COMMISSION
NATIONALE DE
L'INFORMATIQUE
ET DES LIBERTÉS

27e RAPPORT D'ACTIVITÉ 2006

ISBN : 978-2-11-006397-7

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

27e RAPPORT D'ACTIVITÉ 2006

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

Orages sur la CNIL !

Avec 570 % d'augmentation de son activité en trois ans (2003 à 2006), plus de 70 000 fichiers déclarés chaque année, la CNIL connaît une croissance spectaculaire et continue de son champ d'action. Entreprises, administrations, particuliers, organismes professionnels ou élus, tous s'adressent à la CNIL parce que tous mettent en œuvre des fichiers : l'informatique est partout. On mesure ainsi quelle est désormais l'étendue de la mission de la CNIL.

Cette tendance s'est confirmée en 2006, année au cours de laquelle a commencé à se faire sentir réellement le poids des nouvelles missions assignées par le législateur à notre Commission.

Or c'est précisément durant cette période écoulée depuis le dernier rapport annuel que sont apparus, dans le ciel de la CNIL, de gros nuages, noirs et menaçants.

En effet, alors même que notre Commission est ainsi confrontée à un accroissement considérable de son champ d'intervention, voici que son action et, dans une certaine mesure, son existence même ont été fortement mises en cause, et ce de deux manières.

• C'est d'abord la publication du décret du 25 mars 2007 réglementant le fonctionnement de notre Commission qui rend l'exercice de nos missions plus difficile. Le projet de décret avait été soumis à la CNIL pour avis en juin 2006. À cette occasion, notre Commission avait clairement exposé les atteintes graves que feraient courir à son efficacité certaines des dispositions envisagées. Hélas, nous n'avons pas été écoutés et nous devons constater que ce texte comporte un certain nombre de dispositions qui tendent à alourdir à l'excès les procédures, à allonger les délais de réponse des administrations aux citoyens et, parfois, à limiter l'autonomie de fonctionnement de la CNIL.

Tel est le cas, à titre d'exemple, de l'article 2 du décret qui prévoit que la Commission *« ne peut valablement délibérer »* que si le projet de délibération est parvenu *« au commissaire du Gouvernement huit jours au moins avant la date de la séance »*. Ce faisant, le commissaire du Gouvernement se voit attribuer un privilège que les membres de la CNIL n'ont pas retenu pour eux-mêmes et sera désormais en mesure d'invoquer une transmission tardive pour s'opposer à ce que la Commission délibère sur un sujet. Or, chacun sait que la maîtrise de l'ordre du jour de ses travaux par une institution collégiale, quelle qu'elle soit, est la première condition de son indépendance…

• C'est également sur le plan budgétaire que notre Commission s'est vue gravement mise en difficulté ces derniers mois.

En effet une initiative fâcheuse a été prise sous la forme d'un amendement adopté par la Commission des finances de l'Assemblée nationale lors de la discussion du budget pour 2007. Celui-ci en effet réduisait les crédits de fonctionnement de la CNIL de 50 % Autant dire qu'il condamnait celle-ci à l'impuissance pour ne pas dire à la disparition. Grâce à une réaction immédiate et forte de notre Commission, soutenue, il est vrai, par le ministre de l'Intérieur et le ministre de la Justice, cet amendement fut retiré. Mais il mettait néanmoins en lumière la fragilité de l'indépendance de la CNIL, autorité administrative… indépendante. Il soulignait également l'inadéquation de son statut budgétaire. Rattachée, en effet, au ministère de la Justice pour des raisons uniquement techniques, la CNIL est souvent assimilée, à tort, à un service d'une administration centrale.

C'est pourquoi j'ai demandé au Premier ministre de bien vouloir mettre en place une mission de réflexion sur le positionnement budgétaire des autorités administratives indépendantes et sur les modalités de préparation de leurs budgets dont le montant doit être en adéquation avec leur mission.

Le Premier ministre nous a informés à l'automne dernier de sa décision de la création de cette mission. Malheureusement, force est de constater qu'à ce jour, cette mission n'a pas débuté ses travaux…

Cet amendement adopté par la Commission des lois de l'Assemblée nationale constituait une initiative d'autant plus inopportune qu'elle intervenait dans un contexte de sérieuses difficultés budgétaires pour la CNIL. En effet, en novembre 2006, la Commission connaissait un déficit de plus de 530 000 euros, largement provoqué par l'essor considérable de son activité. Ce déficit la conduisit à renoncer à certaines de ses missions, notamment de contrôle de fichiers ou d'instruction rapide de plaintes des citoyens. Parce qu'elle entravait son bon fonctionnement et menaçait l'indépendance de notre Commission, j'ai porté à la connaissance du Premier ministre cette situation. Celui-ci a fait en retour procéder au versement d'une dotation financière d'urgence couvrant une partie significative du déficit.

Pour l'avenir, je souhaite ardemment que chacun comprenne que, s'agissant de la protection des données personnelles, désormais inscrite parmi nos libertés fondamentales, le statut d'autorité administrative indépendante conféré à la CNIL n'est qu'une formule si son indépendance n'est pas réellement assurée.

Et cette indépendance passe, d'une part, par la « sanctuarisation » de son budget et, d'autre part, par l'attribution d'un budget correspondant réellement aux nouvelles missions qui lui ont été confiées par le législateur voici trois ans.

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

ALERTE À LA SOCIÉTÉ DE SURVEILLANCE

La société de surveillance menace notre capital de protection des données et nos libertés

Questions à …

ALEX TÜRK

Sénateur du Nord
Président de la CNIL

Dans quel contexte avez-vous lancé cette alerte à la société de surveillance ?

C'est lors de la conférence mondiale des commissaires à la protection des données, à Londres, en novembre 2006, que j'ai présenté, au nom de la Commission nationale de l'informatique et des libertés, une initiative qui a reçu le soutien des 75 délégations présentes.

« L'informatique doit être au service du citoyen et ne doit porter atteinte ni à l'identité humaine, ni à la vie privée ni aux libertés » est-il écrit dans la loi de 1978. Trente ans après, deux vagues menacent pourtant nos autorités de protection des données et les libertés qu'elles ont pour mission de protéger. La première vague est d'ordre technologique, la seconde de nature normative.

En quoi consiste cette vague technologique ?

Le progrès technologique devient de plus en plus complexe à maîtriser car le délai séparant l'invention de sa mise en œuvre se raccourcit. **Le temps technologique connaît une accélération constante, tandis que le temps juridique demeure particulièrement lent**, régi par le rythme des procédures démocratiques. De même, la dimension internationale des échanges de données rend difficile leur contrôle. Cette tendance à la **globalisation** entre souvent en conflit avec une autre caractéristique de la règle de droit, à savoir son application à un territoire et à un champ de compétence, délimité, ordonné, balisé.

Or, l'innovation technologique est à la fois porteuse de progrès et de dangers. Les individus sont tentés par le confort qu'elle procure, mais ils sont peu conscients des risques qu'elle comporte. Ils ne se préoccupent guère de la surveillance de leurs déplacements, de l'analyse de leurs comportements, de leurs relations, de leurs goûts. Cette **ambivalence du progrès** est difficile à concilier avec la règle juridique qui doit, par définition, être univoque.

Par ailleurs, la technologie tend à devenir **invisible** parce que de plus en plus de traitements de données sont réalisés à l'insu des personnes et permettent de tracer leurs déplacements physiques dans les transports en commun, leurs consultations sur Internet, leurs communications téléphoniques… **Cette surveillance invisible** est « virtuelle » puisqu'elle est liée aux processus informatiques. Elle tend aussi à devenir « réelle » du fait de l'extrême miniaturisation des procédés utilisés. Avec les nanotechnologies, il sera bientôt impossible de distinguer à l'œil nu si une technologie informatique est présente dans un objet : dès lors comment encadrer et contrôler des traitements

mis en œuvre par des instruments invisibles ?

On le voit, les modalités de la protection des libertés personnelles, qui est aussi celle des données personnelles, doivent être repensées. À défaut, nos autorités risquent d'être contournées, submergées, par cette vague technologique.

Qu'en est-il de la vague normative liée à la lutte antiterroriste ?

Le développement des législations antiterroristes représente un défi pour les autorités de protection des données qui doivent éviter les pièges, dénoncer les illusions et combattre les mythes.

En effet, il leur est rarement possible de se prononcer sur un projet de loi de manière tranchée, binaire, « favorable ou défavorable ». L'ensemble des autorités de protection des données reconnaît la légitimité des politiques de lutte antiterroriste mises en œuvre depuis quelques années. Mais elles doivent également, conformément aux missions qui leur ont été confiées par les textes fondateurs, et au nom de la société, **rechercher en permanence un équilibre entre les impératifs de sécurité publique**, d'une part, et **les exigences de la protection de la vie privée et des données personnelles**, d'autre part.

Elles doivent assumer ce rôle en toute indépendance et rejeter les accusations inacceptables d'irresponsabilité qui sont parfois proférées à leur encontre. Elles doivent aussi rappeler sans cesse à l'opinion publique, aux pouvoirs exécutifs, que la création d'un fichier informatique comportant toujours davantage de données ne règle pas tout. Un fichier n'est pas un instrument « magique » et omniscient : il faut désacraliser cette prétendue infaillibilité.

La protection des données ne doit donc pas être conçue comme un thème abstrait, théorique, éloigné de la vie quotidienne. Les règles de protection des données protègent des personnes. Il s'agit de protéger un droit à ne pas être fiché, surveillé, contrôlé de manière abusive et illimitée ; il s'agit de protéger la dignité humaine, de permettre aux personnes d'exercer leurs droits. Préserver ces droits participe aussi de la lutte contre le terrorisme car ce dernier veut détruire notre système démocratique. L'affaissement de nos libertés serait donc une victoire pour le terrorisme à laquelle nos autorités ne sauraient se résoudre.

Est-il encore temps d'agir ?

Oui, mais nous sommes confrontés à une situation d'extrême urgence. Je m'explique. Les effets du progrès technologique sont irréversibles, sauf bouleversements de civilisation. Dans une certaine mesure, sont également irréversibles les effets des législations qui encadrent ce progrès. Ceci m'amène à suggérer une image. Chacun admet aujourd'hui que l'on ne saurait continuer à agir, dans le domaine de la protection du capital naturel, sans risquer d'amputer celui-ci et de mettre en cause sa pérennité. De la même manière, s'agissant du capital représenté par notre identité, notre vie privée et la protection de nos droits fondamentaux, nous devons être conscients que les atteintes qui lui sont portées, de manière irréversible, mettent en cause sa pérennité.

Dès lors, on voit à quel point il est important qu'une autorité comme la nôtre soit en mesure de proposer des équilibres acceptables à la société française, entre la nécessaire défense des libertés individuelles et les exigences de la recherche d'un niveau de sécurité collective suffisant.

Enfin, je voudrais insister sur un point. En cette matière, le rôle de la CNIL n'est pas de juger de l'opportunité de choix opérés par les pouvoirs publics. Sa mission est d'éclairer ces choix et de formuler des solutions permettant de conjuguer des légitimités opposées, en vertu des principes de finalité et de proportionnalité des traitements de données des personnes, tels qu'ils sont définis par le législateur depuis 1978 et renouvelés depuis 2004.

Comment, concrètement, les autorités de protection peuvent-elles réagir ?

Face à ces risques, les autorités doivent provoquer une prise de conscience collective et se rassembler pour agir. À la suite de cette initiative, des groupes de travail réfléchissant aux instruments d'action des autorités, à l'efficacité de leur collaboration et de leur expertise ont été mis en place. Un premier groupe s'est réuni à Paris au début de l'année 2007 pour recenser les « meilleures pratiques » en matière de communication. Toutes les autorités s'accordent en effet à reconnaître l'importance fondamentale des activités de communication et de pédagogie, que ce soit à l'égard des opinions publiques, des parlementaires et des jeunes générations.

D'autres groupes de travail ont également été constitués pour améliorer l'efficacité des différents moyens d'action des autorités, par exemple en matière de contrôles, de sanctions ou de mise en place de correspondants informatique et libertés. Ces travaux, ambitieux puisqu'il s'agit de développer la coopération entre autorités, de rationaliser leur action commune, devraient faciliter la prise de conscience collective à l'égard des risques irréversibles que font peser ces deux vagues sur nos libertés.

Le texte intégral prononcé par Alex Türk en novembre 2006 figure en annexe de ce rapport.

LA CONVERGENCE DES TECHNOLOGIES

La biométrie gagne du terrain

Les tendances observées en 2005 ont été confirmées en 2006

La première concerne l'accroissement continu du recours à cette technologie. La CNIL a ainsi dû faire face à une nette augmentation du nombre de demandes d'autorisation relatives à des dispositifs biométriques. Ces demandes ont en effet été multipliées par dix en un an. C'est la raison pour laquelle la CNIL a adopté, en avril 2006, trois procédures simplifiées d'autorisation relatives aux dispositifs :
– de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire ;
– 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 aux locaux sur les lieux de travail ;
– reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail.

Les traitements strictement conformes à l'une de ces trois décisions cadres (autorisations uniques) peuvent être mis en œuvre après une simple déclaration de conformité. Elles répondent aux finalités le plus souvent assignées à un dispositif biométrique et représentent 299 des 351 autorisations délivrées par la CNIL en 2006.

Les 52 autorisations restantes confirment la seconde tendance observée en 2005 : la diversité des finalités pour lesquelles les dispositifs biométriques sont mis en œuvre.

La Commission a ainsi autorisé certains casinos à proposer une carte de fidélité dans laquelle est enregistrée l'empreinte digitale des personnes volontaires. Ce dispositif s'inscrit dans le cadre de l'obligation de contrôler l'accès aux casinos depuis le 1er novembre 2006. Les clients titulaires de cette carte bénéficient d'une procédure de contrôle automatisée plus rapide.

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…). Elles se rapprochent ainsi de ce qui pourrait être défini comme un « identificateur unique universel », permettant de fait le traçage des individus.

En ce qui concerne les systèmes biométriques reposant sur la reconnaissance de l'empreinte digitale dans une base centralisée, ils doivent être justifiés par un fort impératif de sécurité.

Enfin, l'année 2006 a également été le théâtre d'évolutions concernant des projets d'ampleur nationale et internationale :
– le ministère de l'Intérieur a annoncé lors du 4e forum européen sur l'administration électronique que les futures cartes nationales d'identité électroniques intégreront des données biométriques (les empreintes digitales) ;
– il a aussi décidé de généraliser le projet BIODEV imposant aux demandeurs de visas un titre électronique intégrant les empreintes de leurs dix doigts et leur photo, alors qu'il ne s'agissait jusqu'ici que d'une expérimentation.

MÉMO

BIOMÉTRIE

– en 2005, la CNIL a autorisé la mise en œuvre de 34 dispositifs et en a refusé 5.
– en 2006, elle a :
• enregistré 299 engagements de conformité ;
• autorisé 52 dispositifs et en a refusé 9.

La vidéosurveillance avance

La Commission a enregistré en 2006 un accroissement très sensible du nombre de déclarations relatives aux systèmes de vidéosurveillance (300 en 2005, contre 880 en 2006). Cette augmentation peut s'expliquer par le développement de politiques de sécurité dans les entreprises, mais également par une meilleure connaissance des obligations de la loi informatique et libertés, la CNIL ayant notamment sensibilisé les professionnels du secteur.

Techniquement, ces systèmes évoluent désormais vers la vidéosurveillance dite « IP », c'est-à-dire utilisant des technologies Internet, filaire ou non filaire (Wi-Fi) pour la transmission numérique des images. Certains constructeurs proposent par ailleurs l'enregistrement simultané des sons en complément des images, mais aussi des logiciels d'analyse des images (le système étant, par exemple, capable de détecter seul un colis abandonné ou de procéder au comptage du nombre de clients entrant et sortant d'un magasin).

Les conclusions du rapport d'activité pour 2006 des commissions départementales vidéosurveillance (qui délivrent des avis dans le cadre de la procédure obligatoire d'autorisation par arrêté préfectoral pour la mise en œuvre de systèmes sur la voie publique ou des lieux ouverts au public) seront particulièrement éclairantes pour évaluer l'évolution du développement de la vidéosurveillance en France.

Il faut noter qu'un décret du 26 juillet 2006 est venu préciser les pouvoirs de ces commissions départementales, qui peuvent décider de procéder de leur propre initiative à des contrôles et non seulement émettre des recommandations, mais aussi proposer la suspension d'un système lorsqu'elles constatent qu'il en est fait un usage « anormal ou non conforme à son autorisation ».

La CNIL a de son côté poursuivi ses missions de contrôles sur place.

C'est votre droit

Les modalités d'information du public doivent être précisées, notamment par une obligation d'adapter le format, le nombre et la localisation des affiches ou panonceaux à la situation des lieux et établissements. Désormais ces affichages doivent indiquer le nom ou la qualité et le numéro de téléphone du responsable auprès duquel toute personne intéressée peut s'adresser pour faire valoir son droit d'accès.

La géolocalisation des véhicules de salariés encadrée

La CNIL a adopté, le 16 mars 2006, une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules utilisés par les employés des administrations et des entreprises. Cette recommandation s'inscrit dans le cadre d'une réflexion générale sur les traitements de géolocalisation. Elle vise le cas des employés qui utilisent un véhicule dans le cadre de leur travail et doivent accepter d'être géolocalisés.

À la suite de l'augmentation très sensible des déclarations de traitement des systèmes de géolocalisation des véhicules des employés, la CNIL a jugé utile de rassembler dans une recommandation les principales règles à respecter en termes d'informatique et de libertés. Elle s'est limitée dans un premier temps à la géolocalisation des véhicules, mais elle n'ignore pas que la géolocalisation des employés eux-mêmes, par le truchement de leur téléphone mobile ou de toute autre technologie, est également possible.

Qu'est-ce que c'est ?

LA GÉOLOCALISATION

Il s'agit d'une technologie associée à un traitement de données personnelles, qui a pour but principal de déterminer la localisation plus ou moins précise d'un objet ou d'une personne par le biais d'un système GPS ou d'un téléphone mobile. Ses applications et ses finalités sont multiples : de l'assistance à la navigation, à la mise en relation des personnes, mais aussi à la gestion en temps réel des moyens en personnel et en véhicules des entreprises, etc. De nouvelles possibilités sont venues se greffer sur la finalité initiale, qu'il s'agisse de l'enregistrement des données pour apporter la preuve de la réalisation de certaines prestations ou encore d'analyses sur la rapidité d'exécution desdites prestations.

La recommandation rappelle qu'un traitement automatisé de données à caractère personnel doit répondre à l'exigence d'une finalité légitime. Ainsi, seuls un impératif de sûreté ou de sécurité de l'employé lui-même ou des marchandises ou véhicules dont il a la charge, une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés, le suivi et la facturation d'une prestation ou encore le suivi du temps de travail, lorsque ce suivi ne peut être réalisé par d'autres moyens, peuvent justifier la mise en œuvre de tels dispositifs.

A contrario, la recommandation indique que la géolocalisation ne saurait être justifiée lorsqu'un employé dispose d'une liberté dans l'organisation de ses déplacements. De même, elle ne doit pas conduire à un contrôle permanent de l'employé concerné. Ainsi, la collecte des données relatives à la localisation d'un employé en dehors des horaires de travail devrait être proscrite. Dans cet esprit, la possibilité de désactiver le dispositif de géolocalisation à l'issue du temps de travail doit être offerte lorsque ces véhicules peuvent être utilisés à des fins privées.

Questions à …

DIDIER GASSE

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

Comment la CNIL a-t-elle procédé pour dégager les grands axes de cette recommandation ?

De plus en plus, un processus de consultation approfondi s'avère nécessaire sur des sujets complexes afin que les intérêts et sensibilités légitimes de chacun des acteurs soient pris en compte.

Nous avons procédé en plusieurs temps en élargissant peu à peu la consultation à un grand nombre d'acteurs publics et privés : les ministères intéressés, les fournisseurs de matériels et de services, les utilisateurs, les syndicats et même une fédération d'usagers de la route.

Ces consultations ont évidemment fait évoluer notre position initiale sur un certain nombre de points : à titre d'exemple, la finalité de suivi du temps de travail peut apparaître comme trop intrusive dans une première analyse, alors qu'elle peut être conçue en réalité dans l'intérêt commun de l'employeur et du salarié. En fait, le sujet ne se limite pas à la géolocalisation mais à celui de la collecte et du traitement de toutes les données susceptibles d'être associées à la géolocalisation.

Quel était pour vous l'enjeu ?

Face au développement accéléré de la géolocalisation, l'enjeu était de prendre en compte dans le domaine des relations de travail les impacts de la géolocalisation sur les libertés. Nous avions ressenti une attente à ce sujet, compte tenu du caractère intrusif de la géolocalisation. Au demeurant, la difficulté était de répondre à deux types de situations : celle où l'utilisation du véhicule constitue l'objet même du travail de l'employé ; celle où l'utilisation du véhicule n'en est que l'accessoire. On comprend que les chauffeurs routiers ou les transporteurs de fonds se trouvent au regard de la liberté d'organisation de leur travail dans une situation radicalement différente de celle d'un « commercial ». C'est cette différence que la recommandation prend en compte en répertoriant les finalités acceptables.

L'enjeu était donc d'essayer de clarifier la situation tout en permettant aux entreprises et administrations concernées de pouvoir se référer à une norme simplifiée pour mettre en œuvre les traitements de géolocalisation.

Pourquoi s'être limité à la géolocalisation des véhicules ?

Parce qu'actuellement, c'est le cas le plus fréquent et que vouloir intégrer dans un même texte tous les cas de géolocalisation risquait de le rendre illisible. Remarquons que tous les traitements de géolocalisation touchant directement ou indirectement des personnes sont soumis à la loi informatique et libertés. Si la géolocalisation des employés en dehors de leur véhicule – ou plus exactement celle d'objets dont ils ont l'usage, tel qu'un téléphone mobile – devait se développer, l'élaboration d'une recommandation spécifique serait sans doute utile.

Y aura-t-il des suites à cette recommandation ?

Les services de géolocalisation ne peuvent que se développer, associés à des techniques de plus en plus performantes pour collecter d'autres renseignements, par exemple sur la façon de conduire un véhicule.

Après avoir communiqué sur ce sujet, la CNIL réalisera une série de contrôles sur les dispositifs mis en œuvre. Elle a reçu également quelques plaintes actuellement en cours de traitement. L'intérêt d'effectuer des contrôles sur un tel sujet n'est pas tant de rechercher des entreprises en infraction que de mieux appréhender la mise en œuvre sur le terrain de ces dispositifs et, le cas échéant, de contribuer au redressement de situations irrégulières.

