale du dossier pharmaceutique
2007-368 11 décembre 2007	Délibération portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques
2007-369 11 décembre 2007	Délibération autorisant la mise en œuvre par l'Assistance publique-Hôpitaux de Paris d'un dispositif de signalement et de suivi des événements indésirables et de gestion des risques dénommé OSIRIS
2007-370 11 décembre 2007	Délibération autorisant la mise en œuvre par la caisse nationale d'assurance-maladie des travailleurs salariés d'une base de données transitoire comportant des données à caractère personnel ayant pour finalité l'accompagnement des personnes atteintes de maladies chroniques : expérimentation sur le diabète (autorisation n° 1261011)

2007-371 11 décembre 2007	Délibération autorisant la mise en œuvre par le Syndicat mixte départemental des massifs Concors Sainte-Victoire d'un système d'information géographique à partir des données cadastrales et des données de suivi du débroussaillement obligatoire (autorisation n° 1224896)
2007-372 11 décembre 2007	Délibération autorisant la mise en œuvre par la direction de la recherche, des études, de l'évaluation et des statistiques (DREES) de traitements de données à caractère personnel nécessaires à la réalisation d'études statistiques portant sur les revenus complets des professionnels de santé libéraux (autorisation n° 1245131)
2007-373 11 décembre 2007	Délibération autorisant la mise en œuvre par la société Compagnie IBM France SAS d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 760180)
2007-374 11 décembre 2007	Délibération portant sanction
2007-375 11 décembre 2007	Délibération portant mise en demeure
2007-376 11 décembre 2007	Délibération portant mise en demeure
2007-377 11 décembre 2007	Délibération portant mise en demeure
2007-378 11 décembre 2007	Délibération portant mise en demeure
2007-379 11 décembre 2007	Délibération portant mise en demeure
2007-380 11 décembre 2007	Délibération portant mise en demeure
2007-381 11 décembre 2007	Délibération portant mise en demeure
2007-382 11 décembre 2007	Délibération portant mise en demeure
2007-383 11 décembre 2007	Délibération portant mise en demeure
2007-384 11 décembre 2007	Délibération portant mise en demeure
2007-385 11 décembre 2007	Délibération portant mise en demeure
2007-386 11 décembre 2007	Délibération portant mise en demeure
2007-387 11 décembre 2007	Délibération portant mise en demeure
2007-388 11 décembre 2007	Délibération portant mise en demeure
2007-389 11 décembre 2007	Délibération portant mise en demeure
2007-390 20 décembre 2007	Délibération portant avis sur un projet d'arrêté portant création d'un traitement de numérisation des procédures pénales

2007-391 20 décembre 2007	Délibération portant avis sur le projet de décret pris pour l'application de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, et relatif à la conservation des données de nature à permettre l'identification de toute personne physique ou morale ayant contribué à la création d'un contenu mis en ligne
2007-392 20 décembre 2007	Délibération autorisant la mise en œuvre par le centre hospitalier Pierre Oudot d'un partage d'informations médicales au travers du portail internet régional SIS Rhône-Alpes
2007-393 20 décembre 2007	Délibération autorisant la mise en œuvre par la fondation VSHA Praz-Coutant d'un partage d'informations médicales au travers du portail internet régional sis Rhône-Alpes
2007-394 20 décembre 2007	Délibération autorisant la mise en œuvre par la société Tiffany & Compagny d'un transfert de données à caractère personnel hors de l'Union européenne (autorisation n° 1256295)
2007-395 20 décembre 2007	Délibération autorisant la mise en œuvre par les Hospices civils de Beaune d'un partage d'informations médicales au travers du portail d'accès ville-hôpital (autorisation n° 1222884)

LISTE DES SANCTIONS FINANCIÈRES EN 2007

	TYPE D'ORGANISME	MONTANT (en euros)	MANQUEMENT
Mars 2007	Opérateur de télécommunication	10000	Refus de droit d'accès
Mars 2007	Banque	30000	Inscription abusive dans les fichiers de la banque de France
Mars 2007	Recherche de débiteurs	5000	Non-déclaration du fichier de recherche de débiteurs Durées de conservation excessives
Mars 2007	Société de démarchage téléphonique	10000	Non-respect du droit d'opposition à recevoir des appels téléphoniques de prospection commerciale
Mai 2007	Site internet	15000	Liste noire non régulière de mauvais payeurs locataires
Juin 2007	Recherche de débiteurs	50000	Collecte illicite d'informations relatives à des débiteurs Collecte de données sensibles Durées de conservation excessives
Octobre 2007	Recherche de débiteurs	10000	Traitement non déclaré Collecte illicite d'informations relatives à des débiteurs Aucune durée de conservation définie Non-respect de l'obligation de sécurité
Novembre 2007	Commerce	5000	Non-respect droit d'opposition Non-respect *opt in* (démarchage par télécopies) Traitement non déclaré
Décembre 2007	Société de merchandising et d'animation	40000	Commentaires excessifs dans les fichiers du personnel Absence d'information du personnel Absence de durée de conservation des données Traitement non déclaré

LISTE DES ORGANISMES CONTRÔLÉS EN 2007

ASSURANCES

AGF

FAC INTERNATIONAL

MACIF MUTUALITÉ

MAPA ASSURANCES

MUTUELLE INTÉGRANCE

BANQUES

BANQUE FORTIS FRANCE

BNP PARIBAS

LA BANQUE POSTALE

BIOMÉTRIE

AIR PROMOTION GROUP

BERTRAND DÉMÉNAGEMENTS

CABINET BREESE-DERAMBURE ET MAJEROWICZ

CAVE CANEM SURVEILLANCE SÉCURITÉ

CITÉ DE L'ARCHITECTURE ET DU PATRIMOINE

CLINIQUE ÉDOUARD RIST

CLINIQUE DE GOUSSONVILLE

CRÈCHE L'ENVOL

ÉTABLISSEMENT SCOLAIRE SAINT JOSEPH – SAINTE MARIE-MADELEINE

HÔTEL KUBE

HÔTEL LE BRISTOL

INSTITUT HOSPITALIER JACQUES CARTIER

LA FRANÇAISE DES JEUX

LÉONARD FASHION

LYCÉE CARNOT<OLE_LINK1_FSIG> (CANNES)

LYCÉE EDGAR QUINET (PARIS 9e)

LYCÉE MAURICE RAVEL (PARIS 20e)

LYCÉE POLYVALENT BRISTOL (CANNES)

MAGIC FORM

MAISON DE RETRAITE «MA MAISON»

SMITHS MEDICAL FRANCE

SOCIÉTÉ ICOGES SAS

SOCIÉTÉ DU MARCHÉ D'INTÉRÊT NATIONAL D'AVIGNON

SYMPHONING

TENNIS CLUB DE REIMS

COLLECTIVITÉS LOCALES

CONSEIL GÉNÉRAL DU CALVADOS (CAEN)

CONSEIL RÉGIONAL DE BASSE-NORMANDIE (CAEN)

MAIRIE D'ÉMERAINVILLE

MAIRIE DE NOISY-LE-SEC

COMMERCE

CENTRE LECLERC (MASSY)

CINÉMA GAUMONT (LE GRAND-QUEVILLY)

CORA (ARCUEIL)

EXPLI'SITE

HODORI INTERNATIONAL

HÔTEL FORMULE 1

ILICO.NET

IPSOS

KOHLER FRANCE

L'HOMME MODERNE (TOULOUSE)