La géolocalisation est un cas typique où la CNIL doit s'efforcer non pas de faire obstacle au développement de nouvelles technologies, mais de l'accompagner pour nous préserver de dérives en termes de protection des libertés et de la vie privée.

La Commission a précisé **les conditions dans lesquelles peut être mis en œuvre un traitement de géolocalisation :**
– interdiction de collecter les données relatives aux éventuels dépassements de limitation de vitesse, la collecte d'infractions étant du ressort des pouvoirs publics ;
– mise en place de mesures de sécurité au sein de l'entreprise ;
– définition d'une durée de conservation adéquate ;
– information préalable des employés.

Simultanément à cette recommandation, la Commission a adopté une norme destinée à simplifier les formalités préalables des entreprises dont le traitement de géolocalisation mis en œuvre s'inscrit dans les règles définies par la CNIL.

La recommandation et la norme simplifiée traduisent la volonté de la CNIL de fixer, de manière concrète et précise, des règles en matière de géolocalisation des employés afin que le développement de ce nouvel outil s'effectue dans le respect des dispositions protectrices de la loi du 6 janvier 1978 modifiée en 2004.

LA PROFUSION DES TEXTES EN FRANCE ET EN EUROPE

La loi antiterroriste du 23 janvier 2006

La mise en application de la loi antiterroriste du 23 janvier 2006 a entraîné, depuis un an, un accroissement du nombre de textes réglementaires soumis à la CNIL et élargit les possibilités d'accès et d'exploitation par les services de police de données initialement collectées pour un autre objet. Il faut préciser que l'indication par la loi elle-même des conditions de mise en œuvre de ces traitements a réduit les marges de manœuvre de la CNIL.

• Ainsi, cette loi prévoit notamment **la mise en œuvre de traitements automatisés de données collectées par les transporteurs aériens, ferroviaires ou maritimes**. Selon son article 7, les données des passagers à destination ou en provenance d'États situés en dehors de l'Union européenne pourront être traitées pour les besoins du contrôle aux frontières, de la lutte contre l'immigration clandestine et de la lutte contre le terrorisme. Dans cette dernière hypothèse, la loi dispose que seuls certains agents des services de police, de gendarmerie et des douanes, dûment habilités, auront accès aux données. Enfin, ces données pourront être rapprochées du fichier des personnes recherchées (FPR) et du système d'information Schengen (SIS).

Le ministère de l'Intérieur a ainsi saisi la CNIL, en juin 2006, d'une demande de modification du fichier national transfrontière (FNT) et, en juillet 2006, de la création du fichier des passagers aériens (FPA). La Commission a également été saisie d'un projet de décret en Conseil d'État, pris après avis de la CNIL, fixant, à titre expérimental, les modalités de transmission des données des passagers aériens par les compagnies aériennes au ministère de l'Intérieur.

S'agissant du FNT, la Commission a notamment pris acte de l'absence d'interconnexion entre ce fichier et le FPR ou le SIS.

Elle a également demandé que, conformément à l'article 32 de la loi du 6 janvier 1978 modifiée en 2004, les personnes susceptibles d'être concernées par le traitement soient informées des droits qui leur sont ouverts au titre de la loi précitée au moyen d'affiches apposées aux points de contrôles frontaliers. La Commission estime que ces notes d'information doivent être complétées par la mention des finalités du traitement ainsi que par les catégories de services compétents pour accéder aux données.

Sur le fichier des passagers aériens (FPA), la Commission a souhaité que l'effacement de la mention « *connu* » ou « *inconnu* », obtenue à partir de l'interrogation du fichier des personnes recherchées (FPR) et du système d'information Schengen (SIS), intervienne dans un délai de vingt-quatre heures, par un dispositif technique similaire à celui mis en œuvre pour bloquer l'accès des agents chargés de l'immigration, afin d'éviter le maintien d'informations périmées au sein du FPA.

• La Commission s'est ensuite prononcée sur les textes prévus en application de l'article 9 de la loi du 23 janvier 2006 qui prévoit, pour les besoins de la prévention et de la répression des actes de terrorisme, que **les agents habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent accéder, dans les conditions fixées par la loi du 6 janvier 1978 modifiée en 2004, aux traitements suivants :**
– fichier national des immatriculations (FNI) ;
– système national de gestion des permis de conduire (SNPC) ;
– système de gestion des cartes nationales d'identité (CNI) ;
– système de gestion des passeports (DELPHINE) ;
– système informatisé de gestion des dossiers des ressortissants étrangers en France (AGDREF) ;
– système de délivrance des visas des ressortissants étrangers (BIODEV), application destinée à gérer les données mentionnées aux articles L. 611-3 à L. 611-5 du code de l'entrée et du séjour des étrangers ayant été contrôlés aux frontières et ne remplissant pas les conditions d'entrée requises.

• Par ailleurs, elle a examiné le projet de décret pris pour l'application de l'article 6 de la loi antiterrorisme qui **étend les possibilités d'exploitation, par les services de police, des données liées à l'utilisation des services de communications électroniques**, notamment en élargissant la définition des personnes tenues de conserver ces données.

Enfin, conformément aux dispositions de la loi du 9 mars 2004, la CNIL a été saisie du décret d'application qui précise les conditions de **réquisitions judiciaires par voie télématique ou informatique**, à l'égard des traitements des organismes publics ou des personnes morales de droit privé, à l'exception des églises et groupements à caractère religieux, philosophique, politique, syndical, des organismes de presse et des opérateurs de télécommunications. La CNIL a rendu le 30 mai 2006 un avis très circonstancié sur ce texte estimant qu'il ne comportait pas les garanties nécessaires en particulier s'agissant de la liste des organismes publics ou privés susceptibles de faire l'objet de réquisitions télématiques ou informatiques.

En tout état de cause, la Commission relève que l'article 60-2 du code de procédure pénale vise essentiellement, comme le montrent les travaux parlementaires, les opérateurs de télécommunications et exclut du champ des réquisitions électroniques les données couvertes par le secret professionnel. Cela soulève certaines interrogations relatives au fait que le projet de décret vise, entre autres, les administrations et les organismes de sécurité sociale, qui gèrent précisément des données protégées par le secret professionnel.

Le projet de loi relatif à la prévention de la délinquance

• Il a été examiné par la CNIL, en juin 2006, et a donné lieu à de nombreuses observations relatives aux conditions d'intervention des acteurs sociaux et du maire auprès des personnes en difficulté. De même, la Commission a émis des réserves sur la création d'un fichier des personnes hospitalisées d'office. Ce fichier avait été institué sous l'autorité du ministre de la Santé pour améliorer l'instruction et le suivi des **mesures d'hospitalisation d'office** prises par arrêté préfectoral, au vu d'un certificat médical circonstancié, à l'égard des personnes dont les troubles mentaux nécessitent des soins et compromettent la sûreté des personnes ou portent atteinte, de façon grave, à l'ordre public. Il était également envisagé qu'il soit utilisé préalablement à la délivrance des ports d'armes.

Toutefois, plusieurs syndicats de psychiatres ayant également formulé des critiques sur ces dispositions, celles-ci ont été retirées.

• Les dispositions du projet de loi qui autorisent le maire à **obtenir communication de l'ensemble des données relatives aux difficultés sociales de ses administrés** ont été jugées disproportionnées par la CNIL. En effet, si le maire a vocation à connaître, de façon ponctuelle, des données sur les personnes sollicitant des aides sociales facultatives qui relèvent traditionnellement de ses compétences, il ne devrait pas être rendu systématiquement destinataire des informations que les professionnels de l'action sociale sont conduits à recueillir auprès des personnes et des familles en difficulté.

Suivant en cela les préconisations de la Commission, le texte a ainsi été précisé par le Gouvernement. Les professionnels de l'action sociale informeront le maire des difficultés sociales, éducatives ou matérielles d'une personne ou de personnes composant une même famille « lorsque la gravité » de ces difficultés appelle l'action coordonnée de plusieurs intervenants.

• La CNIL a rappelé que **le partage d'informations entre travailleurs sociaux** relatives à des personnes identifiées est légitime dès lors qu'il est strictement nécessaire à leur prise en charge sociale et est réalisé dans l'intérêt des personnes concernées.

Le texte soumis au Parlement va dans ce sens en ne prévoyant que le partage d'informations entre les professionnels et le coordonnateur intervenant dans le cadre de la mise en place de mesures de prévention fondées sur l'action sociale et éducative. Toutefois demeure la disposition selon laquelle des informations confidentielles nécessaires à l'exercice des compétences dans les domaines sanitaire, social et éducatif peuvent être révélées au maire ou à son représentant par le professionnel intervenant seul et le coordonnateur.

• S'agissant de **l'institution du conseil pour les droits et devoirs des familles**, la Commission a souhaité, dans la mesure où des informations individuelles sensibles, relevant de l'intimité de la vie privée des familles, seraient ainsi recueillies, traitées et conservées, que le législateur définisse précisément les garanties assurant le respect des droits et de la vie privée des personnes. Toutefois, la CNIL n'a pas été suivie sur ce point, car le texte adopté au Parlement ne comportait aucune précision supplémentaire.

• Concernant la mise en place par les maires d'un traitement de données à caractère personnel alimenté à partir des **informations transmises par les organismes chargés du versement de prestations familiales** et par le recteur ou l'inspecteur d'académie pour le contrôle du respect de l'obligation scolaire, la Commission s'est interrogée sur la finalité de ces transmissions d'informations. Elle estimait qu'une solution reposant sur la transmission des listes d'enfants en âge d'être scolarisés, par les caisses chargées du versement des prestations familiales, au seul inspecteur d'académie devrait être privilégiée. Le Gouvernement n'a pas repris cette préconisation de la CNIL lors de l'examen du texte au Parlement.

Toutefois, le souhait exprimé par la Commission qu'un décret en Conseil d'État pris après avis de la CNIL vienne

préciser les modalités des échanges de données, la nature de ces données ainsi que les modalités d'exploitation par le maire, a été pris en compte par le Gouvernement.

La loi a été adoptée par le Parlement le 22 février 2007.

VIS, la plus grande base biométrique au monde

Les négociations relatives au Système d'information sur les visas (ou VIS) sont entrées dans leur phase finale.

En 2006, la plupart des aspects techniques du projet ont été résolus grâce à l'expérimentation menée par la France et la Belgique depuis 2005 dans le cadre du programme BIODEV. La CNIL s'est prononcée à deux reprises, en 2004 et en 2006, sur la mise en place progressive de la partie nationale du système : les autorités consulaires françaises ont délivré aujourd'hui plus de 100 000 visas dits biométriques et les agents de la Police de l'air et des frontières ont vérifié l'authenticité de plus de 50 000 visas.

Certains développements du VIS ne font pas encore l'objet d'un accord entre les autorités européennes. Le Parlement européen, s'appuyant notamment sur les avis G 29 (groupe rassemblant les autorités indépendantes de protection des données des 25 pays membres de l'Union européenne), conteste par exemple les modalités d'accès à la base des autorités chargées de la sécurité intérieure des États membres. Il souhaite également encadrer l'âge des demandeurs dont les identifiants biométriques doivent être collectés, entre douze et quatre-vingts ans, contre six ans selon le texte actuel. La modulation de la durée de conservation des données dans la base selon les situations des demandeurs de visas et notamment la suppression des données relatives aux étrangers ayant obtenu un permis de séjour de longue durée constituent un autre point d'achoppement des négociations. Enfin, la constitution d'une base de données personnelles relatives aux personnes invitantes est un autre point essentiel pour les autorités de protection des données et le Parlement européen.

La CNIL sera très attentive, durant l'année 2007, aux développements du VIS, au sein du groupe 29 et au niveau national : le règlement européen final est en effet attendu pour le début d'année, tandis que le ministère de l'Intérieur français achèvera la constitution de la partie nationale du système, appelée dorénavant VISABIO.

Qu'est-ce que c'est ?

VIS (*VISA INFORMATION SYSTEM*)

Le VIS est destiné à améliorer la mise en œuvre de la politique commune en matière de visas, en permettant l'échange entre États membres de l'Union européenne de données relatives aux demandes de visas Schengen qui leur sont adressées. Le système reposera sur une base centrale (C-VIS) reliée par une interface commune aux systèmes nationaux (N-VIS). Ce fichier est appelé à devenir la plus grande base biométrique au monde : il contiendra les photographies et les empreintes digitales de tous les demandeurs de visas uniformes Schengen, soit à terme les identifiants d'environ cent millions d'individus.

Une décision-cadre pour harmoniser l'échange d'informations dans le cadre de la coopération policière et judiciaire

L'année 2006 a également été l'occasion pour le Conseil de l'Union européenne de faire progresser les négociations sur une décision-cadre relative à la protection des données personnelles traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Ce texte vise à établir des conditions harmonisées de traitement et d'échange des données policières et judiciaires entre les États membres, en contrepartie des possibilités accrues d'échanges de données personnelles entre les autorités de sécurité de l'UE.

La CNIL a accordé une attention particulière aux négociations en cours au sein du Conseil sur ce texte fondamental. Il importe en effet, compte tenu de la sensibilité de cette matière, que ce texte consacre un niveau élevé de garantie et de protection des données personnelles traitées dans ce cadre.

Les négociations entre États membres n'ont pu aboutir en 2006, et se poursuivront donc en 2007. La CNIL suivra de près ce processus, afin de donner son avis sur certains points clés du texte, tels que le respect des principes de base de la protection des données, l'attention particulière à porter aux données traitées dans le cadre policier et judiciaire ou le transfert des données vers des pays tiers.

Le traité de Prüm

La CNIL s'est prononcée sur ce texte, en 2006, et a demandé qu'il apporte des garanties complémentaires afin d'assurer aux citoyens des pays concernés un niveau de protection élevé et à tout le moins équivalent à celui prévu par la loi française. En effet, les données à caractère personnel concernées par le traité sont à la fois très nombreuses et particulièrement sensibles. En outre, les modalités automatiques de l'échange de données constituent une innovation majeure, qui présente des risques importants au regard de la protection des données.

En 2006, des premiers échanges de profils ADN ont eu lieu entre l'Autriche et l'Allemagne, qui ont permis la reconnaissance de plus de 700 traces non identifiées. Hormis ces deux pays et l'Espagne, les autres États signataires n'ont pas encore ratifié le traité mais devraient le faire durant le premier semestre 2007. La Slovénie, l'Italie, la Finlande, le Portugal, la Bulgarie, la Roumanie, la Grèce et la Suède ont également fait part de leur souhait d'adhérer au traité, et les négociations ont bien avancé en 2006. Enfin, le Conseil de l'Union européenne a approuvé l'intégration des dispositions du traité dans le droit européen, dans le cadre de la coopération policière et judiciaire en matière pénale. En 2007, la CNIL suivra donc de très près l'avancement des travaux relatifs à ces développements.

Qu'est-ce que c'est ?

LE TRAITÉ DE PRÜM

Signé le 27 mai 2005 à Prüm par l'Allemagne, la Belgique, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche, ce traité vise à intensifier la coopération policière transfrontière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale. Ce traité facilite les procédures d'échange d'informations entre États membres, en prévoyant un accès réciproque et automatique à des bases de données nationales spécifiques : les registres d'immatriculation de véhicules, les fichiers nationaux d'analyse ADN ou les bases de données dactyloscopiques (empreintes digitales). D'autres modalités de coopération sont également prévues : mise en place de patrouilles communes en cas d'événements de grande ampleur, lutte contre les faux documents d'identité.

LES TEMPS FORTS DE L'ANNÉE 2006

LES PREMIÈRES SANCTIONS FINANCIÈRES

En 2006, **onze sanctions financières et sept injonctions de cesser ou modifier un fichier** ont été prononcées par la formation restreinte. Les sanctions pécuniaires prononcées vont de 300 à 45 000 euros, elles représentent pour cette année un montant total de 168 300 euros.

La formation restreinte a sanctionné deux établissements bancaires pour non-respect des règles d'inscription dans les grands fichiers de la Banque de France. D'autre part, plusieurs entreprises opérant du démarchage publicitaire « sauvage » (marketing téléphonique ne respectant pas le droit d'opposition des personnes, spam) ont été sanctionnées.

Elle a également sanctionné une étude d'huissiers de justice (commentaires abusifs sur des débiteurs) ainsi que des organismes n'ayant pas répondu à ses mises en demeure ou ayant communiqué des informations erronées. C'est le cas de la société Tyco Healthcare France dont la sanction de 30 000 euros a été rendue publique.

La formation restreinte a également prononcé quatre avertissements à l'encontre d'organismes n'ayant pas respecté les dispositions de la loi informatique et libertés (opérateur télécoms, parti politique et banques). Certaines de ces sanctions ont été rendues publiques. Il s'agit du Crédit Lyonnais (45 000 euros) et du Crédit Agricole Centre France (20 000 euros).

En 2006, la formation restreinte a engagé plus d'une centaine de procédures de mise en demeure ou de sanction. La plupart des dossiers provenaient de plaintes déposées auprès de la CNIL ou de contrôles réalisés sur place. L'accent mis par la Commission sur le contrôle effectif, par les responsables de traitement, du respect de la réglementation a pour conséquence de faire croître le nombre de dossiers examinés par la formation restreinte.

Pour autant, de telles procédures ne revêtent aucun caractère systématique et concernent des organismes vis-à-vis desquels la CNIL a épuisé toute possibilité de concertation.

Questions à ...

GUY ROSIER

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

Alors que la CNIL a engagé plus de cent procédures de sanction en 2006, seuls onze organismes ont été sanctionnés. Comment expliquer cette différence ?

Comme vous le savez, la loi informatique et libertés, telle qu'elle a été modifiée en août 2004, prévoit que la CNIL peut prononcer un avertissement à l'égard du responsable de traitement n'ayant pas respecté les obligations fixées par la loi et également mettre en demeure ce responsable de faire cesser le manquement constaté, dans un délai de dix jours à trois mois, selon les cas.

La mise en demeure constitue donc une étape déterminante de la procédure de sanction, excepté l'avertissement. Aussi, pour juger de l'efficacité du dispositif établi à cet effet, il faut considérer le nombre de décisions de cette nature prononcées dans l'année par la CNIL. Il y en a eu 94 en 2006, étant précisé que, dans 82 % des cas, les organismes en cause s'étant conformés aux demandes de la CNIL, il a alors été mis fin à la procédure de sanction engagée, ainsi que le prévoit la loi.

Ce résultat vous paraît-il satisfaisant ?

Entièrement ! Quand on relève que 82 % des « mis en demeure » ont, en définitive, suivi les préconisations de la CNIL, on ne peut que constater qu'une telle procédure fonctionne bien. C'est un succès pour l'action de la Commission et, au-delà, la protection des droits des citoyens.

Pourquoi procéder à une mise en demeure ?

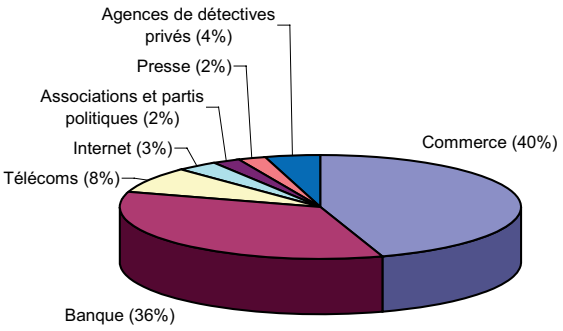
Cette mesure peut être adoptée dans trois situations, en vue de faire respecter :
– l'accomplissement des formalités préalables requises par la loi. Par exemple, lorsque la CNIL n'a pas été saisie d'une demande d'autorisation préalable à la mise en place d'un fichier d'exclusion ou d'un dispositif biométrique ou n'a pas reçu de réponses aux questions posées dans le cadre de ses pouvoirs d'investigation (instruction d'une plainte ou d'une déclaration) ;
– une règle consacrée dans la loi. Il en est ainsi, quand il faut assurer la sécurité des dossiers ou supprimer des informations non pertinentes ou périmées ;
– les droits des personnes. C'est le cas pour la suppression d'un nom sur une « liste noire », lorsque la justification d'une telle inscription n'est pas apportée ou encore pour la reconnaissance par une personne de l'exercice de ses droits d'accès, de rectification ou d'opposition.

Qu'est-ce que c'est ?

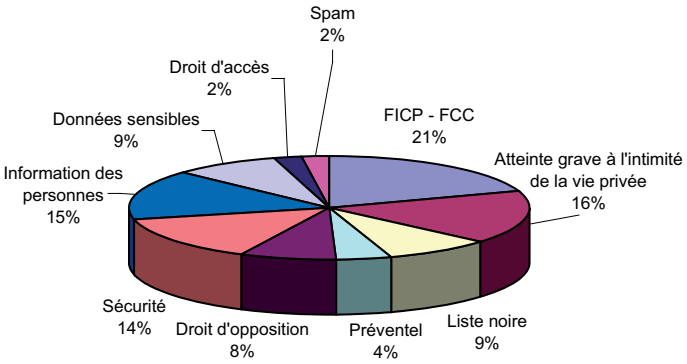
LA FORMATION RESTREINTE

Il s'agit de la formation contentieuse créée en 2004 par le législateur et composée de six commissaires ayant le pouvoir de prononcer des sanctions.

Typologie des dossiers présentés en formation restreinte - secteur privé



Typologie des manquements constatés par la formation restreinte - manquements de fond



Questions à ...

PHILIPPE NOGRIX

Sénateur de l'Ille-et-Vilaine
Commissaire en charge du secteur «Monnaie et crédit»
Rapporteur en formation restreinte dans le dossier Crédit Lyonnais

En quoi la décision de sanction du Crédit Lyonnais vous paraît-elle exemplaire ?

La décision de sanction financière d'un montant de 45 000 euros prise à l'encontre du Crédit Lyonnais est fondamentale, et ceci pour deux raisons.

La CNIL a tout d'abord sanctionné une pratique qu'elle estime être particulièrement stigmatisante pour les personnes concernées, à savoir le fichage abusif dans les fichiers de la Banque de France. Ce faisant, la CNIL entend utiliser ses nouveaux pouvoirs de sanction afin de garantir le respect des droits fondamentaux des personnes.

Mais la CNIL a également sanctionné le manque de coopération dont il avait été fait preuve dans le cas d'espèce. Il convient ainsi de rappeler qu'aux termes de la loi informatique et libertés, tout responsable de traitement est tenu à une stricte obligation de collaboration et de transparence vis-à-vis de la CNIL.

Au-delà, je crois au caractère pédagogique des décisions de sanction prononcées par la CNIL. Par la prise de conscience qu'elle a entraînée, la décision Crédit Lyonnais a eu des répercussions positives au sein de l'ensemble de la profession bancaire.

À la lumière de cette première expérience, considérez-vous que la possibilité de prononcer des sanctions pécuniaires va changer le rapport CNIL/responsables de traitement ?