CENTRE LECLERC DE MASSY

MONOPRIX

SERPIE

SOCIÉTÉ DE GESTION DU CENTRE HÉLIOMARIN RENÉ OLTRA

CRÉDIT

SOCIÉTÉ FINANCO

DROITS D'AUTEUR

ADVESTIGO

CO-PEER-RIGHT AGENCY

CYBERCOM SOLUTIONS

ÉDUCATION

SOS ÉDUCATION

INSTITUT DE FORMATION JOËL SAVATOFSKI

EXPÉRIMENTATION DU DOSSIER PHARMACEUTIQUE

PHARMACIE CABANIE-BIANNIC

PHARMACIE CROIX PAQUET

PHARMACIE GAMBETTA

PHARMACIE LESAGE

PHARMACIE DE LA NATION

PHARMACIE MONGAUZE

PHARMACIE REBOUL

GÉOLOCALISATION

ARNAUD PROPRETÉ

DALLOYAU SA

EASY FIELD SERVICES

EXO 7

JF CESBRON

LES AMBULANCES MARITIMES

SOCIÉTÉ PAYEUX

LOGEMENT

OPHLM (MONTIGNY LES METZ)

MARKETING

CEDRICOM SERVICES

COME & STAY

CONFOLAND

EXPLI'SITE

ISOTHERM

SOCIÉTÉ K PAR K

SANTÉ

CENTRE MÉDICAL MANGINI

SÉCURITÉ

ACTE 2

B & M

CONTRÔLE SANCTION AUTOMATISÉ (RENNES)

DIRECTION GÉNÉRALE DES DOUANES ET DES DROITS INDIRECTS (DGDDI)

DIRECTION GÉNÉRALE GENDARMERIE NATIONALE

FICHIER NATIONAL AUTOMATISÉ DES EMPREINTES GÉNÉTIQUES (FNAEG)

MINISTÈRE DE L'INTÉRIEUR (EURODAC)

MINISTÈRE DE L'INTÉRIEUR (EUROPOL)

MINISTÈRE DE L'INTÉRIEUR SCHENGEN (ARTICLE 96)

MINISTÈRE DE L'INTÉRIEUR (SIS-ARTICLE 99)

POLICE MUNICIPALE (BRY-SUR-MARNE)

POLICE MUNICIPALE (BUSSY SAINT-GEORGES)

POLICE MUNICIPALE (ÉMERAINVILLE)

SECURITAS

SOCIÉTÉ ICTS

SOCIÉTÉ SGA

SOCIÉTÉ PENNAVAIRE ET ASSOCIÉS

STIC

COMMISSARIAT DE POLICE (CRÉTEIL)

COMMISSARIAT DE POLICE (ÉPERNAY)

COMMISSARIAT DE POLICE (PARIS-18e ARRONDISSEMENT)

COMMISSARIAT DE POLICE (REIMS)

COMMISSARIAT DE POLICE (ROUEN)

DIRECTION RÉGIONALE DES RENSEIGNEMENTS GÉNÉRAUX DE LA HAUTE-NORMANDIE DE ROUEN

MINISTÈRE DE L'INTÉRIEUR (STIC)

PARQUET DU TRIBUNAL DE GRANDE INSTANCE DE CRÉTEIL

PARQUET DU TRIBUNAL DE GRANDE INSTANCE DE TROYES

PRÉFECTURE DE POLICE DE PARIS

PRÉFECTURE DE L'AUBE (TROYES)

PRÉFECTURE DU VAL-DE-MARNE (CRÉTEIL)

SERVICE RÉGIONAL DE POLICE JUDICIAIRE (SRPJ REIMS)

SERVICE RÉGIONAL DE POLICE JUDICIAIRE (SRPJ ROUEN)

TÉLÉCOMMUNICATIONS

BOUYGUES TELECOM

FRANCE TELECOM

FREE

IC TÉLÉCOM

NEUF TELECOM

NOOS

OMER TELECOM

ORANGE FRANCE

SFR

SRR

TELECOM ITALIA

TÉLÉ 2

T-ONLINE

TRAVAIL

ATOS ORIGIN

BRISTOL-MYERS SQUIBB

CABINET D'AVOCATS CMS BUREAU FRANCIS LEFEBVRE

CADBURY FRANCE

FRANCE INCENDIE

FRANCE 2

FRANCE 3

FRANCE TÉLÉVISIONS

FRANCE TÉLÉVISIONS SERVICES

GILEAD SCIENCES

ICAS FRANCE

KOHLER FRANCE

MILLIPORE

RENAULT TRUCKS

SERVICE INNOVATION GROUP

SOCIÉTÉ BOISSONNADE

SOCIÉTÉ CIRCULAR FRANCE

SOCIÉTÉ CIRCULAR PRO-VENTE

SOCIÉTÉ COMBAULT RESTAURATION (QUICK)

SOCIÉTÉ GIBAG

SOLYMATIC FRANCE

01 CONSULTING

LEXIQUE INFORMATIQUE ET LIBERTÉS

CNIL

Autorité administrative indépendante, composée d'un collège pluraliste de dix-sept commissaires, provenant d'horizons divers (quatre parlementaires, deux membres du Conseil économique et social, six représentants des hautes juridictions, cinq personnalités qualifiées désignées par le président de l'Assemblée nationale (1), par le président du Sénat (1), par le Conseil des ministres (3)). Le mandat de ses membres est de cinq ans. Le président est élu par ses pairs.

Correspondant informatique et libertés

Créé en 2004, le correspondant informatique et libertés (CIL) est chargé d'assurer de manière indépendante le respect des obligations prévues par la loi du 6 janvier 1978 modifié en 2004 ; en contrepartie de sa désignation, les traitements de données personnelles les plus courants sont exonérés de déclarations auprès de la CNIL.

Destinataire

Personne habilitée à obtenir communication de données enregistrées dans un fichier ou un traitement en raison de ses fonctions.

Donnée biométrique

Caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales…).

Donnée personnelle

Toute information identifiant directement ou indirectement une personne physique (nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale…).

Donnée sensible

Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Droit à la protection des données personnelles

Le droit à la protection des données à caractère personnel est inscrit dans la charte des droits fondamentaux de l'Union européenne au titre des libertés fondamentales telles que la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information ou le respect de la vie privée et familiale, etc.

Droit à l'information

Toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union européenne.

Droit d'accès direct

Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

Droit d'accès indirect

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.

Droit d'opposition

Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser

sans avoir à se justifier que les données qui la concernent soient utilisées à des fins de prospection commerciale.

Droit de rectification

Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsque ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Fichier des fichiers

Liste des fichiers déclarés à la CNIL, ainsi que leurs caractéristiques.

Finalité d'un traitement

Objectif principal d'une application informatique de données personnelles. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.

Formalités préalables

Ensemble des formalités déclaratives à effectuer auprès de la CNIL avant la mise en œuvre d'un traitement de données personnelles ; selon les cas, il peut s'agir d'une déclaration ou d'une demande d'autorisation.

Formation contentieuse

Pour prendre des mesures à l'encontre des responsables de traitement qui ne respectent pas la loi informatique et libertés, la CNIL siège dans une formation spécifique, composée de six membres appelée « formation contentieuse ». À l'issue d'une procédure contradictoire, cette formation peut notamment décider de prononcer des sanctions pécuniaires pouvant atteindre 300 000 euros.

Listes d'opposition

Les listes d'opposition recensent les personnes qui ont fait connaître leur opposition à être prospectées dans le cadre d'opérations de marketing.

NIR

Le numéro d'inscription au répertoire ou numéro de sécurité sociale est attribué à chaque personne à sa naissance sur la base d'éléments d'état civil transmis par les mairies à l'INSEE.

Responsable de données

Personne qui décide de la création d'un fichier ou d'un traitement de données personnelles, qui détermine à quoi il va servir et selon quelles modalités.

Séance plénière

C'est la formation qui réunit les dix-sept membres de la CNIL pour se prononcer sur des traitements ou des fichiers et examiner des projets de loi ou de décrets soumis pour avis par le Gouvernement.

Traitement de données

Collecte, enregistrement, utilisation, transmission ou communication d'informations personnelles, ainsi que toute exploitation de fichiers ou bases de données, notamment des interconnexions.

Transfert de données

Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

Crédits photo :

© CNIL : p. 7, 17, 21, 24, 26, 31, 32, 39, 43, 47, 55 (bas d et g), 57 (bas), 60, 65, 69, 71, 75, 81, 82.
© Fotolia : p. 16, 20, 23, 25, 55 (haut), 57 (haut), 59, 64, 68.