La CNIL est une institution multiforme qui dispose, par la loi, d'une multitude de compétences très différentes. Tenue à une obligation de conseil à l'égard des responsables de traitement, elle est également une autorité de contrôle (contrôle des déclarations, instruction des plaintes et missions de vérification sur place) et, désormais, une autorité de sanction.

Dans ce contexte, la CNIL s'engage, vis-à-vis de ses interlocuteurs, dans une démarche cohérente où la mise en œuvre d'une procédure de sanction n'est que l'aboutissement d'un long processus, lorsque les étapes préalables du conseil et du contrôle se sont avérées insuffisantes à engager par exemple une entreprise dans une démarche de mise en conformité.

Le conseil, la recommandation et la persuasion sont préférables à l'injonction et à la contrainte. C'est donc le bon sens et l'intérêt stratégique qui justifient tout d'abord la mise en œuvre d'un partenariat entre la CNIL et les responsables de traitement. Pour autant, il faut clairement reconnaître que les nouveaux pouvoirs dont dispose aujourd'hui la CNIL modifient le regard que portent les responsables de traitement sur la réglementation. En effet, il est indéniable que le risque d'image et le risque juridique liés à l'exploitation de données personnelles sont plus importants qu'ils ne l'étaient hier.

LA PROSPECTION POLITIQUE : ANTICIPER 2007

Dans la perspective des échéances électorales de 2007 et 2008, la CNIL a entendu les professionnels du marketing direct et les gestionnaires de bases de données et organisé une table ronde réunissant les partis politiques. Elle a ensuite adopté, le 5 octobre 2006, une recommandation sur la protection des données personnelles lors d'opérations de prospection politique.

La Commission a ainsi rappelé que certains fichiers ne peuvent en aucun cas être utilisés à des fins de prospection politique (par exemple, les fichiers des administrations ou des collectivités locales tels que les registres d'état civil, les fichiers de taxes et de redevances ou encore les fichiers d'aide sociale). La liste électorale, elle, peut être communiquée à quiconque pour une utilisation de prospection politique. Aucune disposition de la loi n'interdit à un parti ou à un candidat d'utiliser les mêmes moyens de prospection que ceux utilisés en matière commerciale, tels que la location de fichiers auprès de sociétés spécialisées.

Néanmoins, la Commission a estimé que la sensibilité particulière des opérations de prospection politique impose une information claire et transparente des personnes sur les conditions d'utilisation de leurs données.

C'est votre droit

Lors de la collecte de leurs données, les personnes doivent ainsi avoir été averties de la possible utilisation de leurs données à des fins de prospection politique et mises en mesure de s'opposer à la transmission de leurs données à des tiers. En matière de prospection politique opérée par courrier électronique, la CNIL a souhaité aligner le régime protecteur que la loi prévoit en matière commerciale à la prospection politique : seules les personnes qui y ont expressément consenti peuvent être démarchées par voie électronique.

Surtout, il est apparu indispensable d'améliorer l'information des personnes lorsqu'elles recevaient un message de nature politique : elles peuvent, en effet, avoir l'impression d'être « fichées » par le parti ou l'élu à l'origine du message. C'est pourquoi, la CNIL recommande que le message reçu précise l'origine du ou des fichiers utilisés, le fait que le parti ou l'élu ne dispose pas de l'adresse utilisée mais a eu recours à un prestataire extérieur et le moyen dont la personne dispose pour s'opposer à la réception de tels messages.

Enfin, la CNIL recommande aux partis et aux élus de ne pas utiliser des moyens de prospection qui pourraient être jugés particulièrement intrusifs par les personnes démarchées, tels que les automates d'appel ou les télécopieurs, ou qui ne permettent pas de délivrer une information complète (les SMS sont limités à 160 caractères).

Les opérations de parrainage, qui conduisent les partis ou élus à s'adresser à des personnes qui n'ont pas fourni elles-mêmes leurs coordonnées, doivent préciser que les coordonnées de la personne parrainée sont effacées à l'issue de cette opération et l'identité de la personne (le parrain) qui a transmis au parti ou à l'élu les coordonnées de la personne démarchée.

La recommandation de la Commission rappelle aussi les conditions dans lesquelles les partis doivent gérer, au regard de la loi informatique et libertés, leurs propres fichiers d'adhérents, de militants, d'internautes, etc. : information des personnes, exercice facilité de leurs droits et mise en place de mesures de confidentialité.

Enfin, la Commission a décidé, d'une part, d'actualiser sa norme simplifiée n° 34 afin de permettre aux partis, élus ou candidats de pouvoir déclarer simplement leurs fichiers utilisés à des fins de communication politique et, d'autre part, d'éditer un guide pratique qui reprend les principales règles établies par la CNIL dans le cadre de sa recommandation du 5 octobre 2006.

LE DOSSIER UNIQUE DU DEMANDEUR D'EMPLOI

La loi du 18 janvier 2005 de programmation sociale a redéfini le champ du service public de l'emploi, qui regroupe désormais les actions de placement, d'indemnisation, d'insertion, de formation et d'accompagnement des demandeurs d'emploi.

Techniquement, le dossier unique est une interface permettant la consultation de données déjà contenues dans les bases de données de l'ANPE et de l'Unedic, mais aussi la saisie en ligne d'informations relatives au demandeur d'emploi. Les données sont conservées pendant un an à compter de la date d'annulation de la demande d'emploi.

Lors de l'examen de ce nouveau système d'information, le 26 octobre 2006, la Commission a été particulièrement vigilante sur les garanties de confidentialité apportées, notamment par la définition de règles d'habilitation d'accès très précises.

Qu'est-ce que c'est ?

LE DUDE

Élément clé du « plan de cohésion sociale », le déploiement du dossier unique du demandeur d'emploi (DUDE) a été rendu possible par la signature, le 5 mai 2006, de deux conventions tripartites entre l'État, l'ANPE et l'Unedic.
Le dossier unique vise à simplifier les démarches des demandeurs d'emploi en leur évitant d'avoir à constituer un nouveau dossier auprès des différents acteurs chargés de leur prise en charge, qu'il s'agisse des services et institutions qui constituent le service public de l'emploi ou de ceux qui y participent (maisons de l'emploi, sociétés d'intérim), et à améliorer la cohérence des actions d'accompagnement menées par ces derniers.
Des annexes précisent notamment la liste des données traitées, les règles de sécurité et de gestion des habilitations d'accès.

Questions à …

HUBERT BOUCHET

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

Qui peut accéder au dossier unique du demandeur d'emploi (DUDE) ?

Le DUDE n'est accessible dans sa totalité qu'aux agents habilités de l'ANPE, des institutions de l'assurance chômage, et des services du ministère de l'Emploi, dans le cadre de leurs missions légales. Le personnel des partenaires ou des prestataires doit être dûment habilité et n'accédera qu'aux seules informations pertinentes, définies par une convention de partenariat ou par un contrat d'adhésion, et pour les seuls publics relevant de leur champ de compétence et de leur territoire géographique.

La CNIL a relevé que l'accès au DUDE est subordonné, pour tous les personnels utilisateurs, à une procédure individuelle d'habilitation comportant une obligation de formation spécifique sur les objectifs de mise à disposition de données *via* le dossier unique, la déontologie et les règles de confidentialité.

Chaque personne habilitée à accéder au DUDE s'engage en outre, par la signature d'un engagement de confidentialité, à respecter des règles de sécurité.

La Commission a insisté sur la nécessité que l'accès à certaines données relatives à l'historique professionnel du demandeur d'emploi (historique des emplois exercés, identification des anciens employeurs, périodes de suspension d'activité) soit différencié, pour les partenaires et prestataires, en fonction de leurs besoins et de leurs missions.

Le DUDE comporte trois zones de saisie libre (se rapportant à la formation, aux entretiens professionnels et aux actions menées pour le retour à l'emploi), qui ne devraient comporter que des informations objectives, pertinentes et strictement nécessaires.

Un correspondant sécurité des systèmes d'information pour la mise en œuvre du DUDE est systématiquement désigné au niveau local ou national. La Commission a invité les acteurs du service public de l'emploi à envisager également la désignation, à court terme, de correspondants informatique et libertés.

La CNIL sera-t-elle à nouveau amenée à se prononcer en 2007 ?

Des évolutions importantes devront être examinées en 2007 par la CNIL, notamment la mise en place de liaisons directes vers les systèmes d'informations de partenaires institutionnels, mais également et surtout, le remplacement de l'actuelle liaison informatisée entre l'Assedic et les Directions départementales du travail et de l'emploi pour le contrôle des demandeurs d'emploi indemnisés (LICRE) par un module intégré au dossier unique. Autant de traitements informatiques qui visent à simplifier la vie du demandeur d'emploi et assurer la cohérence des actions d'accompagnement le concernant dans le respect le plus strict de la loi informatique et libertés.

SÉCURITÉ CONTRE PROTECTION DES DONNÉES : le grand débat transatlantique

L'affaire SWIFT : quand les autorités américaines surveillent les transferts bancaires internationaux

La presse américaine a révélé le 23 juin 2006 l'existence d'un programme de surveillance de la finance internationale mis en place par la CIA depuis les attentats du 11 septembre 2001. Ces révélations ont notamment porté sur le fait que la CIA et le département du Trésor américain surveillent, depuis des années, des millions de données transitant par SWIFT. Cette surveillance, que les autorités américaines et SWIFT déclarent être uniquement liée à la poursuite d'objectifs liés à la lutte contre le financement du terrorisme, concerne non seulement des transferts financiers vers les États-Unis, mais également des transferts domestiques ou intra-UE. Cette surveillance a été réalisée sans information préalable des autorités publiques européennes ou nationales, et hors du cadre légal de coopération normalement établi à ces fins.

Dès sa révélation, les institutions européennes (Commission, Parlement, puis Conseil) se sont saisies de cette affaire afin de se prononcer sur le soupçon de surveillance irrégulière du réseau SWIFT au regard des règles européennes de protection des données personnelles.

À l'issue de sa session plénière des 21 et 22 novembre 2006, le G29 a considéré que la société SWIFT n'avait pas respecté les règles européennes de protection des données, notamment en prêtant un concours actif à la mise en œuvre du programme de surveillance des données bancaires et financières par les autorités américaines. Le Groupe a également considéré que les institutions financières ont une part de responsabilité dans cette affaire. Il a également invité les banques centrales du G10 à mener une réflexion sur la forme de surveillance qu'elles se doivent d'exercer sur SWIFT.

La CNIL a participé à la rédaction de cet avis, en totale coopération avec ses homologues. Elle participe également aux travaux de suivi de la mise en œuvre de cet avis. À cet effet, elle a pris contact avec les institutions françaises concernées (ministère de l'Économie et des Finances, Banque de France, notamment) ainsi qu'avec la Fédération bancaire française et les institutions financières concernées.

Différentes hypothèses étaient évoquées, fin 2006, quant à la manière de régler cette affaire. La CNIL, comme le G29, insiste sur le fait que, quelle que soit l'hypothèse retenue, les acteurs européens concernés (gouvernements nationaux de l'UE, Commission, Banque centrale européenne) doivent placer la protection des libertés des citoyens de l'UE ainsi que le maintien de la souveraineté économique européenne au cœur de leurs travaux.

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 à ses clients des secteurs bancaire et financier un ensemble de services, dont un système de messagerie sécurisée et standardisée assorti d'une palette de services financiers. Une grande partie des transferts bancaires internationaux transite aujourd'hui par cette société, dont les services sont devenus incontournables pour les milieux concernés. À l'horizon 2008, SWIFT devrait en outre être au cœur du futur Système européen des systèmes de paiement (SEPA), dont il constituera le système par défaut. L'intégralité des ordres de paiement nationaux, européens ou internationaux, transitera donc à terme par ce réseau.

Le nouvel accord PNR

Peu après les attentats terroristes du 11 septembre 2001, les États-Unis ont exigé des compagnies aériennes européennes opérant des vols vers leur territoire, ou traversant simplement celui-ci, que les données PNR sur chaque passager leur soient transmises.

En 2004, l'Union européenne et les États-Unis avaient difficilement conclu un accord pour légaliser ces transferts. Ce compromis a été annulé par un jugement du 30 mai 2006 de la Cour de justice européenne, saisie par le

Parlement européen, au motif que l'accord reposait sur une base juridique erronée. La Cour a également fixé la date butoir au 30 septembre 2006 pour la conclusion d'un nouvel accord.

Dans deux avis des 14 juin et 27 septembre 2006, la CNIL et ses homologues, réunis au sein du groupe de l'article 29, rappelaient la nécessité que le nouvel accord à conclure consacre un niveau de sécurité juridique et de protection des personnes supérieur ou, à tout le moins, équivalent à celui mis en place par l'accord du 14 mai 2004.

Un accord n'a été conclu que le 6 octobre 2006, après de longues et difficiles négociations. Malgré les exigences américaines de départ, le compromis maintient inchangés les types de données accessibles mais prévoit un élargissement des destinataires des données PNR : le département de la Sécurité intérieure américain pourra les transférer au FBI et à la CIA. La durée de conservation reste de trois ans et demi.

En outre, dans l'attente de la mise en place d'un système « push » dans lequel les compagnies aériennes seront maîtresses des données consultées par les autorités américaines, celles-ci sont autorisées à extraire les données PNR directement des bases de données des compagnies aériennes (« pull »).

Qu'est-ce que c'est ?

LES PNR

De manière générale, les compagnies aériennes et les agences de voyage collectent ces informations auprès des passagers dans le cadre des services de réservation. Stockées dans les bases de données des systèmes de réservation, elles sont échangées entre les entreprises intervenantes du moment de la réservation jusqu'à la réalisation des prestations demandées par les passagers. Les données présentes dans ces bases prennent la forme d'enregistrements d'informations standardisés sur le plan international dénommés « PNR » *(Passenger Name Record)*.

À noter que l'accord va régir le transfert des données jusqu'au 31 juillet 2007, date à laquelle un nouveau compromis devra être négocié. L'Union européenne et les États-Unis ont repris les négociations en vue d'un accord définitif dès le mois de novembre 2006. La CNIL et ses homologues européens suivront avec la plus grande attention ces négociations, afin de veiller au respect des droits et libertés des personnes.

Questions à …

GEORGES DE LA LOYÈRE

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

Pourquoi le précédent accord PNR était-il insatisfaisant ?

Depuis les attentats du 11 septembre 2001, les autorités américaines ont mis la question de la sécurité des transports aériens en haut de leurs préoccupations. Ainsi, toutes les compagnies aériennes qui desservent ou simplement survolent le territoire américain doivent fournir une série de données (PNR) sur chacun des passagers qu'elles embarquent.

Que la vérification des identités et le contrôle avant embarquement soient nécessaires au regard des impératifs de sécurité, nul n'en doute. Mais le nombre de transferts opérés et l'abondance des renseignements fournis – 34 rubriques par voyageur – paraissent excessifs au regard des objectifs poursuivis. Ces transferts ne sont encadrés par aucune autorité de contrôle.

Quels sont les objectifs de la CNIL dans le contexte de la négociation du nouvel accord ?

La Cour de justice européenne, sans se prononcer sur le fond, a considéré que la base juridique sur laquelle reposait le principe de l'accord PNR – États-Unis – Europe n'était pas soutenable puisque sa finalité, la sécurité publique, se trouvait être hors du champ communautaire. L'enjeu pour nos autorités de contrôle va être de veiller à ce que le nouvel accord soit plus protecteur que le précédent ou pour le moins d'éviter une diminution des garanties prévues.

Peut-on parler d'un « déséquilibre transatlantique » dans cette affaire ?

La partie américaine va continuer à exercer des pressions considérables grâce au traitement des *No fly lists* (listes de passagers indésirables aux États-Unis, fournies par les autorités américaines aux compagnies aériennes). Elles contiennent des dizaines de milliers de noms sans aucune garantie sur la qualité de ces fichiers. Elle entend aussi imposer la collecte et la conservation de données concernant les problèmes de santé et notamment la propagation des maladies infectieuses telles que la grippe aviaire.

Il s'agit maintenant, pour nos autorités de contrôle agissant conjointement au niveau européen, et pour la CNIL en particulier de proposer un juste équilibre entre la sécurité à laquelle tout le monde aspire et des transferts anarchiques de données plus ou moins sensibles contraires à nos principes.

LA VIE DE LA CNIL

LA CNIL EN CHIFFRES

Les délibérations de la CNIL

En 2006, la CNIL a siégé 39 fois au cours de 25 séances plénières, 9 formations restreintes, 5 bureaux délibératifs. Ces réunions ont conduit à l'adoption de **299 délibérations**. Pour mémoire, la CNIL a connu une augmentation de 570% de son activité en trois ans (2003 à 2006).

Au titre du conseil et de l'expertise

9 avis sur projet de loi ou de décret, parmi lesquels l'avis sur le projet de loi relatif à la prévention de la délinquance, l'avis sur un projet de ratification d'un Traité relatif à la coopération transfrontalière en vue de lutter contre le terrorisme, la criminalité et la migration illégale, l'avis sur un projet de décret visant la lutte contre le terrorisme.

2 recommandations, l'une concernant les fichiers des partis politiques et des élus ou candidats à des fonctions électives dans le cadre de leurs activités politiques, l'autre encadrant les dispositifs de géolocalisation des véhicules utilisés par des salariés.

Au titre des sanctions

11 sanctions pécuniaires d'un montant total de 168 000 euros correspondant à des amendes allant de 300 à 45 000 euros.

7 injonctions de cesser ou de modifier un traitement de données personnelles et **94 mises en demeure.**

4 avertissements concernant deux opérateurs de télécommunications, une banque et un parti politique.

Au titre de la simplification

4 normes simplifiées

5 dispenses de déclaration exonérant de toute formalité déclarative certains traitements.

8 autorisations uniques auxquelles peuvent se conformer d'autres traitements de même nature.

1 avis sur un acte réglementaire unique auquel peuvent se rattacher les traitements de données personnelles relatifs aux espaces numériques de travail « ENT ».

La liste complète des mesures de simplification se trouve en annexe de ce rapport.

Au titre des formalités déclaratives

132 autorisations

19 refus d'autorisation concernant en particulier des contrôles de salariés par le biais de l'empreinte digitale, ou certaines utilisations du numéro de sécurité sociale, ou encore des traitements de données fondés sur la consonance des noms.

17 avis sur des traitements sensibles ou à risques se rapportant par exemple au placement sous surveillance électronique mobile, aux réquisitions télématiques ou informatiques, aux données des passagers aériens ou encore au fichier national des personnes recherchées.

Comment ça marche ?

Les membres de la CNIL se réunissent en séance plénière environ une fois par semaine sur un ordre du jour établi à l'initiative de leur président. Une partie importante de ces séances est consacrée à l'examen de projets de loi et de décrets soumis à la CNIL pour avis par le Gouvernement. Lors de ces séances plénières, la Commission adopte aussi des délibérations qui sont des avis ou des autorisations sur des traitements ou des fichiers. Parfois, c'est le bureau, constitué du président et des deux vice-présidents, qui adopte ces délibérations. En ce qui concerne les sanctions, la compétence a été confiée en 2004 à la formation restreinte de la CNIL, composée de six de ses membres. Enfin, nombre de rapports font le point sur les évolutions de l'informatique afin d'éclairer les membres de la CNIL dans la conduite de leurs missions. Compte tenu de la grande variété des dossiers que la CNIL doit traiter, une répartition par secteur d'activité est établie entre les commissaires. Celle-ci a l'avantage d'instaurer une forme de spécialisation et de faciliter les contacts des commissaires avec les responsables de traitements. Néanmoins, les délibérations de la CNIL sont débattues selon les principes de la collégialité.

Les saisines de la CNIL

Comment ça marche ?

Dans ses missions, la CNIL répond aux demandes de conseil qui lui sont adressées par des responsables de fichiers, instruit les plaintes dont elle est saisie par les citoyens, procède aux vérifications nécessaires dans le cadre du droit d'accès indirect aux fichiers intéressant la sécurité publique et la sûreté de l'État.

En 2006, la CNIL a reçu **5 167 saisines** qui correspondent à **3 572 plaintes** et **1 595 demandes** de droit d'accès indirect aux fichiers de police et de gendarmerie.

Les secteurs d'activité qui, par ordre décroissant, ont suscité le nombre le plus important de plaintes sont : Prospection commerciale – Banque – Travail – Télécommunications. L'objet le plus fréquent des plaintes est l'opposition à figurer dans un traitement.

Les plaintes fondent les deux tiers des dossiers examinés par la formation restreinte de la CNIL qui est en charge de prononcer des sanctions. De même, 25 % des missions de contrôle effectuées par la CNIL trouvent leur origine dans des plaintes de personnes ou des signalements effectués par le biais du site Internet de la CNIL. Enfin, il faut noter qu'à la suite d'une plainte du Conseil représentatif des institutions juives de France (CRIF), la CNIL a décidé de dénoncer au parquet de (s) responsable (s) d'un site web diffusant une liste de personnes publiques présentées comme étant de confession juive.

Les chiffres du quotidien

Chaque jour, en moyenne, la CNIL :

- **répond à 475 appels téléphoniques ;**
- **reçoit 70 courriers ;**
- **enregistre 285 nouveaux traitements de données ;**
- **reçoit 15 plaintes.**

Les déclarations de fichiers à la CNIL

Pour la période du 1er janvier au 31 décembre 2006, la CNIL a enregistré 72 000 nouveaux traitements de données personnelles et 1 800 déclarations de modification de traitements déjà déclarés, soit au final **73 800 dossiers** à gérer sur l'année. Le nombre global annuel de déclarations de fichiers à la CNIL tend à se stabiliser depuis la réforme de la loi informatique et libertés de 2004 qui a permis d'exonérer de toutes formalités déclaratives les fichiers qui ne posent pas de difficultés sur le plan de la protection des données et de dispenser de certaines déclarations lorsqu'un correspondant informatique et libertés est désigné. Ces évolutions ont certes pour effet de contenir le flux de déclarations de fichiers, mais elles traduisent en réalité une augmentation d'activité de la CNIL qui a trait par exemple à la formation des correspondants ou bien à la production de normes d'exonération.

Depuis 1978, ce sont au total 1 160 000 fichiers qui ont été déclarés à la CNIL.

Les chiffres à la loupe

En 2006, la CNIL a :

- **enregistré 73 800 traitements de données nominatives ;**
- **reçu 3 572 plaintes ;**
- **adopté 299 délibérations ;**
- **contrôlé 127 organismes ;**
- **adressé 94 mises en demeure ;**
- **adressé 4 avertissements ;**
- **prononcé 11 sanctions financières (soit 168 000 euros).**

Les moyens

Le personnel

La CNIL dispose de **95 postes budgétaires en 2006**, ce qui la place au même niveau que des pays de l'Union européenne à la population bien moindre, tels que la République tchèque (10 millions d'habitants et 113 agents). Ainsi, au sein des 27 pays membres de l'Union européenne, la France se situe parmi les trois dernières nations en termes de nombre d'agents alloués à l'autorité de protection des données. À titre d'exemple, le Royaume-Uni et l'Allemagne ont respectivement doté leurs « CNIL » nationales de 270 et 400 agents.

Dans ce contexte, la CNIL a obtenu la création de 10 postes supplémentaires pour 2007, conformément au programme 2006-2009 de développement de ses ressources, dit « plan de rattrapage », présenté au Premier ministre au mois de mars 2005. Cependant, ce plan se révèle déjà notoirement insuffisant.

En effet, entre 2003 et 2006, les saisines et délibérations de la CNIL ont augmenté de 570% ! Les nouvelles missions dévolues à la CNIL par le législateur en août 2004, à savoir le développement des missions de contrôles, des sanctions, des correspondants informatique et libertés dans les entreprises et les administrations, de l'information du public requièrent toujours davantage de ressources humaines. Ainsi, si la CNIL a réalisé près de 130 contrôles en 2006, soit une augmentation de près de 30% par rapport à 2005, l'autorité espagnole de protection des données en effectuait pour sa part plus de 600 au cours de cette même année !

Le budget

L'effort consenti par le Gouvernement pour tenter de « mettre à niveau » les moyens de la CNIL au regard de ses missions et de ses homologues européens s'observe au travers des évolutions du budget délégué 2006. En effet, ce dernier augmente de 25% par rapport à 2005 en raison de l'accroissement de ses effectifs et de la concrétisation du projet de déménagement de la CNIL. Désormais regroupée sur un site unique (et non plus sur trois), ce qui est un gage d'efficacité et de rationalité, la CNIL dispose de locaux lui permettant, notamment, d'améliorer l'accueil du public et d'assurer la formation des correspondants informatique et libertés.

Cependant, l'augmentation de ses charges immobilières, de +124%, absorbe une part considérable des ressources budgétaires, au détriment des dépenses d'informatique et de fonctionnement courant. À titre d'illustration, les dépenses courantes (c'est-à-dire les dépenses hors immobilier et informatique) par agent atteignaient 9960 euros par agent en 2007 contre 12770 euros en 2002 (soit une baisse de 22%).

En outre, en 2007, la CNIL ne disposera toujours pas des ressources suffisantes pour engager une véritable politique d'information des citoyens, le budget consacré à cette action atteignant 90000 euros contre 3 millions au Royaume-Uni !

en millions d'euros	2005	2006	2007	% 05-06	% 06-07
Budget total voté (LFI)	7,121	8,999	9,880	26%	10%
Budget délégué	7,315	9,112	9,683	25%	6%
Dépenses de personnel	4,848	5,325	6,116	10%	15%
Dépenses de fonctionnement	2,467	3,787	3,568	54%	-6%

Execution du budget

	2005	2006	2007 prev	% 05-06	% 06-07
Immobilier	0,934	2,092	2,193	124%	5%
Informatique	0,589	0,610	0,502	4%	-18%
Dépenses courantes	0,945	1,137	0,801	20%	-30%
Total Fonctionnement	2,467	3,839	3,496	56%	-9%

POUR UNE MEILLEURE DÉFENSE DES DROITS

La CNIL instruit les plaintes

Comme chaque année, la CNIL a reçu, en 2006, des milliers de plaintes (3 572) dénonçant le non-respect de la loi informatique et libertés. Les plaignants sont très souvent des particuliers qui rencontrent des difficultés dans leur vie quotidienne à cause de leur présence injustifiée dans un fichier ou de l'impossibilité de consulter leur dossier personnel ou d'en demander la modification en cas d'erreur.

Ces plaintes sont donc autant d'appels à l'aide pour débloquer des situations parfois très préjudiciables pour les personnes qui en sont victimes et pour garantir la bonne application de la loi par les services publics, les entreprises et les associations.

Si le service des plaintes ne peut malheureusement pas traiter toutes les demandes, faute de moyens, son intervention auprès des responsables de fichiers permet de trouver une issue favorable à nombre de situations. Il a également la possibilité de proposer, si nécessaire, des contrôles sur place et des sanctions.

Ces cinq petites histoires (vraies) permettent d'illustrer l'action conduite chaque jour par la CNIL en faveur des particuliers.

LA MAISON FAIT À NOUVEAU CRÉDIT

▶ Monsieur A. est inscrit par une banque au Fichier national des incidents de remboursement des crédits aux particuliers (FICP). N'étant pas co-emprunteur, contrairement à ce que prétend la banque, il adresse une plainte à la CNIL pour inscription abusive au FICP.

La CNIL demande à l'établissement bancaire des explications sur le cas de M. A.

En réponse, la banque confirme à la CNIL que le plaignant, qui était bien indiqué comme co-emprunteur sur le formulaire contractuel, n'a jamais signé celui-ci. L'inscription de M. A. au FICP est donc immédiatement annulée.

Grâce à l'intervention de la CNIL, M. A. peut à nouveau déposer sereinement une demande de crédit auprès de l'ensemble des banques établies en France.

ANNUAIRES ET RISQUES D'ATTEINTE À LA VIE PRIVÉE

▶ Madame P., fonctionnaire de police, souscrit deux abonnements de téléphonie mobile, dont un pour sa fille mineure.

Quelque temps après, sa fille reçoit sur son téléphone mobile des appels menaçants et injurieux à l'encontre de Mme P. Cette dernière découvre ainsi que ses coordonnées (adresse, plan d'accès et numéro de téléphone mobile) apparaissent dans les annuaires diffusés sur Internet.

Mme P. demande par téléphone et par courrier à l'opérateur la suppression de ses coordonnées des annuaires. L'opérateur lui oppose une fin de non-recevoir. Mme P. qui n'a jamais figuré dans l'annuaire compte tenu de son activité professionnelle, craint pour sa sécurité et celle de sa fille. Elle saisit alors la CNIL d'une plainte.

La CNIL demande à l'opérateur la suppression immédiate des coordonnées de la plaignante des annuaires.

Rapidement, l'opérateur adresse à Mme P. un courrier l'informant que ses coordonnées n'apparaîtront plus dans les annuaires. Il lui propose également de changer gratuitement de numéro de téléphone.

TRANSPARENCE ASSURÉE !

▶ Madame F. est en arrêt de travail. Elle est indemnisée grâce au contrat de prévoyance souscrit auprès d'une compagnie d'assurance.

À la demande de son assureur, Mme F. passe une expertise médicale auprès d'un médecin. Les conclusions de cette expertise conduisent la compagnie d'assurance à cesser de verser à Mme F. ses indemnités journalières.

Dès février 2006, le médecin traitant de Mme F. réclame la copie du compte rendu d'expertise médicale. Après des demandes renouvelées, il reçoit en août 2006 les seules conclusions du rapport et non son intégralité.

Début octobre, Mme F. envoie une lettre recommandée avec accusé de réception à son assureur pour demander, conformément à la loi informatique et libertés, la transmission de l'intégralité du rapport d'expertise médicale. N'ayant reçu aucune réponse, elle saisit la CNIL en novembre.

Quelques jours après l'intervention de la CNIL, la totalité du dossier établi par le médecin expert est enfin transmise au médecin de la plaignante. Mme F a ainsi pu faire valoir ses droits à indemnités journalières.

DROIT À LA TRANQUILLITÉ

▶ Monsieur D. reçoit quotidiennement sur son télécopieur des sollicitations commerciales pour l'achat de matériel informatique, émanant d'une société dont il a été client.

Depuis le mois d'avril 2006, il demande pourtant à cette société de cesser ses pratiques par courriers électroniques, téléphone et courrier recommandé avec accusé de réception. Il porte même plainte auprès du procureur de la République pour non-respect de son droit d'opposition.

Le harcèlement publicitaire se poursuivant malgré toutes ses démarches, il saisit la CNIL d'une plainte en septembre.

La CNIL demande alors à l'entreprise de respecter le droit d'opposition de M. D. Quelques jours plus tard, la CNIL est informée que les coordonnées de M. D. ne sont plus enregistrées dans les bases de données de cette entreprise.

MAUVAISSOUVENIRS.COM

▶ Madame B. alerte la CNIL après avoir constaté que la saisie, sur un moteur de recherche, des nom et prénom de sa fille mineure renvoie sur différents sites Internet spécialisés dans la diffusion de décisions de justice.

Ces sites laissent apparaître que la fille de la plaignante a été, dans le passé, témoin d'une affaire pénale dans laquelle son père a été condamné.

La CNIL appelle sans délai l'attention du responsable des trois sites sur sa recommandation du 29 novembre 2001. Cette recommandation pose le principe de l'anonymisation des décisions de justice diffusées sur Internet, afin de préserver notamment la vie privée des parties et témoins au procès.

Le responsable des sites fait alors le nécessaire pour se conformer aux demandes de la CNIL. La jeune fille ne craint plus désormais que cet épisode douloureux de sa vie soit accessible à tous sur Internet.

La CNIL reçoit des signalements

Tout citoyen peut désormais témoigner sur le site de la CNIL (www.cnil.fr) des difficultés qu'il rencontre au quotidien en matière de protection des données personnelles. La CNIL a en effet mis en ligne, en mars 2006, un formulaire permettant à toute personne de l'informer de toute difficulté dont elle aurait connaissance et, si elle le souhaite, de l'identité de l'organisme concerné.

Depuis la mise en œuvre de ce système d'alerte, la CNIL reçoit plusieurs centaines de messages chaque semaine. Ces témoignages, qui ne constituent pas des plaintes et ne font donc pas l'objet d'un traitement individuel, permettent à la Commission de mieux connaître la réalité des problèmes auxquels les citoyens sont confrontés. En fonction des informations ainsi recueillies, la CNIL agit avec les moyens dont elle dispose et en particulier les pouvoirs de contrôle que la loi lui a confiés.

Voici deux exemples dans lesquels la boîte de signalements a permis de faire cesser des manquements importants à la loi informatique et libertés :

▶ Plusieurs internautes signalent qu'ils reçoivent de leur opérateur télécoms des factures téléphoniques concernant d'autres clients. Ces documents précisent l'identité et les coordonnées de ces personnes et apportent des informations sur la nature des communications téléphoniques effectuées. Après enquête, il s'avère qu'une faille de sécurité est détectée dans le dispositif d'archivage électronique du fichier client.

L'intervention de la CNIL a ainsi contribué à résoudre ce problème.

▶ Plusieurs internautes transmettent la copie d'un mail adressé par une société spécialisée dans la réalisation d'enquêtes marketing à plusieurs dizaines de milliers de personnes : « Nous vous offrons 50 euros de chèques cadeaux si vous trouvez l'une des personnes ci-dessous. Nous recherchons (…) des hommes homosexuels vivant en couple (…) des hommes ou des femmes d'origine africaine (…). » Après vérification, la CNIL a constaté que cette société avait ainsi constitué un fichier faisant état de la race ou des mœurs supposées de près de 4 000 personnes, ce qui est formellement interdit par la loi (collecte déloyale, absence du consentement exprès des personnes concernées).

L'intervention de la CNIL a abouti à la suppression pure et simple du fichier.

Exemple de message reçu sur la boîte de signalement

Alerte du : Mardi 06 Fevrier 2007 à 14h44 GMT

Domaine : Travail

Envoyé par : ALAIN[redacted]

Coordonnées de l'organisme mis en cause :

[redacted]

Signalement :

Je travaille en tant que réceptionniste de nuit en hôtellerie. La direction de l'hôtel a installé une caméra de surveillance au motif de connaître les clients de l'hôtel. Cependant je suis filmé dans mes faits et gestes, la présence d'une caméra n'est pas indiquée aux clients. La direction est-elle dans les Lois ou bien à côté?. Quelles actions a effectuées?. Merci d'avance de votre réponse Lyon, le 06 février 2007

La CNIL effectue des contrôles sur place

Les contrôles en 2006

- **127 organismes ont été contrôlés (soit une augmentation de 34,73% par rapport à 2005).**
- **135 déplacements ont été opérés par une délégation de la CNIL (soit une augmentation de 40% par rapport à 2005).**
- **25% des contrôles effectués ont pour origine des plaintes de particuliers (plaintes adressées par courrier à la Commission) ou des « signalements » déposés sur le site Internet de la CNIL par les internautes.**

Les principaux secteurs d'activités contrôlés en 2006[1] sont, compte tenu du programme de contrôles adopté en séance plénière le 6 avril 2006 :

• **Le marketing commercial** :
– contrôles auprès de sociétés spécialisées dans la mise à disposition de tiers de fichiers d'adresses postales ou électroniques (modalités de collecte et de mise à jour des données) ;
– contrôles opérés auprès de sociétés de vente par correspondance, d'opérateurs de téléphonie fixe et mobile, de fournisseurs d'accès à Internet (gestion de leurs fichiers clients, des opérations de prospection, notamment par Internet, etc.) ;
– contrôles de sociétés commerciales auprès desquelles les personnes ont des difficultés à faire valoir leur droit d'opposition à être démarchées ;
– contrôles opérés auprès des principaux constructeurs automobiles implantés en France, afin de vérifier les modalités d'information et d'opposition des personnes quant à l'utilisation à des fins commerciales des données permettant de procéder à l'immatriculation des véhicules (fichier de l'Association auxiliaire de l'automobile).

• **Les agents de recherches privés** (gestion des fichiers, principalement de débiteurs, et modalités de collecte des données) ;

• **L'application de télébillettique Navigo mise en œuvre par la RATP** (vérification des conditions de mise en œuvre des traitements sur lesquels la Commission s'est prononcée à différentes reprises, en particulier par une délibération du 8 avril 2004, et de l'effectivité des engagements pris alors par les acteurs participant au dispositif) ;

• **Le recrutement** (vérification des données gérées afin de s'assurer notamment de l'absence de toute politique de discrimination).

Par ailleurs, afin de poursuivre certaines des politiques de contrôles engagées en 2005, des vérifications sur place ont été menées auprès de collectivités locales, auprès d'organismes ayant installé des applications faisant appel à des procédés biométriques (établissements scolaires, hôtels ou foyers d'hébergement, clubs de sport, etc.) ou des systèmes de vidéosurveillance.

Dans le cadre de la coopération internationale, des contrôles sur pièces ont été conduits, à partir d'un questionnaire-type établi au niveau européen, auprès de dix organismes implantés en France proposant des contrats d'assurance complémentaires en matière de santé. Au vu des réponses adressées à la CNIL dans ce cadre, l'un d'entre eux a fait l'objet d'une mise en demeure. Il a été décidé, pour deux autres d'entre eux, de vérifier, notamment d'un point de vue technique, que les mesures décrites sont effectivement mises en œuvre.

Une série de contrôles a été effectuée auprès de chacun des six hébergeurs participant à l'expérimentation du dossier médical personnel (DMP). Les constats opérés lors des missions de vérifications, auxquelles, pour la première fois depuis l'entrée en vigueur des nouvelles dispositions de la loi du 6 janvier 1978 modifiée le 6 août 2004 et de son décret d'application du 20 octobre 2005, des médecins inspecteurs de santé publique étaient associés, ont permis à la CNIL d'être mieux informée du dispositif mis en œuvre avant de se prononcer en 2007 sur sa généralisation[2].

De la même manière, pour la première fois depuis l'entrée en vigueur de la loi modifiée, un contrôle a dû être opéré, en raison du refus opposé dans un premier temps par le responsable des lieux, sur autorisation du président du tribunal de grande instance territorialement compétent (Créteil) et, dans le cas d'espèce, en présence du commissaire de police local.

Enfin, la procédure de convocation prévue par l'article 44 de la loi a été utilisée par la Commission à la suite d'un contrôle opéré en province auprès d'un service déconcentré, dont il est apparu que les manquements à la loi constatés relevaient en fait de la responsabilité des instances centrales, seules en mesure d'apporter des modifications au traitement mis en œuvre, de nature à ce qu'il soit conforme à la loi informatique et libertés.

À propos des contrôles

Pratiquement un quart des contrôles ont donné lieu à une délibération de la formation restreinte :
- **31 mises en demeure ;**
- **5 sanctions financières ;**
- **1 avertissement.**

1. *Cf.* Liste des organismes contrôlés en annexe.

2. *Cf. infra* « Le dossier médical personnel », p. 63.

HISTOIRE D'UN CONTRÔLE

Affaire de spam !

La CNIL a été saisie de plaintes portant sur la réception de courriels non sollicités à caractère publicitaire proposant une prestation de création de site Internet, et les difficultés rencontrées par les personnes ainsi démarchées pour exercer leur droit d'opposition.

Les réponses apportées par le responsable de la société ayant procédé à ces envois sur l'origine des adresses électroniques utilisées et les modalités effectives d'opposition à recevoir de la prospection commerciale n'étant pas satisfaisantes, les membres de la formation restreinte de la Commission ont adopté une mise en demeure visant à obtenir toute garantie sur la conformité des pratiques mises en œuvre à la loi du 6 janvier 1978 modifiée en 2004 et à la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

Au vu des éléments d'informations communiqués sur ces deux points par le responsable de la société, il a été décidé de procéder à une mission de contrôle sur place afin de vérifier la réalité des procédures décrites dans le courrier adressé à la Commission.

Une délégation de la CNIL s'est rendue au siège de la société, mais s'est vu opposer par son gérant un refus d'entrer dans les locaux à usage professionnel. Ce refus a été consigné dans le procès-verbal établi par les agents habilités de la Commission, en la présence des services du commissariat de la police nationale territorialement compétent.

Compte tenu de ce refus, le président de la CNIL a sollicité du président du tribunal de grande instance (TGI) compétent, en application de l'article 44-II de la loi du 6 janvier 1978 modifiée, l'autorisation de procéder à la mission de contrôle.

Munis de l'ordonnance délivrée en ce sens par le magistrat, les services de la CNIL, accompagnés des forces de police, se sont à nouveau rendus dans les locaux de la société.

Il a été constaté dans ces conditions que des adresses électroniques permettant d'identifier des personnes physiques étaient collectées à partir de sites Internet, et que le dispositif mis en œuvre au sein de la société ne permettait pas de garantir le bon exercice du droit d'opposition par les personnes qui le souhaiteraient.

Les membres de la formation restreinte ont donc décidé de prononcer une sanction financière à l'encontre du responsable de la société mise en cause, et de lui enjoindre de cesser toute opération de prospection commerciale par voie électronique effectuée sur la base d'une collecte directe, sur des sites Internet, d'adresses électroniques permettant d'identifier une personne physique.

La CNIL prononce des sanctions

Quelques exemples dans lesquels la formation restreinte a contribué au respect des droits les plus fondamentaux dont bénéficient les citoyens :

Vouloir accéder aux données détenues par son fournisseur d'accès Internet

▶ **La CNIL reçoit une plainte d'un client ayant demandé à son fournisseur d'accès Internet de lui communiquer la copie de ses comptes rendus d'appels téléphoniques passés avec la *hotline*. La société refuse en indiquant que « la liste énumérant les appels téléphoniques passés auprès de nos services avec la rédaction de nos notes et de réécoute des conversations téléphoniques enregistrées pour chaque appel sont des informations internes à notre entreprise ». La CNIL met en demeure le fournisseur d'accès de communiquer ces informations au client.**

Recevoir chez soi, tous les soirs, des propositions commerciales par téléphone

▶ **La CNIL reçoit plusieurs dizaines de plaintes concernant des appels téléphoniques d'une enseigne proposant la vente de fenêtres. Malgré les nombreuses demandes des personnes démarchées pour que les données les concernant soient supprimées des fichiers, elles continuent à être appelées le soir à leur domicile, parfois plusieurs fois par semaine. Après instruction, la CNIL constate que ces sociétés n'ont pas mis en place les mesures nécessaires pour satisfaire les demandes des personnes. Cette enseigne a ainsi été condamnée à 60 000 euros d'amende.**

Quand des huissiers dérapent…

▶ **La CNIL reçoit une plainte concernant les pratiques d'une étude d'huissiers de justice. Le requérant vient de recevoir une injonction de payer sur laquelle apparaît, à côté de son identité, la mention « méchant imbécile ». Une délégation de la CNIL se rend dans les locaux de l'étude afin de vérifier le contenu des fichiers utilisés, s'agissant, notamment, de l'utilisation des zones « bloc-notes ». Elle relève ainsi l'existence de nombreux commentaires diffamant ou faisant référence à l'état de santé des personnes comme par exemple : « odieuse », « connasse », « séropositif depuis 23 ans », « déprime », « opération cancer des intestins », « incarcéré Baumettes attend liberté conditionnelle », « tentative de suicide », etc. L'étude d'huissiers a été condamnée à 5 000 euros d'amendes. D'autres études d'huissiers font actuellement l'objet d'une procédure de mise en demeure pour des motifs similaires.**

Retrouver un débiteur et le faire payer

▶ **La CNIL reçoit de nombreuses plaintes concernant les méthodes utilisées par des sociétés de recouvrement de créances pour retrouver les coordonnées de débiteurs. Des contrôles sont alors effectués auprès de sociétés d'enquêtes spécialisées dans la recherche de débiteurs. Des scripts téléphoniques sont découverts dont l'utilisation a manifestement pour but de procéder à des appels téléphoniques auprès de certaines administrations en usurpant certains titres ou fonctions afin d'obtenir de façon détournée des informations sur les personnes recherchées (voir p. 38). Plusieurs mises en demeure ont ainsi été adressées par la CNIL à ces sociétés. Les procédures sont toujours en cours d'instruction.**

LES PRIVÉS À LA LOUPE

Exemples de scripts téléphoniques découverts dans des cabinets d'enquêtes.

Parents ou membre famille

Bonjour caisse d'assurance Maladie,

Je vous appelle un petit peu au hasard, car j'ai un petit souci sur Mr x à qui j'essaie d'envoyer des courriers au (adresse dossier)

~~c'est bien votre fils ?~~

~~car~~ j'ai des reliquats de frais de remboursements médicaux et un problème de mise à jour sur son dossier et à chaque fois que ~~je~~ lui écrit, le courrier me fais retour.

→ Je sais pas - demenager sur quelle commune ? où ? quand ?

↳ mais comme pb mise à jour sur son dossier, je sais pas si actuellement il est salarié ou demandeur d'emploi ??

→ Travail : Pour qui ? depuis quand ? poste ?

la Poste (courriers) [redacted]

Poste comptable
BCL : bureau comptable local

bjr la poste de [redacted]

Pourrais-je avoir le service des AR (ordre de réexpédition)

Je me permet de T'appeler, car je souhaiterais savoir si tu as un ordre de réexpédition en place, au (adresse dossier) au nom de M/Mme (Nom dossier) ?

POURQUOI ?

Eh ! bien, ces personnes ~~gens~~ sont passés à mon bureau pour modifier l'adresse de de réexpédition, et m'ont simplement indiqué où ils avaient été mis en place

Donc j'aimerais en savoir un peu plus

Je comprends, je te donne mon BCL -

oui - A quelle date mise en place ?
- Pour quelle adresse ?

La CNIL conseille

La recommandation sur l'« anonymisation des décisions de justice »

L'adoption, en 2001, d'une recommandation relative à la diffusion de données personnelles sur Internet par les banques de données de jurisprudence répondait au souci de concilier cette diffusion avec la protection des personnes physiques qui y sont citées. Il s'agit, principalement de prévenir les risques de détournement de finalité de ces bases qui pouvaient, par l'utilisation des moteurs de recherche, se transformer en véritables fichiers de renseignements sur ces personnes. La CNIL a ainsi préconisé que les éditeurs de bases de données de décisions de justice librement accessibles sur des sites Internet s'abstiennent d'y faire figurer le nom et l'adresse des parties ou des témoins au procès, quels que soient l'ordre et le degré de la juridiction et la nature du contentieux.

La modification de la loi informatique et libertés par la loi du 6 août 2004 a conduit la Commission à dresser un bilan de l'application de sa recommandation, notamment grâce à l'audition et à la consultation des cours suprêmes (Conseil d'État, Cour de cassation, Cour des comptes), du Secrétariat général du Gouvernement, des associations d'utilisateurs de bases de données de jurisprudence et des éditeurs privés.

La Commission a ainsi estimé que les principes dégagés en 2001 étaient, pour l'essentiel, appliqués par les différents acteurs et, qu'au total, sa recommandation avait permis d'encadrer de manière équilibrée la diffusion des décisions de justice sur Internet et le respect de la vie privée des personnes citées dans ces décisions.

La Commission a néanmoins relevé les évolutions législatives relatives à la protection des données à caractère personnel dans le cadre des bases de données jurisprudentielles.

Ainsi, l'analyse des nouvelles dispositions de la loi informatique et libertés de même que le nouveau régime applicable à la diffusion des données publiques ont conduit la Commission a attiré l'attention du Gouvernement sur l'intérêt qui s'attacherait, au regard des droits et libertés des personnes, à l'adoption d'une mesure législative spécifique prévoyant l'anonymisation des bases de données jurisprudentielles lors de leur diffusion par des moyens électroniques **(voir en conclusion de ce rapport les propositions de la CNIL aux pouvoirs publics)**.

Cette solution serait de nature à inscrire la pratique française dans le mouvement européen en faveur d'une protection accrue des personnes.

L'ensemble des travaux menés par la CNIL sur cette question est synthétisé dans un document public accessible depuis son site Internet.

Questions à …

EMMANUEL DE GIVRY

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

Pourquoi avoir voulu dresser un bilan de la recommandation de la CNIL du 29 novembre 2001 ?

D'une manière générale, il me semble nécessaire que la CNIL dresse, après un certain temps, un bilan de l'application de ses recommandations. Cette démarche était particulièrement opportune sur le sujet délicat de l'anonymisation des décisions de justice au regard de l'évolution des contextes juridique et technique. En effet, d'une part, le sujet est particulièrement sensible en ce qu'il procède de données relatives parfois à des infractions ou condamnations et, d'autre part, le cadre général a considérablement évolué depuis 2001.

Quelles sont ces évolutions dont vous parlez ?

Trois évolutions me paraissent notables. La première, c'est naturellement la modification de la loi du 6 janvier 1978 par la loi du 6 août 2004 qui a renforcé les droits des personnes. La deuxième résulte de l'ordonnance du 6 juin 2005 modifiant la loi du 17 juillet 1978 qui, sans être directement applicable aux décisions de justice, pose un principe général d'anonymisation des documents publics. Enfin, la dernière évolution est de nature technologique, les performances des moteurs de recherche au sein des bases de données, notamment celles diffusées sur Internet ayant été considérablement accrues.

Pourquoi avoir préconisé l'adoption d'une disposition législative sur la question de l'anonymisation des décisions de justice ?

La Commission a considéré que l'adoption, dans la loi du 17 juillet 1978, d'une règle générale d'anonymisation pour la réutilisation d'informations publiques devrait conduire à appliquer ce même principe aux décisions de justice contenues dans des bases de données informatiques. Aussi, en application de l'article 11 de la loi du 6 janvier 1978 modifiée, a-t-elle attiré l'attention du Gouvernement sur l'intérêt qu'il y aurait à consacrer ce principe par une disposition législative spécifique.

La CNIL assure le droit d'accès indirect aux fichiers intéressant la sûreté de l'État, la défense et la sécurité publique

En 2006, la CNIL a reçu **1 595 demandes** de droit d'accès indirect.

Les magistrats de la CNIL en charge du droit d'accès indirect ont procédé en 2006 à **162 missions d'investigations** : 140 au ministère de l'Intérieur et 22 au ministère de la Défense.

Au cours de cette même année, les services de la CNIL ont pu **clôturer 1 370 demandes** qui concernaient pour une large part des saisines reçues au cours des années 2002, 2003, 2004, 2005 et quelques-unes en 2006. L'instruction de ces demandes a nécessité **5 183 vérifications**.

Il convient de préciser que les demandes de droit d'accès indirect concernent plusieurs fichiers et nécessitent de nombreuses vérifications. Par exemple, pour les fichiers de police judiciaire, les magistrats de la CNIL opèrent des vérifications dans les fichiers du système de traitement des infractions constatées – STIC –, dans les fichiers de la sécurité publique des commissariats, dans le fichier du système judiciaire de documentation et d'exploitation – JUDEX – de la gendarmerie.

Au 1er janvier 2007, il restait encore un stock de **2 800 vérifications non traitées** imputable au manque de moyens de la CNIL, aux procédures plus lourdes et aux délais de réponse des services de police judiciaire et des parquets.

C'est votre droit

En application de l'article 41 de la loi de 1978 modifiée en 2004, toute personne peut demander à la CNIL qu'elle vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique. Cette demande s'effectue par écrit à l'attention du président de la CNIL. Les vérifications sont ensuite effectuées par certains membres de la Commission, magistrats du Conseil d'État, de la Cour de cassation ou de la Cour des comptes. Tout citoyen peut obtenir communication directe dans les locaux de la CNIL ou à la préfecture de son lieu de domicile des informations le concernant, dès lors qu'elles ne mettent pas en cause la sûreté de l'État, la défense ou la sécurité publique.

À propos des fichiers

STIC

Le système de traitement des infractions constatées (STIC) est un fichier central de police judiciaire tenu par la Direction générale de la police nationale, sous le contrôle du procureur de la République compétent. Ce fichier répertorie des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause dans ces procédures et les victimes des infractions concernées.

JUDEX

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

Bilan des 5 183 vérifications effectuées au titre du droit d'accès indirect par les magistrats de la CNIL pour les 1 370 demandes clôturées au cours de l'année 2006

	Vérifications	% sur le nombre total de vérifications (soit 5183) en 2006
MINISTÈRE DE L'INTÉRIEUR	**3121**	**60%**
Renseignements Généraux	549	11%
Police Judiciaire – STIC	1481	29%
- dont mis en cause	750	
- dont victimes	731	
Sécurité Publique-commissariats	636	12%
Direction de la Surveillance du Territoire et Direction Centrale de la Sécurité du CEA	57	0.99%
Système d'Information Schengen	397	7 %
Autres (TRACFIN)	1	0.01%
MINISTÈRE DE LA DÉFENSE	**2062**	**40%**
Gendarmerie Nationale	2012	39%
- dont mis en cause	677	
- dont victimes	672	
- dont Fichier Alphabétique de Renseignements- FAR	663	
Direction de la Protection de la Sécurité de la Défense- DPSD-	24	0,5%
Direction Générale de la Sécurité Extérieure – DGSE-	26	0,5%
TOTAL	**5183**	**100%**

Les fichiers de police judiciaire – STIC et JUDEX

Analyse des 1 427 vérifications effectuées dans les fichiers de police judiciaire pour les mis en cause (750 dans le STIC et 677 dans JUDEX) pour les demandes clôturées en 2006[1] :

– 895 personnes (soit 63 %) n'étaient pas signalées en tant que « mis en cause »[2]

– 532 personnes (soit 37 %) étaient signalées en tant que « mis en cause » :

• Pour 244 personnes fichées en tant que « mis en cause », (soit 46 % des 532 personnes fichées en tant que mis en cause), l'enregistrement dans les fichiers STIC ou JUDEX était exact, les faits incriminés étaient avérés ou la suite judiciaire ne donnait pas lieu à une mise à jour ou à une suppression.

• Pour 288 personnes fichées en tant que « mis en cause », (soit 54 % des 532 personnes fichées en tant que mis en cause), les signalements enregistrés dans les fichiers STIC ou JUDEX ont été modifiés parce qu'ils étaient inexacts, incomplets ou périmés.

---

1. Les statistiques 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 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.
2. Implication d'une personne dans la commission d'une infraction.

Comment ça marche ?

ÉTAPE 1

Lorsque la CNIL reçoit la demande d'un requérant, elle transmet la demande au ministère de l'Intérieur et au ministère de la Défense. Les directions de la police judiciaire vérifient l'existence d'une fiche ou d'un dossier non seulement dans les STIC et JUDEX mais aussi dans les fichiers manuels centraux et dans les fichiers locaux de la sécurité publique.
Si le requérant est effectivement connu des services de police judiciaire du ministère de l'Intérieur ou du ministère de la Défense :
– les services de police judiciaire rapatrient aux sièges de ces directions les dossiers de procédure conservés par les directions départementales et régionales pour les mis en cause ;
– les services de police judiciaire saisissent le procureur de la République du Tribunal compétent pour connaître la suite judiciaire des affaires mentionnées et recueillir son accord de communication en cas de maintien de la fiche STIC ou JUDEX, qu'il soit mis en cause ou victime.
L'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure confère, en effet, au procureur de la République territorialement compétent un pouvoir d'appréciation s'agissant de la mise à jour, voire de l'effacement, de la fiche du requérant dans les fichiers de police judiciaire.
Si la procédure a fait l'objet d'une décision de classement sans suite pour insuffisance de charges ou de non-lieu, le procureur de la République doit préciser à la police judiciaire s'il ordonne ou non l'effacement des informations concernant le requérant dans les fichiers de police judiciaire. En cas de refus, la fiche doit cependant être mise à jour par la mention de la décision de classement ou de non-lieu.
Si la procédure a fait l'objet d'une décision de relaxe ou d'acquittement devenue définitive, les informations concernant l'intéressé doivent en principe être effacées, sauf si le procureur de la République en prescrit le maintien dans les fichiers de police judiciaire.
Ces premières démarches prennent en moyenne actuellement plus d'un an si la personne est connue en tant que mise en cause.

ÉTAPE 2

Une réunion est ensuite organisée soit au ministère de l'Intérieur soit à la direction de la Gendarmerie nationale à Rosny-sous-Bois soit dans les locaux de la PJ à Écully afin que les membres de la CNIL qui ont la qualité de magistrats puissent examiner les différentes pièces du dossier (compte rendu d'enquête, pièces du FAED et/ou Canonge, procès-verbaux d'audition et éventuellement documents plus anciens non répertoriés dans le STIC).
Dans le cadre des investigations, le magistrat de la CNIL examine successivement :
– **la qualification des faits** : si une personne a été mise en cause lors d'une enquête préliminaire de flagrance ou sur commission rogatoire d'une juridiction d'instruction, la qualification des faits peut être redéfinie par l'autorité judiciaire et se substituer à la qualification initialement enregistrée dans le fichier ;
– **les durées de conservation** : les articles 7 des décrets STIC du 14 octobre 2006 et JUDEX du 20 novembre 2006 fixent les durées de conservation des mentions en fonction de la gravité des faits commis ;
– les mises à jour ou suppressions éventuelles des données concernant :

- les personnes ayant bénéficié d'un non-lieu ;
- les personnes mises en cause qui ont bénéficié d'une décision judiciaire de classement sans suite motivée par l'insuffisance des charges ;
- les personnes ayant bénéficié d'une décision de relaxe ou d'acquittement devenue définitive ;
- éventuellement, la requalification des faits à la lecture de la procédure ;
- les erreurs d'enregistrement (infraction ne devant pas être enregistrée dans le STIC ou dans JUDEX, personne signalée comme « auteur » alors qu'elle n'était que victime, plainte au nom d'une personne morale et enregistrée au nom de la personne physique qui a procédé au dépôt de la plainte…).

Lors de la réunion d'investigation, les services de police judiciaire remettent à la CNIL les fiches STIC ou JUDEX qui ont recueilli l'accord de communication du ministère de l'Intérieur ou du ministère de la Défense et du procureur de la République.
Si la radiation a déjà été effectuée par les services de police judiciaire lors de l'examen du dossier, ils présentent au magistrat de la CNIL l'ancienne et la nouvelle versions de l'enregistrement et donnent leur accord pour informer le requérant de cette suppression.
La CNIL demande aux services de police judiciaire de transmettre les signalements rectifiés aux services préfectoraux concernés dès lors que le signalement initial a pu être utilisé notamment dans le cas des habilitations, des assermentations ou d'embauches…

ÉTAPE 3

Enfin le président de la CNIL notifie par écrit au requérant qu'il a été procédé aux vérifications demandées dans les fichiers visés dans la saisine initiale et transmet les fiches STIC ou JUDEX si le procureur a donné son accord. En cas de refus de communication ou de refus de suppression du ministère de l'Intérieur ou du ministère de la Défense suite à la demande du procureur de la République, la CNIL précise au requérant qu'un recours devant le tribunal administratif lui est ouvert dans un délai de deux mois. C'est à ce stade que la saisine est considérée comme « clôturée ».

Les fichiers des Renseignements généraux

Analyse des 549 vérifications effectuées dans les fichiers des Renseignements généraux pour les demandes clôturées en 2006

		% sur le total des vérifications aux RG (soit 549)
Requérants non fichés aux RG	**321**	**58%**
Requérants fichés aux RG	**228**	**42%**
– Dossier non communicable	*12*	*2%*
– Dossier partiellement communicable	*11*	*2%*
– Dossier totalement communicable	*205*	*38%*
TOTAL	**549**	**100%**

* Sur les 216 communications totales ou partielles, 33% (soit 71) ont eu lieu dans les locaux de la CNIL, et les 67% (soit 145) des autres saisines ont été communiquées 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, seuls quatre 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 six dossiers.

Comment ça marche ?

ÉTAPE 1

Lorsque la CNIL reçoit la demande d'un requérant, elle transmet la demande au ministère de l'Intérieur. La Direction centrale des Renseignements généraux vérifie l'existence d'un dossier papier. Il convient de préciser que les recherches portent à la fois sur le fichier informatique d'indexation détenu par la Direction centrale des Renseignements généraux et sur les dossiers individuels éventuellement détenus par les directions régionales et départementales des Renseignements généraux, sur les extraits de dossiers collectifs contenant des données nominatives sur les demandeurs, ainsi que sur les dossiers conservés dans les sections spécialisées de la Direction centrale des Renseignements généraux. Le magistrat de la CNIL exerce, s'il y a lieu, le droit de rectification ou d'effacement des données inexactes ou des données dont la collecte est interdite par la loi.
Si les Renseignements généraux ne détiennent aucune information concernant un requérant, en accord avec le ministre de l'Intérieur, ils en informent la CNIL qui, à son tour, avise le requérant de l'absence de signalement dans les fichiers des Renseignements généraux.

ÉTAPE 2

Si les Renseignements généraux détiennent des informations relatives à un requérant, l'ensemble des dossiers le concernant est rassemblé à Paris au siège du ministère de l'Intérieur.
Une réunion est ensuite organisée au ministère de l'Intérieur afin que les membres de la CNIL qui ont la qualité de magistrats puissent examiner les différentes pièces du dossier des Renseignements généraux notamment pour :
– décider du caractère communicable des informations, c'est-à-dire celles qui ne mettent pas en cause la sûreté de l'État, la défense et la sécurité publique, en précisant s'il y a lieu d'occulter les mentions relatives aux tiers ;
– les mises à jour ou suppressions éventuelles des informations périmées, inexactes ou incomplètes…
Si les services des Renseignements généraux et le magistrat de la CNIL sont d'accord, les services des RG remettent, lors de la séance d'investigations, l'accord du ministre de l'Intérieur.

ÉTAPE 3

Une fois l'accord du ministre de l'Intérieur obtenu, la communication des informations s'effectue de la façon suivante :
– si le requérant est domicilié en province : la communication du dossier s'effectue à la préfecture du lieu de domicile du requérant ;
– si le requérant réside dans la région parisienne, la communication du dossier s'effectue à la CNIL.
Dans l'hypothèse d'une communication totale ou partielle d'un dossier, le requérant a la possibilité de formuler ses observations qui, après examen du magistrat de la CNIL, sont transmises aux Renseignements généraux pour mise à jour ou effacement selon le cas.
Si la communication de toutes les informations peut nuire à la sûreté de l'État, à la défense ou à la sécurité publique, la CNIL notifie simplement au requérant qu'il a été procédé aux vérifications en lui précisant les voies de recours.

Ça la fiche mal

▶ Monsieur X, âgé de 24 ans, postulant pour un emploi de sécurité avait été entendu dans un commissariat de police en 2005 pour une affaire de recel, mention qui devait rester dans le STIC pour 40 ans. À la suite des investigations par le magistrat de la CNIL, et à la lecture de la procédure il a pu être constaté qu'il n'y avait pas d'élément contre cette personne. Elle avait été interpellée à bord d'un véhicule volé acheté de bonne foi par son frère. Ce signalement a donc été supprimé car le requérant ne correspondait pas à la notion de mis en cause.

▶ Un jeune homme était signalé à la suite d'un contrôle de la circulation pour défaut de rétroviseur. L'agent de police avait saisi de façon incomplète le numéro de série du véhicule. En juin 2003, l'intéressé effectue une formation à l'aéroport de Nice pour devenir agent de piste. Sa demande de badge reste bloquée à la Police de l'air et des frontières (PAF). L'agent de la PAF l'informe alors de son inscription au fichier STIC pour recel. L'erreur sur le numéro de série avait conduit les services de police à le mettre en cause pour une affaire de recel d'un scooter volé. Le signalement a donc été effacé à la suite des démarches de la CNIL car l'infraction n'était pas constituée.

▶ Monsieur X. occupait un emploi en CDI dans une société de gardiennage, mais la Police de l'air et des frontières a refusé son agrément pour occuper un emploi de sécurité dans l'enceinte de l'aéroport. Lors des investigations menées par le magistrat de la CNIL, le 18 juillet 2006, il a été constaté que M. X était signalé dans le STIC en tant que mis en cause dans une affaire de menaces d'atteinte aux personnes sous condition. L'affaire a été classée sans suite pour infraction insuffisamment caractérisée. Le parquet ayant demandé l'effacement de la fiche le 21 juillet 2006, les services de police judiciaire, seize mois après la saisine de la CNIL, ont confirmé la suppression.

▶ Monsieur Y. s'est vu refuser sa demande de naturalisation car il avait été mis en cause dans une affaire de recel, de vol et d'escroquerie (la durée de conservation de cette affaire est de 40 ans dans le STIC). Il a donc saisi la CNIL le 24 mars 2005. Les services de police judiciaire ont rassemblé les éléments de la procédure et les investigations de la CNIL effectuées le 5 juillet 2006 ont permis de constater que M. Y ne correspondait pas à la notion de mis en cause, le signalement dans le STIC a donc été supprimé, ce qui a été confirmé le 10 juillet 2006 par les services de police judiciaire, soit seize mois après la première saisine de la CNIL.

▶ Monsieur R. postulant pour un emploi nécessitant un agrément s'est vu refuser son agrément par la préfecture du Vaucluse le 21 juin 2005. Il a aussitôt saisi la CNIL le 24 juin 2005. Professeur, il avait été mis en cause par une de ses élèves et était signalé dans le STIC depuis 2003 pour atteinte à la dignité de la personne. Cette mention a été supprimée car il s'agissait d'une contravention de 4e classe qui n'aurait jamais dû être inscrite dans le STIC. C'est en juillet 2006 que le ministère de l'Intérieur a confirmé cette suppression.

▶ Monsieur X., employé à la RATP au sein du service interne de sécurité GPSR, s'est vu refuser le renouvellement de son agrément parce qu'il était connu dans le STIC pour une affaire de violences volontaires entraînant une ITT de plus de huit jours. Le procureur de la République du TGI de Bobigny a informé la CNIL que cette affaire avait fait l'objet d'un classement sans suite résultant d'un désistement du plaignant, ce qui n'est pas un motif de suppression. Cette mention sera maintenue 40 ans dans le STIC.

Dernière minute !

Explosion des demandes de droit d'accès indirect

Début mai 2007, la CNIL avait déjà reçu 1 325 demandes de droit d'accès indirect dont 75 % concernent les Renseignements généraux. Il faut savoir que ces demandes vont donner lieu à environ 3 700 vérifications dans différents fichiers.

POUR UNE MEILLEURE CONNAISSANCE DES DROITS

La CNIL vous informe au quotidien

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 décembre 2006 par TNS Sofres sur un échantillon de 1 000 personnes représentatives de la population française.

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

	Juin 2004	Décembre 2005	Décembre 2006	Évolution 2005-2006
Oui	32	37	39	+2
Non	68	63	61	–2
	100 %	100 %	100 %	100 %

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

	Juin 2004	Décembre 2005	Décembre 2006	Évolution 2005-2006
Oui	45	49	50	+1
Non	55	51	50	–1
	100 %	100 %	100 %	100 %

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

	2006
Oui, tout à fait	5
Oui, plutôt	22
Sous-total oui	**27**
Non, plutôt pas	43
Non, pas du tout	27
Sous-total non	**70**
Sans opinion	3
	100 %

Les interventions de la CNIL

La CNIL est très souvent sollicitée pour intervenir à l'occasion de colloques, séminaires, conférences ou formations sur des thèmes généraux concernant la loi informatique et libertés, le correspondant informatique et libertés ou des sujets plus sectoriels.

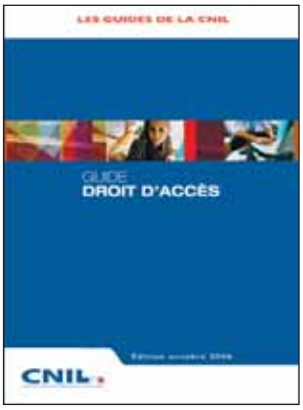
En 2006, la CNIL a assuré 170 interventions à des conférences, colloques, séminaires ou animations de formation qui ont mobilisé 235 membres ou agents. Au total, la CNIL a reçu plus de 200 sollicitations d'interventions.

Le tour de France des régions

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

En 2006, six régions ont été visitées : Lorraine, Champagne-Ardenne, Rhône-Alpes, Provence-Alpes-Côte d'Azur (Nice), Basse-Normandie et Alsace. À la suite de ces visites, la CNIL a enregistré de nombreuses désignations de correspondants informatique et libertés. Après deux années d'organisation des rencontres, la CNIL se situe à mi-parcours, puisqu'il reste environ la moitié des régions à visiter.

Les publications



En 2006, la CNIL a édité deux guides pratiques destinés au grand public et aux professionnels : *Droit d'accès* et *L'utilisation des fichiers dans le cadre d'activités politiques*.

La **Lettre InfoCNIL** comptait 16 800 abonnés au 31 décembre 2006, contre 12 900 abonnés en 2005. Dans une version enrichie, avec des informations mieux hiérarchisées, une nouvelle *Lettre InfoCNIL* a vu le jour en octobre et clôt l'année 2006 sur un gain d'abonnés de 30 %.

Le site Internet

Le site de la CNIL recense 110 000 visiteurs différents par mois en 2006, soit une progression mensuelle de 10 000 visiteurs par rapport à 2005 : c'est un gain annuel de 10 % de l'audience du site. En 2006, la CNIL a organisé un sondage en ligne concernant la diversité qui a recueilli près de 1 000 contributions.

Les nouveaux locaux de la CNIL

En juin 2006, la CNIL a déménagé dans de nouveaux locaux situés au 8 rue Vivienne à Paris. Jusqu'alors réparti sur trois sites, l'ensemble des équipes a pu se réunir. Ces locaux permettent également d'organiser des séances de formation (correspondants) ou d'information.

À l'occasion du déménagement, la CNIL a revu sa charte graphique et son logo. Le nouveau logo capitalise désormais sur le sigle CNIL qui est bien intégré par le grand public et les organismes.

POUR UN MEILLEUR ACCUEIL

La CNIL vous répond au quotidien

Le SORP assure :
– l'accueil et le renseignement téléphoniques. La mise en place d'une permanence téléphonique tous les jours de 10 heures à 12 heures et de 14 heures à 16 heures permet notamment de répondre aux personnes souhaitant un renseignement juridique d'ordre général ou une aide à l'accomplissement des formalités préalables ;
– le traitement des requêtes générales qui parviennent à la CNIL par courrier ou télécopie ;
– l'enregistrement du courrier entrant.

Il a également pour vocation de contribuer à la rédaction, en liaison avec la direction des affaires juridiques, le service documentation et le service communication, de documents destinés à l'information du public.

L'activité du SORP est en constante augmentation depuis sa création.

Qu'est-ce que c'est ?

LE SORP

Le service d'orientation et de renseignement du public (SORP), créé en juin 2006, a pour mission d'améliorer les relations de la Commission avec les usagers, qu'ils soient citoyens ou responsables de fichiers, et notamment de réduire les délais de réponse et d'attente. Le SORP, composé de dix personnes, est le point d'entrée des appels, demandes et courriers adressés à la CNIL.

Le SORP en chiffres

- **120 000 appels reçus en 2006.**
- **15 000 courriers enregistrés en 2006.**

PROLONGEMENT DE L'ACTION DE LA CNIL AU NIVEAU EUROPÉEN

Qu'est-ce que c'est ?

LE GROUPE DE L'ARTICLE 29 – 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. Ce groupe, dit « de l'article 29 », a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays tiers et de conseiller la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles. Le G 29 se réunit à Bruxelles en séance plénière tous les deux mois environ. La CNIL est représentée dans les quatorze sous-groupes de travail en activité et qui ont la charge de préparer les travaux de la séance plénière.

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

En 2006, davantage encore qu'en 2005, les sujets abordés et les documents adoptés par le groupe ont été dominés par des problématiques transatlantiques, à l'instar des avis adoptés dans les affaires PNR et SWIFT[1]. Le groupe a été amené à plusieurs reprises à donner la vision des autorités de contrôle européennes sur les enjeux que les relations US-UE font peser sur les règles européennes de protection des données personnelles. De nombreux autres sujets ont été abordés, qui illustrent la diversité des attentes reposant aujourd'hui sur ce groupe (alertes professionnelles, services de messagerie électronique, réexamen du cadre réglementaire pour les réseaux et services de communications électroniques, projet eCall, etc.).

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

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

Qu'est-ce que c'est ?

SCHENGEN

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

EUROPOL

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

SYSTÈME D'INFORMATION DOUANIER

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

L'ACC d'Europol, qui s'est réunie à quatre reprises en 2006, a pour la première fois, le 17 octobre 2006, organisé une conférence pour tirer le bilan de sept années de fonctionnement de l'Office européen de Police, et de sa coopération avec les autorités de protection des données. Cette conférence avait également pour objectif d'alimenter la réflexion à l'aube d'une évolution radicale du fonctionnement d'Europol, dont les grandes lignes seront présentées en 2007.

L'ACC Schengen, dont Georges de la Loyère, le Commissaire en charge des affaires internationales, a été

élu vice-président le 2 mars 2006, s'est également réunie à quatre reprises durant l'année 2006. L'ACC a adopté un deuxième avis sur le Système d'information Schengen (SIS), au regard de la future intégration dans le SIS d'éléments biométriques. L'ACC a également initié un contrôle au titre de l'article 99 de la Convention d'application des accords de Schengen, qui établit les modalités de l'intégration de données relatives à des personnes ou à des véhicules aux fins de surveillance discrète et de contrôle spécifique. Ce contrôle s'est naturellement prolongé au niveau national, la CNIL ayant ainsi opéré divers contrôles auprès des autorités françaises de sécurité intérieure sur ce point.

Les CNIL européennes se réunissent également de manière informelle sur les questions liées au troisième pilier dans le cadre du dit **« Groupe Police »**. Ce Groupe, créé à l'initiative de la Conférence annuelle des commissaires européens à la protection des données, a mené divers travaux en 2006 sur la protection des données dans les secteurs police – justice, notamment sur une importante proposition de décision-cadre sur la protection des données dans le 3e pilier. Compte tenu de leur importance, ces travaux se poursuivront sur l'année 2007.

Qu'est-ce que c'est ?

LES PILIERS DE L'UNION EUROPÉENNE

Le premier pilier

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

Le deuxième pilier

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

Le troisième pilier

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

OÙ EN EST-ON SUR…?

LE CORRESPONDANT INFORMATIQUE ET LIBERTÉS MONTE EN PUISSANCE

Environ un an après son entrée en vigueur, le correspondant à la protection des données personnelles ou correspondant informatique et libertés (CIL) est un succès.

Rappelons que c'est à l'occasion de la refonte, en 2004, de la loi informatique et libertés que le correspondant à la protection des données personnelles, désormais désigné « Correspondant informatique et libertés », a été institué. Tous les responsables de traitements sont concernés, quelle que soit la taille ou l'activité de l'organisme, public ou privé, association, grande administration, PME ou entreprise internationale.

La désignation d'un CIL a l'avantage de réduire considérablement les formalités obligatoires de déclaration, seuls les traitements soumis à autorisation n'étant pas exonérés. Le correspondant veille à la bonne application de la loi informatique et libertés au sein de son organisme.

Le bilan 2006

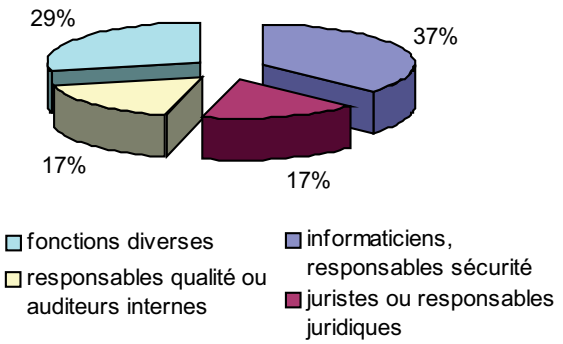
Le correspondant en chiffres

Au 31 décembre 2006, 320 correspondants avaient été désignés par 650 organismes (plusieurs organismes ayant désigné le même correspondant). Ces nominations proviennent de grands groupes industriels (Vivendi, Groupe Exxonmobil, General Electrics, Bosch…), de compagnies d'assurance et de mutuelles (AG2R, Swiss Life, Gras Savoye, Groupama), de collectivités locales et territoriales (Mairie de Paris, communauté urbaine de Brest, communauté d'agglomération de Montpellier, etc.), d'associations, d'hôpitaux, d'universités, de cabinets d'avocats, de PME : autant d'exemples d'organismes qui, en désignant un correspondant, se sont engagés pour le respect des droits relatifs à la protection des données.

Qui sont les correspondants ?

Les correspondants sont à ce jour principalement des salariés de l'entreprise ou de la collectivité locale. S'agissant de leurs origines, la plupart d'entre eux sont issus des métiers de l'informatique.

Le profil des correspondants désignés



Les secteurs qui désignent des correspondants

83 % des correspondants sont issus du secteur privé et représentent principalement :
– les entreprises industrielles ;
– les compagnies d'assurance ;
– les banques.

Il est à noter qu'en désignant un correspondant mutualisé, les notaires sont très largement représentés grâce à l'initiative de l'ADSN (Association pour le développement du service notarial).

17 % des correspondants sont issus des organismes publics et représentent principalement :
– les organismes de protection sociale et de retraite ;
– les collectivités locales et territoriales ;
– les organismes de santé ;
– les organismes gérant le logement social.

Les partenariats

La CNIL a initié, depuis plusieurs mois, une vaste opération de communication et de pédagogie auprès des acteurs concernés.

Ainsi, les plus grandes entreprises françaises ont été invitées à se doter de correspondants, mais aussi les collectivités locales à travers l'Association des maires de France.

De plus, la CNIL a signé des accords de partenariat avec l'ACFCI (Assemblée des chambres de commerce et d'industrie) et la CPU (Conférence des présidents d'université). Ces partenariats visent à améliorer la connaissance de la loi informatique et libertés par la mise en place d'actions de sensibilisation à la protection des données et la diffusion de la culture « informatique et libertés ».

Ces initiatives doivent être saluées et encouragées.

En outre, lors des six rencontres régionales qu'elle a organisées, la CNIL a poursuivi son programme d'information et de sensibilisation sur la fonction de correspondant informatique et libertés.

Les moyens au service des correspondants

Un accueil privilégié

La CNIL a créé une cellule entièrement dédiée aux correspondants leur offrant un accueil privilégié et prioritaire afin de les aider dans l'accomplissement de leurs missions. Une adresse de courrier électronique et un numéro de téléphone à l'usage exclusif des correspondants désignés ont été mis en place.

Cette cellule offre un service dont l'objectif est d'apporter aux correspondants les conseils, l'information et l'orientation nécessaires au développement de leur action en proposant une réponse personnalisée ainsi qu'un accès privilégié aux services de la CNIL. Elle crée un point d'entrée unique pour les correspondants, quelle que soit la nature de leurs demandes.

Une formation « sur mesure » des correspondants

Dans le cadre des dix journées de rencontres organisées durant l'année 2006, plus de 250 correspondants désignés ont participé à une journée de formation à la CNIL.

La cellule « correspondants » propose :
– une formation généraliste comprenant une présentation de la CNIL et des services, les attentes de la CNIL vis-à-vis des correspondants, l'application de la loi informatique et libertés ;
– des réunions d'information thématiques sur des sujets particuliers (tels que la biométrie, les ressources humaines, l'administration électronique, la santé, les collectivités locales…) sont également proposées.

LES JEUNES ET LA PROTECTION DES DONNÉES

Questions à ...

FRANCIS DELATTRE

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

La CNIL participe-t-elle à des programmes de sensibilisation des jeunes aux risques liés à l'utilisation de l'Internet ?

Oui, et je rappelle que la CNIL a toujours considéré comme essentielle la mise en place d'opérations de sensibilisation des jeunes, des parents et des éducateurs, pour une utilisation plus sûre d'Internet. C'est donc dans ce cadre que notre Commission est associée à la mise en œuvre du projet « Confiance » mené en partenariat avec le ministère de l'Éducation nationale. Ce projet vise à valoriser et conduire de manière concertée, des actions de sensibilisation des enfants et de leurs parents à la sécurité et à la civilité de l'Internet, en impliquant l'ensemble des acteurs de l'Internet, institutions publiques, associations et industriels. Ce projet a ainsi conduit à la mise en ligne d'un site web de référence en matière de prévention des risques appelé www.internetsanscrainte.fr. Ce site propose notamment un ensemble de courtes animations de type dessins animés destinées à des enfants de 7 à 11 ans (« Vinz et Lou sur Internet ») qui vise par exemple à sensibiliser les jeunes sur l'exploitation de leurs données personnelles à des fins marketing. Des fiches pédagogiques sont également proposées sur la problématique du spam et la création de blogs. Enfin, j'ajouterai que l'objectif poursuivi par la 1re journée européenne du 28 janvier 2007 sur la protection des données personnelles s'inscrit pleinement dans notre démarche de sensibilisation des jeunes générations au droit fondamental de la protection des données et de la vie privée.

Développez-vous des partenariats spécifiques avec le monde éducatif afin de sensibiliser les jeunes à la question de la protection des données ?

Oui, l'accord-cadre signé en 2003 entre la CNIL et le ministère de l'Éducation nationale doit être prochainement reconduit. Il visera notamment à favoriser la réalisation de programmes de sensibilisation informatique et libertés au sein des établissements d'enseignement. Il s'attachera également à promouvoir la fonction de correspondant à la protection des données qui a pour mission de veiller au sein des établissements d'enseignement à la bonne application de la loi informatique et libertés. Enfin, cet accord est destiné à encadrer la mise en place des espaces numériques de travail (ENT) dans le primaire, le secondaire et le supérieur au regard des principes de la protection des données. Une telle démarche a également été initiée de manière plus spécifique auprès de l'enseignement supérieur avec la signature d'une convention le 25 janvier 2007 avec la Conférence des présidents d'université.

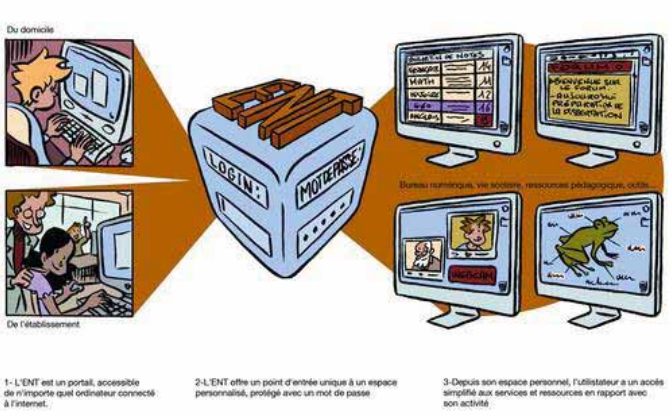
Que pensez-vous du déploiement des espaces numériques de travail (ENT) dans les établissements d'enseignement ?

Les ENT sont d'abord de formidables outils pour la promotion concrète et efficace de « l'Égalité des chances » puisqu'ils transcendent les handicaps de la naissance ou de la géographie en permettant un accès facile à toutes les bibliographies, mémoires, cours, débats et amphithéâtres, liens de culture, utiles à un travail personnel ou collectif. Face à un tel enjeu, la CNIL doit, simplement, réguler la circulation des données personnelles et sensibiliser les acteurs, à savoir les enseignants, les élèves et leurs parents, sur les principes de la protection des données à caractère personnel et de la vie privée. Ainsi, par exemple, la CNIL a appelé l'attention des responsables d'établissement sur la nécessité de sensibiliser les utilisateurs des ENT aux mesures élémentaires de sécurité telles que la non-divulgation de leur identifiant de connexion à leur compte ENT. Pour encourager et faciliter cette sensibilisation, la désignation de correspondants informatique et libertés me semble être la voie à privilégier. De plus, cette désignation pourrait utilement être accompagnée de la mise en place de structures locales d'utilisateurs ENT sur le modèle des Commissions locales informatique et libertés (CLIL). Je me félicite à cet égard de l'initiative prise par l'académie de Nancy – Metz qui a été l'une des premières académies à désigner un correspondant à la protection des données dans le cadre du déploiement des ENT.

Qu'est-ce que c'est ?

UN ENT
ESPACE NUMÉRIQUE DE TRAVAIL

Considérés comme des téléservices de l'administration électronique, les ENT, parfois aussi appelés « cartable électronique », « cartable numérique » ou « bureau virtuel » sont des sites web portail permettant aux élèves et à leurs parents, aux étudiants, aux enseignants, aux personnels administratifs et plus généralement à tous les membres de la communauté éducative, d'accéder, via un point d'entrée unique et sécurisé, à un bouquet de services numériques (accès à des contenus à vocation pédagogique et éducative, diffusion d'informations administratives ou relatives à la vie scolaire et au fonctionnement de l'établissement). Un ENT permet, par exemple, à un élève d'avoir accès via Internet à son cahier de textes, à ses notes et à ses bulletins trimestriels. Un élève peut se connecter à son ENT depuis son domicile, dès lors qu'il dispose d'un micro-ordinateur équipé d'un navigateur Internet et d'une connexion à Internet, ou à partir des points d'accès à Internet disponibles dans chaque établissement.



Source de l'image: Cellule d'animation ENT – Ministère de l'Éducation nationale/Caisse des Dépôts.

CONFIANCE
INTERNET SANS CRAINTE

La CNIL est partenaire du projet « CONFIANCE » mené par le ministère de l'Éducation nationale.

Vinz et Lou sur internet

LE NIR : UN NUMÉRO PAS COMME LES AUTRES

Questions à …

JEAN MASSOT

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

Quelles sont les raisons qui justifient un encadrement particulier de l'utilisation du NIR ?

Le numéro de sécurité sociale, parce qu'il est plus facile à reconstituer à partir des éléments d'état civil, parce qu'il rend plus aisées les possibilités de rapprochements de fichiers et facilite la recherche et le tri des informations dans les fichiers, reste associé au risque d'une interconnexion généralisée ou d'une utilisation détournée des fichiers.

Cela justifie les précautions prises, depuis 1978, par le législateur et par la CNIL pour encadrer l'usage du NIR. Ainsi, même dans les cas où le législateur a cru devoir autoriser, sous certaines conditions, le recours au NIR dans les fichiers, il a prévu que les modalités d'utilisation du numéro seraient déterminées après avis ou autorisation de la CNIL. S'appuyant sur les dispositions de la loi, la CNIL a développé une doctrine de « cantonnement », selon laquelle chaque sphère d'activité (fiscalité, éducation nationale, banques, police…) devait être dotée d'identifiants sectoriels. Cela vaut notamment dans le domaine fiscal avec la mise en place d'un identifiant spécifique, le SPI. En revanche, le NIR ayant été utilisé dès l'origine dans le secteur de la sécurité sociale, la CNIL a admis qu'il soit enregistré dans l'ensemble des fichiers des organismes en relation avec ce secteur.

Pourquoi le NIR ne peut-il être aujourd'hui l'identifiant du secteur médical ?

Il est vrai que le recours à l'identifiant fiable (car associé à des éléments d'état civil certifiés) et disponible qu'est le NIR peut apparaître comme la solution permettant de résoudre les problèmes qui résulteraient de la création d'un identifiant spécifique pour une population de plus de 60 millions de personnes.

La Commission n'ignore pas, en outre, que des informations relatives à la santé (informations nécessaires à la prise en charge des assurés et à une meilleure connaissance des dépenses de santé) figurent dans les fichiers de l'assurance maladie et, chez les professionnels et établissements de santé, dans les fichiers de gestion administrative des patients identifiés alors par leur numéro de sécurité sociale. Ces extensions de l'utilisation du NIR ne remettent toutefois pas en cause le principe du « cantonnement » de son usage à la sphère sociale, car elles ont répondu à une même finalité de protection sociale.

Tout en évaluant précisément les arguments favorables à l'utilisation du numéro de sécurité sociale comme identifiant du dossier médical, la Commission a estimé que le NIR, compte tenu des risques précédemment évoqués et du caractère particulièrement sensible des données de santé, ne constitue pas, aujourd'hui, un numéro adapté pour identifier le dossier médical de chacun.

En outre, elle a considéré que, même si des mesures de protection toutes particulières étaient prises en ce qui concerne les procédures d'accès et d'authentification, l'utilisation directe d'un numéro aussi répandu que le NIR serait de nature à altérer le lien de confiance entre les professionnels de santé et les patients, ceux-ci pouvant légitimement s'interroger sur les risques d'accès non-contrôlé à leur dossier médical par cet identifiant largement connu.

Quelle est la solution préconisée par la CNIL ?

La Commission a estimé que la méthode la plus à même d'apporter les garanties souhaitables serait **la création d'un identifiant de santé spécifique, généré à partir du NIR certifié selon les procédures déjà éprouvées**, actuellement utilisées pour les bénéficiaires de l'assurance maladie, mais transcodé selon des techniques reconnues d'anonymisation. Ce numéro, non signifiant, constituerait l'identifiant de santé utilisable dans l'ensemble du système de soins.

Cette solution qui se veut équilibrée permet de bénéficier des avantages du NIR au moment de la création de l'identifiant tout en maintenant un niveau de garantie élevé. La Commission a toutefois souhaité faire valoir en outre que le choix de l'identifiant de santé, quel qu'il soit, ne permettra pas de faire l'économie des procédures de vérification de l'identité du patient et de normalisation qui sont nécessaires, en particulier dans les établissements de soins, tant lors de l'admission que tout au long du parcours de soins, afin d'éviter tout risque de confusion dont les conséquences pourraient être particulièrement graves pour les personnes. Il est indispensable de mettre en place, dans l'ensemble des structures de soins, des procédures spécifiques d'« identité-vigilance » permettant de s'assurer que le dossier médical se rapporte bien à la personne concernée, en particulier au vu des autres éléments d'identité, produits par la personne, et des actes médicaux réalisés.

Quel identifiant pour le secteur de la santé ?

Le 26 octobre 2006, M. Alex Türk, président de la CNIL, a décidé la création d'un groupe de travail ayant pour mission l'évaluation de la doctrine sur l'utilisation du NIR, numéro d'inscription au Répertoire national d'identification des personnes physiques (RNIPP), communément appelé numéro de sécurité sociale, au regard des nouveaux contextes juridiques et techniques, et dans la perspective de l'apparition d'autres identifiants nationaux.

Le groupe de travail, présidé par M. Jean Massot, a procédé à plusieurs auditions et effectué des visites sur place lui permettant d'effectuer un certain nombre de constats et de dégager des conclusions qui ont été approuvées par la Commission en séance plénière le 20 février 2007.

Le constat selon lequel « le NIR n'est pas un numéro comme les autres » a d'abord été rappelé. Il est signifiant, unique et pérenne et *a priori* fiable puisqu'il est certifié par l'INSEE à partir des données d'état civil.

Il apparaît ainsi que l'évolution des techniques qui facilite le rapprochement de fichiers sans numéro d'identification commun et l'émergence d'autres identifiants très intrusifs (biométrie), ne font pas disparaître les craintes suscitées par l'utilisation et la diffusion généralisée d'un identifiant national unique et signifiant comme le NIR.

La question du choix d'un identifiant pour le secteur de la santé était plus particulièrement posée à la CNIL. En effet, le législateur a prévu la création d'un identifiant de santé des personnes prises en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé, notamment pour l'ouverture et la tenue du dossier médical personnel (DMP). Un décret pris après avis de la CNIL doit déterminer cet identifiant ainsi que ses modalités d'utilisation.

Le NIR ne peut pas être utilisé par des organismes de recouvrement de créance ou des établissements de crédit

En adoptant quatre refus d'autorisation lors de sa séance plénière du 23 février 2006, la CNIL a rappelé qu'au regard des risques présentés par la généralisation de l'usage du NIR et de l'application du principe de proportionnalité défini à l'article 6-3° de la loi du 6 janvier 1978 modifiée en 2004, l'utilisation du NIR par des organismes de crédit ou de recouvrement n'intervenant pas dans le secteur de la protection sociale ne peut être admise.

Questions à ...

BERNARD PEYRAT

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

Pouvez-vous nous rappeler la dimension historique du NIR dans la loi informatique et libertés ?

À l'origine de la loi informatique et libertés se trouve le rejet du projet SAFARI d'interconnexion de fichiers publics à partir du numéro de sécurité sociale ou NIR. En effet, l'utilisation généralisée d'un identifiant unique dans l'ensemble des fichiers, en ce qu'elle faciliterait leur interconnexion, permettrait de suivre les individus dans tous les actes de la vie courante si un encadrement et des garanties précises n'avaient été prévues par le législateur en 1978 puis en 2004.

Ces considérations ont conduit la CNIL à limiter l'usage du NIR en tant qu'identifiant propre à la sphère de la santé et à la sphère sociale et à recommander le recours à des identifiants spécifiques à chaque secteur d'activité. Les dérogations prévues par le législateur n'ont porté que sur des cas limités, justifiés par l'intérêt général.

Quel est l'encadrement spécifique de l'utilisation du NIR par des organismes privés ?

L'article 25-5° de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 soumet désormais à l'autorisation de la CNIL les traitements des organismes privés portant sur des données parmi lesquelles figure le NIR. Par ailleurs, il résulte des dispositions de l'article 7-5° que la réalisation de l'intérêt légitime du responsable de traitement doit être prise en compte sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Quels sont les motifs principaux qui ont motivé les refus d'autorisation ?

La lutte contre la fraude ou l'homonymie sont des finalités qui, bien que légitimes, ne suffisent pas, à elles seules, à justifier l'utilisation du NIR dans le cadre de gestion de produits d'épargne, de gestion de crédits ou encore du recouvrement de créance. Les mutuelles, les entreprises d'assurances et les institutions de retraite complémentaires et de prévoyance sont autorisées à utiliser le NIR pour l'exercice de leurs activités d'assurance maladie, de maternité, d'invalidité complémentaires et d'assurance vieillesse mais non pour la gestion de la relation commerciale. Pour la gestion de ses actions commerciales, chaque organisme doit se doter d'un identifiant spécifique.

LA CONSULTATION ADMINISTRATIVE DES FICHIERS DE POLICE

Le recrutement à certains emplois publics participant à l'exercice des missions de souveraineté de l'État, aux emplois relevant de la sécurité ou des domaines des jeux, paris et courses impose qu'il soit procédé à des enquêtes administratives dites de moralité. Pour apprécier la situation de l'intéressé, la loi prévoit que les administrations puissent obtenir un extrait du casier judiciaire. Mais depuis 2001, les fichiers de police judiciaire dits d'antécédents (STIC et JUDEX) peuvent aussi être consultés. Ainsi, le décret du 6 septembre 2005 a considérablement élargi la liste des enquêtes donnant lieu à consultation des fichiers de police judiciaire. Depuis plusieurs années, la CNIL tire la sonnette d'alarme sur les conséquences sociales de la consultation des fichiers de police judiciaire et sur le rôle de casiers judiciaires parallèles qu'on leur fait ainsi jouer sans qu'ils bénéficient des règles rigoureuses d'effacement prévues par le code de procédure pénale pour le casier (*cf.* notamment le 26e rapport d'activité de la CNIL).

Comment améliorer le contrôle et l'organisation des fichiers de police judiciaire utilisés dans le cadre des enquêtes administratives ?

Pour répondre à cette question, deux réflexions ont été lancées au cours de l'année 2006.

L'une pilotée par la CNIL, au sein d'un groupe de travail constitué en son sein, sous la présidence de Patrick Delnatte, avait pour objet d'évaluer les raisons pour lesquelles les conditions de fonctionnement actuelles du casier judiciaire ne sont pas étrangères à l'orientation prise de privilégier la consultation de ces fichiers de police et, le cas échéant, de faire œuvre de propositions pour encourager l'utilisation du casier.

L'autre mission de réflexion, confiée par le ministre de l'Intérieur au président du conseil d'orientation de l'Observatoire national de la délinquance, M. Alain Bauer, devait permettre, après un recensement des fichiers de police disponibles, de proposer des solutions visant à améliorer l'organisation de ces fichiers afin d'éviter le maintien d'informations erronées ou dépassées. Cette réflexion a été conduite dans le cadre d'un groupe de travail composé notamment des responsables concernés de la police nationale et de la gendarmerie, d'autorités administratives concernées – dont la CNIL –, de personnalités qualifiées et d'avocats.

Le groupe de travail de la CNIL relatif au fonctionnement du casier judiciaire

Questions à ...

PATRICK DELNATTE

Député du Nord
Commissaire en charge du secteur «Justice»

Pourquoi la CNIL a-t-elle créé un groupe de travail chargé d'évaluer la réalité des difficultés de fonctionnement du casier judiciaire national ?

À maintes reprises, et notamment dans ses précédents rapports annuels, la Commission a souligné les difficultés que soulevait le recours aux fichiers de police judiciaire (le STIC pour la police nationale et JUDEX pour la gendarmerie), dans le cadre des enquêtes administratives réalisées pour l'accès à certains emplois de gardiennage et de sécurité.

Les conséquences pour les personnes peuvent être très importantes : ainsi, des candidats à l'embauche peuvent se voir refuser un emploi ou encore des salariés peuvent être licenciés sur la base de signalements, parfois injustifiés, erronés ou périmés figurant dans le STIC ou dans JUDEX.

Or, les services préfectoraux ne disposent pas que des seuls fichiers de police judiciaire pour mener leurs enquêtes dans ce secteur. Ils sont en effet en droit d'obtenir communication d'extraits du casier judiciaire, les bulletins dits n° 2, qui comportent un grand nombre de condamnations, à l'exception notamment de celles prononcées contre les mineurs.

La CNIL a donc souhaité comprendre pourquoi les autorités administratives privilégiaient la consultation des fichiers de police judiciaire, plutôt que celle du casier judiciaire, pour prendre ses décisions et a constitué, à cet effet, un groupe de travail.

Quels travaux ont été menés par ce groupe de travail ?

Afin d'avoir une vision concrète des difficultés, le groupe de travail s'est déplacé auprès du service du casier judiciaire national à Nantes, d'un tribunal de grande instance et d'une préfecture de la région parisienne.

Il a par ailleurs organisé de nombreuses auditions de syndicats représentant des magistrats, des avocats, des greffiers, des professionnels de la sécurité et des personnalités ou «experts», ainsi que des représentants du ministère de la Justice et du ministère de l'Intérieur.

Ces travaux, très riches, ont permis à la Commission d'aboutir à plusieurs constats.

Quels sont ces constats ?

Le groupe de travail a pu constater que les délais d'alimentation du casier judiciaire par les juridictions sont, faute de moyens humains et matériels, de l'ordre de plusieurs mois. Par exemple, au tribunal visité par le groupe, ce délai est compris entre huit et quatorze mois.

Dans ces conditions, les services préfectoraux ne peuvent disposer d'un bulletin n° 2 «à jour», et c'est pourquoi, alors que ce n'est qu'une simple faculté, ils se tournent vers les fichiers de police judiciaire. Or, la mise à jour de ces fichiers, si elle s'est améliorée, demeure encore insuffisante, ce qui conduit aux difficultés constatées par la Commission depuis plusieurs années dans ce domaine.

Pour remédier à ces difficultés, le groupe de travail a proposé plusieurs pistes d'amélioration tant du casier judiciaire que des fichiers de police judiciaire qui ont été portées à la connaissance du garde des Sceaux et du ministre de l'Intérieur. **(voir aussi les propositions de la CNIL aux pouvoirs publics p. 83)**

Le rapport de l'Observatoire national de la délinquance

Le 23 novembre 2006, le président du conseil d'orientation de l'Observatoire national de la délinquance a remis au ministre de l'Intérieur le rapport du groupe de travail sur le contrôle de l'utilisation administrative des fichiers de police auquel la CNIL a activement participé.

Ce rapport pointe certains dysfonctionnements liés à l'utilisation administrative des fichiers de police et formule des propositions pour y remédier.

Pour la CNIL, ces dysfonctionnements sont de quatre ordres.

L'exercice des droits individuels : des délais de réponse excessifs

Les délais de réponse du ministère de l'Intérieur aux demandes de droit d'accès indirect transmises par la CNIL sont actuellement de l'ordre de plusieurs mois.

Au 1er septembre 2006, la CNIL était en attente de la réponse des services de police judiciaire pour plus de 500 dossiers dont certains datant de 2004. **Ainsi, en définitive, pour les personnes mises en cause signalées dans le STIC, l'ensemble de la procédure peut atteindre deux ans.**

Or, le décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée en 2004 prévoit, en son article 87, que la CNIL notifie au demandeur le résultat de ses investigations dans un délai de quatre mois à compter de sa saisine. Ce texte prévoit aussi que le responsable du traitement dispose, pour réaliser ses investigations, d'un délai de trois mois à compter de la transmission de la demande de droit d'accès par la Commission.

Les modalités actuelles d'instruction des demandes par le ministère de l'Intérieur et la lenteur des réponses des parquets ne permettent donc pas, en l'état, à la Commission de respecter les termes du décret. Même si les moyens en personnel du ministère de l'Intérieur ont été récemment renforcés, ceux-ci restent sans doute insuffisants pour traiter les demandes. Au-delà, le retard constaté dans le traitement des dossiers provient aussi des parquets, qui, compte tenu de leur charge de travail et du manque de moyens en personnel, ne peuvent aujourd'hui transmettre leurs réponses aux demandes de suites judiciaires dans les délais impartis.

De son côté, la CNIL connaît elle-même un certain retard dans le traitement des dossiers, ne disposant actuellement que de deux personnes pour assurer la gestion de l'instruction des demandes.

Il apparaît impératif aujourd'hui de prendre les mesures nécessaires pour traiter les demandes dans des délais raisonnables. Les exemples présentés dans le chapitre sur le droit d'accès indirect montrent combien les délais de traitement peuvent pénaliser les personnes, tout particulièrement lorsqu'il s'agit de cas de signalements erronés.

La question des mises à jour, rectifications et effacements

Les statistiques de la CNIL fondées sur les contrôles qu'elle assure dans le cadre du droit d'accès indirect mettent en lumière **des dysfonctionnements liés à l'absence d'une procédure de transmission régulière par les parquets des suites judiciaires favorables au gestionnaire du STIC**, pourtant prévue et demandée par la CNIL à plusieurs reprises (*cf.* sur ce point les avis successifs rendus par la CNIL sur le fichier STIC).

S'agissant des durées de conservation, il doit être relevé que le logiciel mis en place en 2004 a permis d'éliminer plus de 1,2 million de fiches (pour des motifs d'expiration des délais) et, du fait de l'épurement désormais réalisé tous les mois, conduit à effacer les données dont la durée de conservation arrive à expiration dans le mois en cours. Cette cause de signalement injustifié devrait donc disparaître.

Les autres motifs – problème de requalification de l'infraction, infraction non constituée, enregistrement à tort comme mis en cause, absence d'archive – semblent relever d'erreurs de saisie à la source et du contrôle insuffisant des parquets sur le contenu des fiches STIC. Le fait que les parquets ne disposent pas de terminaux d'accès au STIC leur permettant en temps réel de vérifier le contenu des fiches STIC constitue assurément un obstacle à l'exercice effectif de leur contrôle.

L'information insuffisante des personnes sur leurs droits

Alors que le législateur, en particulier par la loi du 18 mars 2003, a expressément reconnu aux personnes inscrites dans les fichiers de police judiciaire un certain nombre de droits, tels que la possibilité, sous certaines conditions, de demander la rectification des données en cas de requalification judiciaire et, s'agissant des victimes, l'effacement des données les concernant, ces droits ne sont, en pratique, pas ou peu exercés, faute d'être connus.

L'information des personnes sur l'existence et les conditions d'exercice de ces droits, ainsi que sur leur droit d'accès, devrait être reconnue et garantie par des mesures spécifiques telles que l'affichage dans les locaux des commissariats et/ou des mentions sur les dépôts de plaintes.

Quant à la communication aux intéressés des informations les concernant, elle n'est effective que depuis août 2005 (soit plus de quatre ans après l'entrée en vigueur du décret du 5 juillet 2001) et met en œuvre une procédure particulièrement longue et complexe puisqu'elle nécessite le double accord du ministère de l'Intérieur et du parquet.

La question se pose donc de maintenir cette procédure d'accord préalable, alors même qu'une instruction du 15 avril 2005 adressée par le ministre de l'Intérieur aux préfets leur fait désormais obligation de motiver leur décision de refus et d'indiquer précisément les raisons de celui-ci et notamment les faits pour lesquels ils sont signalés dans le STIC. Dès lors que les intéressés connaissent les motifs pour lesquels ils sont fichés (au moins pour ce qui concerne les personnes employées ou susceptibles de l'être dans le cadre d'activités de sécurité privée), on peut légitimement s'interroger sur l'intérêt qu'il y a à requérir le double accord du ministère de l'Intérieur et du parquet.

Il en est de même s'agissant des victimes : dès lors qu'elles ont déposé plainte pour tel ou tel fait, et que la procédure qui s'ensuit donne lieu à signalement dans le STIC, on ne comprend pas véritablement les raisons pour lesquelles elles ne pourraient pas accéder directement au contenu de leur fiche.

Le problème des infractions mineures et de la durée de conservation

Quel est le bien fondé d'une consultation systématique à des fins administratives des fichiers de police judiciaire s'agissant des personnes mises en cause pour des faits relevant d'une contravention de 5e classe ou de certains délits qui, à l'évidence, ne mettent pas en cause « la protection de la sécurité des personnes ou la défense des intérêts fondamentaux de la nation » ?

La CNIL a ainsi eu connaissance de plusieurs cas de personnes licenciées (alors qu'elles étaient employées depuis de nombreuses années dans une société de sécurité) ou refusées à l'embauche en raison d'un signalement dans le STIC, pour des infractions qui, après lecture de la procédure, ne relevaient pas, de son point de vue ni d'ailleurs de l'avis du parquet compétent, des cas justifiant que la personne ne soit pas recrutée ou soit licenciée : par exemple des cas de signalement pour violences conjugales (dont il s'avérait, à la lecture de la procédure, qu'il s'agissait d'un différend réglé par la voie d'un classement sans suite) ou pour non-représentation d'enfant dans le cadre d'un divorce, ou d'infractions telles que des atteintes à la dignité de la personne (qui relevaient plutôt d'un problème relationnel entre un professeur et son élève).

Comme la CNIL l'a déjà souligné, **il apparaît indispensable qu'une véritable réflexion de fond soit menée sur ce sujet**. À cet égard, la situation risque de s'aggraver, d'une part avec l'élargissement considérable de la liste des enquêtes donnant lieu à consultation des fichiers de police judiciaire, que consacre le décret du 6 septembre 2005, et d'autre part, avec l'extension possible du champ d'application du fichier STIC à l'ensemble des contraventions de 5e classe contre les biens, contre les personnes et contre la nation, l'État ou la paix publique.

Questions à ...

FRANÇOIS GIQUEL

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

Selon quelles modalités la CNIL a-t-elle contribué aux travaux du groupe ?

À la demande du président de la CNIL, j'ai représenté la Commission au sein du groupe de travail et participé à l'ensemble de ses séances et j'ai ainsi pu faire part des constats et propositions de notre Commission sur cette question qui constitue depuis longtemps pour nous un important sujet de préoccupations. Je tiens à cet égard à souligner la qualité des travaux menés par le groupe ainsi que la richesse des débats.

Par différentes contributions écrites, souvent illustrées de statistiques précises et de cas concrets, nous avons dressé, à la demande du groupe de travail, un état des dysfonctionnements constatés par la CNIL dans l'utilisation administrative du fichier de police judiciaire STIC, tels qu'ils ont pu être relevés dans le cadre de l'instruction des demandes de droit d'accès indirect qui lui sont présentées.

Que pensez-vous des propositions du groupe de travail ?

La Commission souscrit à ces propositions qui, pour une large part, s'inscrivent dans le cadre de ses propres préconisations.

Ainsi, elle est tout à fait favorable à ce qu'une véritable action de communication publique sur les modalités de fonctionnement des fichiers de police judiciaire soit réalisée chaque année et à ce que les personnes signalées dans ces fichiers soient mieux informées de leurs droits (et en particulier de leur droit d'accès) et des voies de recours existantes. Il faut améliorer la transparence des fichiers.

Elle ne peut aussi qu'accueillir favorablement les différentes propositions formulées par le groupe de travail pour assurer une mise à jour régulière des fichiers de police judiciaire, telles que la mise en place d'un groupe de travail police – justice – gendarmerie chargé d'étudier, de façon concertée, les modalités d'amélioration des systèmes informatiques de ces différentes administrations. De même, la démarche « qualité » dans l'alimentation et la mise à jour des fichiers par ceux qui en sont responsables doivent être bien évidemment poursuivies.

Enfin, la Commission approuve pleinement la recommandation du groupe de travail préconisant une réflexion de fond sur les modalités de prise en compte des contraventions de 5e classe dans le cadre des enquêtes administratives,

LE DOSSIER MÉDICAL PERSONNEL

L'encadrement juridique des hébergeurs

La procédure particulière d'agrément des hébergeurs de données de santé à caractère personnel prévue par la loi est entrée en vigueur le 4 janvier 2006, date de parution du décret d'application des dispositions issues de la loi de 2002 sur les droits des malades. À la veille des expérimentations du dossier médical personnel, l'intervention de ce texte était indispensable pour encadrer l'activité des organismes appelés à conserver des dossiers médicaux.

Cet agrément est délivré par le ministre chargé de la Santé, qui se prononce après avis de la CNIL et du comité d'agrément créé auprès de lui.

Il s'agit donc d'organiser le dépôt et la conservation des données de santé dans des conditions de nature à garantir leur pérennité et leur confidentialité, à charge pour l'hébergeur de les mettre à la disposition des personnes autorisées selon des modalités définies par contrat et de les restituer en fin de contrat. La prestation de l'hébergeur ne se limite donc pas à un simple stockage de données.

Un grand nombre d'applications sont ainsi susceptibles d'être concernées par ces dispositions : le dossier médical personnel (DMP), les réseaux de soins dès lors que ceux-ci font héberger leurs données de santé, les sites ouverts au public et qui hébergent les données de santé des patients qui s'y connectent et l'archivage externe des dossiers médicaux des établissements de soins.

Les personnes à l'origine du dépôt des données sont exclusivement la personne concernée, les professionnels de santé et les établissements de santé participant à l'acte médical, qu'il soit préventif, diagnostic ou de soin. À cet effet, un contrat doit être conclu entre le déposant et l'hébergeur, qui détermine en particulier les droits et obligations de chacun et les modalités d'accès et de transmission des informations hébergées.

Dans le cadre de l'expérimentation du DMP, les dossiers médicaux personnels des patients volontaires pour participer ont été hébergés par six hébergeurs de données de santé agréés par décision du ministre de la Santé du 22 mai 2006, après avis de la CNIL du 21 mars 2006 et du comité d'agrément placé auprès du ministre du 16 mai 2006. Le groupement d'intérêt public du dossier médical personnel (GIP-DMP) qui coordonne l'expérimentation a conclu des conventions d'expérimentation avec ces hébergeurs.

La suspension de la procédure d'agrément des hébergeurs de données de santé

La loi du 30 janvier 2007 ratifiant l'ordonnance du 26 août 2005 relative à l'organisation de certaines professions de santé **a suspendu, sauf lorsqu'il s'agit d'héberger des dossiers médicaux personnels, la procédure d'agrément pendant deux ans** à compter du 2 février 2007.

Cette suspension est justifiée par la nécessité de définir préalablement des référentiels de sécurité communs à l'ensemble du secteur de la santé.

La loi précise également que l'hébergeur doit satisfaire aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. De même, les réseaux de soins, les professionnels de santé et les établissements de soins sont soumis au régime d'autorisation (article 25-IV de la loi du 6 janvier 1978 – traitements de données de santé justifiés par l'intérêt public) dans la mesure où ils sont responsables des applications de dossiers médicaux partagés.

Questions à ...

JEAN-PIERRE DE LONGEVIALLE

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

À quelles conditions la CNIL a-t-elle subordonné la mise en œuvre des traitements nécessaires à l'expérimentation du DMP ?

La CNIL a délibéré le 30 mai 2006 sur les applications informatiques mises en œuvre par les hébergeurs, au sein des établissements de soins et par les professionnels de santé participant à l'expérimentation du dossier médical personnel dans treize régions et dix-sept sites pilotes retenus par le GIP-DMP.

Cette expérimentation a impliqué la participation de 1 500 professionnels de santé libéraux, 68 établissements de soins publics et privés et 37 réseaux de soins.

La finalité principale de l'expérimentation du dossier médical personnel était de tester la faisabilité et l'acceptabilité du dispositif envisagé. En particulier, les objectifs étaient d'identifier les conditions d'appropriation du DMP par les professionnels de santé et les patients, de mettre en évidence l'impact du DMP sur les pratiques médicales et d'obtenir ainsi une évaluation de la satisfaction des acteurs. Il s'agissait également de mesurer la qualité de service assurée par les hébergeurs et l'intérêt effectif des services proposés.

Compte tenu des modalités ainsi définies, la CNIL a rappelé sa préoccupation sur trois points importants :

– la nécessité d'une **information complète des patients** sur les conditions de participation à cette expérimentation, leur consentement libre et éclairé devant être recueilli. Une note d'information remise par le professionnel de santé en contact avec le patient précisait notamment la finalité poursuivie par la création à titre expérimental d'un dossier médical personnel, le processus de création du DMP, le contenu de ce dossier, les différentes modalités d'alimentation et d'utilisation du DMP et les conditions d'accès à son dossier. Le patient pouvait avoir accès directement à son dossier. Il avait également la possibilité de « masquer » certaines informations de son dossier aux professionnels de santé ;

– s'agissant **des mesures de sécurité** mises en œuvre par les hébergeurs du DMP, la Commission, dont c'est une recommandation constante en matière de sécurisation des bases de données sensibles, estime nécessaire que les bases de données des hébergeurs fassent l'objet d'un chiffrement complet pour assurer de façon satisfaisante la confidentialité des données. Une architecture de sécurité reposant uniquement sur le chiffrement des canaux de télétransmissions et sur un contrôle d'accès au système informatique n'est pas suffisante au regard de la sensibilité des données médicales ;

– sur **l'utilisation de la carte de professionnel de santé (CPS)** et la mise en œuvre du certificat électronique qui lui est attaché, la Commission réaffirme la nécessité pour les établissements de soins d'utiliser la CPS ou tout dispositif logiciel équivalent, tout en reconnaissant qu'un délai est indispensable pour la mise en œuvre pratique de ces exigences.

Quel bilan tirez-vous des expérimentations du DMP ?

La Commission a mené, au cours de l'année 2006, une vaste opération de contrôle sur place afin d'apprécier les conditions de mise en œuvre du DMP. Une quinzaine de missions de contrôle ont ainsi été menées auprès des principaux acteurs de l'expérimentation dans chacune des zones géographiques retenues et auprès des hébergeurs bien sûr, mais aussi des centres hospitaliers, réseaux de santé, médecins libéraux et centres d'appel.

Ces contrôles ne visaient pas à avoir une vision exhaustive des pratiques des hébergeurs et des professionnels de santé dans le cadre de l'expérimentation du DMP, mais à apprécier l'application des garanties demandées par la CNIL dans ses décisions de mars 2006, notamment en ce qui concerne la mise en place des pratiques de chiffrement par les hébergeurs ou l'utilisation de la CPS par les professionnels de santé concernés par l'expérimentation.

Il a pu être constaté que, si l'objectif fixé de créer cinq mille DMP par hébergeur a été atteint, en revanche, peu de DMP ont réellement fonctionné, la durée de l'expérimentation ayant été trop courte.

On peut le regretter, dans la mesure où l'expérimentation avait pour objet de tester l'acceptabilité du DMP et son appropriation par les patients, ou encore l'usage qui serait fait du droit de masquage de certaines données ou de la procédure de « bris de glace » permettant aux professionnels de santé en cas d'urgence d'accéder au DMP.

La question qui reste préoccupante pour la CNIL est celle du nombre relativement restreint, dans le monde hospitalier, de professionnels de santé qui utilisent de façon effective la carte de professionnel de santé ou un certificat logiciel équivalent pour accéder au dossier médical personnel, ce qui pose la question plus générale du niveau de sécurité actuellement appliqué dans les établissements de santé.

C'est votre droit

LE DROIT DE MASQUAGE DES INFORMATIONS DANS LE DMP

Le droit de masquage des informations contenues dans le DMP, prévu par les dispositions de l'avant-projet de décret sur le DMP, peut apparaître comme une application du droit, reconnu par **l'article 40 de la loi informatique et libertés**, à toute personne physique dont des données à caractère personnel font l'objet d'un traitement de les rectifier, les compléter ou les supprimer lorsqu'elles s'avèrent inexactes, incomplètes, équivoques ou périmées.
Il constitue également une application du droit reconnu par **l'article 38** de la même loi permettant à toute personne de s'opposer pour des raisons légitimes à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.
Si l'exercice du droit d'opposition reconnu par l'article 38 de la loi du 6 janvier 1978 modifiée en août 2004 doit être apprécié au regard du caractère « pratiquement » obligatoire du DMP, dès lors que le législateur a subordonné à l'ouverture et à la consultation de ce dossier le niveau de remboursement des soins, la reconnaissance d'un droit de masquage des informations est de nature à équilibrer la relation entre le patient et le professionnel de santé.
Le DMP est le dossier personnel du patient. Dès lors, il est normal qu'il en maîtrise le contenu et les accès. L'exercice du droit de masquage permettra également de traduire une certaine réalité de la relation médecin – patient dans laquelle le patient ne se dévoile pas toujours immédiatement. L'argument selon lequel la reconnaissance d'un droit de masquage serait de nature à nuire à l'efficacité des soins doit être relativisé dans la mesure où la relation médecin – patient s'est toujours accompagnée de « non-dits » et où une information « cachée » à un moment donné pourra être révélée à un autre moment de la relation ou en fonction de la nature des soins prodigués.
L'exercice du droit de masquage doit nécessairement s'accompagner d'une information complète et claire du patient sur ses conséquences.

Dernière minute !

La Commission a décidé, lors de sa séance du 21 mars 2007, de synthétiser les constats opérés à l'issue des missions de contrôle effectuées dans le cadre de l'expérimentation du DMP dans un document public, accessible depuis son site web. Ce document, qui constate notamment l'insuffisance de certaines mesures de sécurité, a parallèlement été adressé au GIP-DMP et au ministère de la Santé.

LE VOTE ÉLECTRONIQUE

Le vote électronique des Français de l'étranger

Questions à ...

ISABELLE FALQUE-PIERROTIN

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

Quelles étaient les spécificités du vote électronique des Français de l'étranger en 2006 ?

Il avait plusieurs caractéristiques propres : son étendue (plusieurs dizaines de milliers de Français répartis dans différentes régions du monde) et son caractère politique. Il s'agissait, en effet, du seul scrutin politique où un vote électronique à distance est autorisé par le législateur.

Quelle a été la position de la CNIL sur le dispositif mis en place ?

La Commission a regretté, dans l'avis du 23 février 2006 qu'elle a rendu sur ce dispositif, l'absence d'expertise indépendante. Alors même que le décret organisant le vote par correspondance électronique ainsi que l'arrêté pris en application de ce décret le prévoyaient, aucun rapport d'expertise n'a été transmis à la CNIL ni avec le dossier de formalités préalables ni après les opérations de vote. La CNIL a cependant reconnu, dans le dossier soumis, l'intérêt de la mise en place d'un bureau central du vote électronique chargé du contrôle de l'ensemble des opérations de vote électronique et du dépouillement du vote qui était assisté par un comité technique. La Commission a demandé que ce comité soit composé d'experts techniques. Elle a également pris acte que le système de vote présenté entendait mettre en œuvre des procédés rendant impossible l'établissement d'un lien entre le nom de l'électeur et l'expression de son vote et garantissant le secret du vote. Toutefois, les éléments d'analyse du système de vote qui lui ont été fournis ne permettaient pas de s'assurer de l'effectivité de la séparation de l'urne et du fichier des électeurs sur des systèmes distincts, dédiés et isolés. Il en va de même pour le chiffrement des bulletins de vote.

S'agissant de l'authentification des électeurs, la CNIL a rappelé que la fiabilité d'un envoi postal non recommandé des codes personnels est étroitement liée aux conditions de fonctionnement de la poste de chaque pays. Elle a donc demandé qu'en cas de perte des codes personnels d'un électeur, celui-ci soit explicitement autorisé à voter le jour du scrutin dans un bureau de vote.

En conclusion, l'avis de la CNIL a été de prendre acte des efforts des organisateurs et du prestataire pour sécuriser le dispositif de vote tout en considérant ceux-ci comme insuffisants eu égard à la grande sensibilité du scrutin en cause.

Quel avenir pour le vote électronique ?

On constate que de plus en plus de textes prévoient la possibilité de recourir à des dispositifs de vote électronique pour des élections où le vote par correspondance était traditionnellement utilisé. Il a donc un avenir certain. Mais cet avenir dépend étroitement de la qualité et de la sécurité des solutions techniques qui seront mises en place.

Un bilan critique des expériences de vote électronique menées depuis cinq ans en France et à l'étranger est dès lors nécessaire si l'on souhaite offrir au citoyen les garanties qu'il attend.

AU PROGRAMME 2007

MESURE DE LA DIVERSITÉ, « STATISTIQUES ETHNIQUES », ÉGALITÉ DES CHANCES... LA CNIL ENGAGE LE DÉBAT

Pour lutter contre les discriminations, encore faut-il pouvoir les mesurer. Cette question de la mesure de la diversité dans le cadre de la lutte contre les discriminations concerne directement la CNIL puisque la collecte d'informations faisant apparaître les origines ethniques ou religieuses est précisément interdite par la loi informatique et libertés, à l'exception de quelques cas limitativement énumérés.

La CNIL, en juillet 2005, a rendu publiques ses premières recommandations à destination des employeurs privés et publics qui, dans le cadre de leur politique de lutte contre les discriminations, auraient à utiliser des données à caractère personnel.

Toutefois, il apparaît que ses recommandations n'ont pas toujours été bien comprises car depuis leur publication, la CNIL est régulièrement interpellée sur ce point par les entreprises et les chercheurs, notamment. Avec la mise en place d'un nouveau groupe de travail, il s'agit aussi pour la Commission de mieux expliquer sa position, de dissiper les malentendus qui ont pu résulter d'une mauvaise compréhension de ses positions sur le sujet qui laisseraient à penser que la CNIL s'oppose à la mise en place des outils de lutte contre les discriminations.

Questions à ...

ANNE DEBET

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

Pourquoi la CNIL a-t-elle « relancé » un groupe de travail sur le sujet de la mesure de la diversité ?

La Commission a publié, le 9 juillet 2005, ses premières recommandations sur la mesure de la diversité dans le cadre de la lutte contre les discriminations.

Compte tenu des enjeux que soulève cette question qui concerne tous les domaines de la vie sociale, qu'il s'agisse de l'éducation, du travail, du logement ou de la santé, la CNIL a décidé de poursuivre ses réflexions au sein d'un groupe de travail constitué à cet effet.

En quoi consistent les travaux de ce groupe de travail ?

Un programme ambitieux d'auditions a été réalisé afin de recueillir les analyses des représentants du monde associatif, des syndicats, des entreprises, des universités, des chercheurs, des représentants des grandes religions monothéistes et d'autres acteurs concernés par ce thème : on dénombre plus de soixante auditions de novembre 2006 à février 2007. Parmi ces auditions, celles des 18 et 25 janvier 2007 ont été ouvertes à la presse, ce qui représentait une première pour la CNIL. Ainsi, les journalistes de la presse écrite et audiovisuelle, rassemblés dans la salle Médicis du Sénat, ont pu assister aux échanges de points de vue entre les membres de la CNIL et les personnalités auditionnées. Ces auditions ont été retransmises sur la chaîne Public Sénat. Pour élargir le débat, la CNIL a mis en ligne sur son site un questionnaire afin de recueillir le point de vue des internautes sur cette question.

Quand rendrez-vous vos conclusions ?

Les résultats de cette enquête ainsi que les conclusions du groupe de travail précisant le cadre et les conditions pour une mesure de la diversité conforme aux obligations légales seront rendus publics en mai 2007.

Les enquêtes fondées sur la consonance des patronymes

Au cours de l'année 2006, la Commission s'est prononcée sur deux dossiers portant sur la mesure de la diversité. Il s'agit des traitements du **Conseil représentatif des institutions juives de France (CRIF)** et **de l'Institut national des études démographiques (INED)** qui ont fondé leur méthodologie d'enquête sur la consonance des patronymes. Si cette méthode, consistant à mettre en corrélation un patronyme et une nation ou une ethnie, reste peu fiable de façon générale (notamment pour les originaires des DOM-TOM, en cas de mariages mixtes ou en cas de francisation des noms), elle est employée au service de finalités bien précises. C'est à la lumière de l'analyse de cette finalité que la CNIL a pris ses décisions.

Quelles étaient les finalités des traitements de ces deux organismes ? Pour le CRIF, il s'agissait de constituer une liste des personnes supposées appartenir à la communauté juive, donc à une communauté religieuse, afin de *« mesurer, objectiver et analyser l'état de son opinion en France »*. Pour l'INED, l'objectif de l'enquête était d'analyser l'intégration des descendants d'immigrés marocains et turcs, le critère étant donc la nationalité des personnes cibles.

Le CRIF

La CNIL s'est opposée au traitement du CRIF à deux reprises. Dans sa délibération du 2 février 2006, la Commission a considéré que l'obstacle réside dans *« la constitution de l'échantillon des personnes à interroger qui repose uniquement sur un tri sur la consonance de leur nom et que ce tri a pour objet même de faire apparaître l'appartenance, réelle ou supposée, des intéressés à la communauté juive »*. Par ailleurs, la Commission a estimé que *« le postulat selon lequel les personnes ayant un nom figurant dans le* Guide des patronymes juifs *appartiennent à la communauté juive «est contestable et souligne les risques liés à une sélection de ce type» »*. Elle a donc considéré que *« le traitement de données ne répondait pas aux conditions posées par l'article 6 de la loi aux termes duquel les données doivent être «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées», d'autant que les objectifs poursuivis par l'enquête, dont* **la légitimité n'est pas en cause**, *semblent pouvoir être atteints en modifiant la méthode de constitution de l'échantillon des personnes à interroger »*.

L'INED

Quant à l'enquête de l'INED, sa mise en œuvre a été autorisée par la délibération du 27 juin 2006 sur la base de l'exception relevant de l'article 8-IV de la loi informatique et libertés. En effet, la Commission a considéré que *« l'enquête envisagée par l'INED est justifiée par l'intérêt public dans la mesure où elle doit permettre de mesurer l'intégration des secondes générations turques et marocaines et contribuer à remédier ainsi à l'insuffisance actuelle de données statistiques dont souhaitent disposer les pouvoirs publics pour définir et mettre en œuvre des politiques en matière d'intégration à l'attention de ces populations, tant au niveau national qu'européen »*.

La Commission a également pris acte que le consentement écrit des personnes enquêtées serait recueilli.

RFID ET NANOTECHNOLOGIES : QUELS ENJEUX POUR LA PROTECTION DES DONNÉES ?

Les puces RFID (Radio-Frequency IDentification) et les nanotechnologies constituent deux défis majeurs pour la CNIL et ses homologues européens, et nécessitent un important travail de prospective et d'anticipation.

Qu'est-ce que c'est ?

LES RFID

Les puces RFID reposent sur une technologie, déjà plus que cinquantenaire, largement améliorée au fil des ans. Il s'agit d'étiquettes silicium/cuivre miniatures composées d'une mémoire pouvant atteindre une grande capacité, associée à un dispositif de communication sans contact et un mécanisme de production d'énergie. Bien que s'étant déjà prononcée à plusieurs reprises sur des dispositifs reposant sur cette technologie (le passe Navigo de la RATP), la CNIL constate que l'usage des RFID entre dans une nouvelle ère : un usage massif pour des finalités toujours plus variées.

Questions à …

PHILIPPE LEMOINE

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

En quoi consistent les nanotechnologies ?

De la micro-informatique, reposant sur des composants dont l'échelle de grandeur est le micron, les nanotechnologies font passer l'informatique à l'échelle du nanomètre, c'est-à-dire de l'atome. Ce changement d'échelle technologique permet de nouveaux gains de performance et devrait également provoquer un phénomène de « méta-convergence » entre les nanotechnologies, les biotechnologies, l'informatique et les sciences cognitives. Les nanotechnologies devraient ainsi trouver des applications dans la médecine, la cosmétique, l'armement ou l'informatique elle-même.

Quels sont les risques en termes de protection des données ?

Bien que très différentes, ces deux technologies (RFID et nanotechnologies) posent de nouvelles problématiques en matière de protection des données personnelles au premier rang desquelles figure leur invisibilité ou quasi-invisibilité (certaines puces RFID mesurent moins d'un millimètre).

Comment garantir le respect de la loi en présence de technologies invisibles ?

Ainsi, certains risques, déjà identifiés par la CNIL concernant les puces RFID, existent, mais sous une forme considérablement amplifiée, concernant les nanotechnologies :

– la possibilité « d'équiper » une personne à son insu ;

– la faculté d'accéder aux données à l'insu de son porteur et la traçabilité de celui-ci ;

– la capacité de stockage en progression constante.

Dans le cas des nanotechnologies, s'ajoute la prospective possible d'un adressage de chaque atome de chaque objet, avec la nouvelle version du protocole Internet, IPV6.

Quel est le rôle de la CNIL ?

La CNIL a déjà proposé des solutions permettant d'améliorer la protection des données à caractère personnel dans le cadre des RFID (désactivation du dispositif à la demande des personnes, sécurisation des données au sein de la puce permettant notamment d'empêcher leur captation frauduleuse…). Pour les nanotechnologies deux priorités animent la CNIL. Il s'agit de participer aux différents débats relatifs à ces questions pour garantir l'application et la cohérence des principes de protection des données à caractère personnel en la matière. Il s'agit également, à l'heure de cette « méta-convergence », de promouvoir et faire appliquer ces principes transversaux à l'échelle mondiale.

LA FRANCOPHONIE : UN ESPACE PRIVILÉGIÉ POUR LA PROTECTION DES DONNÉES

Au centre, M. A. Türk et M. B. Campaoré, président du Burkina Faso, entourés à gauche de M. B. Peyrat, membre de la CNIL, et à droite de Mme M. Ilboudo, ministre des Droits humains du Burkina Faso, Ouagadougou, 21 juillet 2006.

L'influence majeure exercée dans le passé par la France et les autres pays francophones européens dans l'émergence au nord du droit de la protection des données personnelles est connue[1] hors d'Europe. Alors que la législation nationale s'appliquait surtout dans le secteur public, le premier pays à en avoir étendu la portée au secteur privé est la province du Québec en 1993. Le commissaire fédéral chargé de la protection des données en Suisse a pris l'initiative de lancer en 2005, très opportunément à la veille du sommet mondial de la société de l'information, un appel, auquel tous ses homologues ont souscrit, en faveur de l'élaboration d'un instrument de portée mondiale. Cela suppose cependant l'adhésion des pays du Sud.

Compte tenu des missions de la Francophonie, c'est très naturellement au sein de **l'OIF** (Organisation internationale de la Francophonie) que **les enjeux Nord/Sud** concernant la garantie du **droit fondamental de la protection des données dans la société de l'information** ont pu être en premier posés. Les chefs d'État et de gouvernement, conscients de l'opportunité que constituent les technologies de l'information pour la consolidation de l'État de droit, mais aussi pour l'insertion d'activités nouvelles utiles au développement dans le marché mondial, ont pris **l'engagement lors du sommet de Ouagadougou de 2004** de développer les règles de ce droit fondamental et de soutenir la coopération entre les autorités indépendantes. La CNIL s'est fixée pour objectif de contribuer à donner effet à ces engagements qu'elle avait elle-même suscités[2].

LA FRANCOPHONIE

La Francophonie 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 et en transition acquièrent les moyens de générer leur propre dynamique et de maîtriser le processus de leur développement. Présente par ses membres sur les cinq continents, elle entend contribuer à l'humanisation de la mondialisation, selon les termes d'Abdou Diouf, le secrétaire général de l'organisation.

http://www.francophonie.org/oif/missions.cfm

Bilan des actions 2006 : intensification des travaux législatifs et institutionnels dans les pays du Sud

Lors de la visite effectuée par une délégation de la CNIL, conduite par son président, en juillet 2006, auprès d'autorités et de représentants de la société civile du continent

1. Contribution majeure à l'élaboration et à l'adoption de la convention 108 du Conseil de l'Europe de 1981, des lignes directrices de l'OCDE de 1980, des principes directeurs de l'ONU de 1991, de la directive européenne de 1995.

2. CNIL, *25e rapport d'activité 2004*, La Documentation française, 2005, p. 18.

africain, le président de la République du **Burkina Faso**, le Premier ministre du **Mali** et le ministre de la Justice du **Bénin** ont fait part de leur volonté d'accélérer les travaux législatifs et institutionnels pour instituer le droit de la protection des données (préparation d'une législation au Mali et au Bénin, installation de l'autorité indépendante au Burkina Faso). Ils ont également souligné l'intérêt **d'examiner au sein de l'OIF la question de l'élaboration d'une convention internationale**. Ces deux objectifs ont été repris par l'ensemble des chefs d'État et de gouvernement membres et associés de la Francophonie dans la **déclaration de Bucarest en septembre 2006.**

La coopération initiée depuis 2005 avec les autorités du **Sénégal** a donné lieu à de nombreux échanges parallèlement au processus d'élaboration du projet de loi qui doit être déposé au Parlement début 2007.

Plusieurs autorités du **Maroc** ont consulté et invité en 2006 des représentants de la CNIL à participer à des conférences à Marrakech et à Rabat en vue de populariser la dimension de la protection des données. Une coopération est envisagée avec le ministre en charge des Affaires économiques et générales dans le cadre d'un accompagnement législatif.

Enfin, la CNIL se félicite que des services de l'État (Premier ministre, Affaires étrangères, Finances, Intérieur) ainsi que ceux de l'Assemblée nationale et du Sénat aient acquis le réflexe d'inclure, au titre de la sensibilisation, le partage de l'expérience de la CNIL dans des coopérations, lors de visites effectuées en France où de conférences et séminaires organisés à l'étranger. Ainsi, la CNIL a reçu pour des séances de travail des délégations ministérielles ou parlementaires du **Bénin** (fichiers du secteur de la sécurité), du **Liban** (questions droits de l'homme) et du **Vietnam** (administration électronique). Elle a animé **deux séminaires parlementaires** d'une semaine à **Madagascar** (protection des données et droit des nouvelles technologies). Enfin, la CNIL entend poursuivre les relations avec l'ensemble de ces pays avec le soutien des ambassades concernées.

Création d'une association regroupant les autorités indépendantes francophones

Le principe de créer une association a été acquis lors d'une rencontre de dix-sept autorités francophones, en présence du représentant du secrétaire général de l'OIF, organisée par l'autorité de **Monaco** en septembre 2006. L'objectif principal est double : offrir aux autorités nouvellement installées une structure d'accueil et d'échanges, constituer un pôle d'expertise pour les pays non encore dotés d'une législation. L'association sera lancée lors de la **première conférence francophone sur le droit de la protection des données**, qui se tiendra à Montréal le 24 septembre 2007, organisée par l'autorité indépendante du **Québec.** Y seront conviés des représentants de tous les États membres ou observateurs de la Francophonie.

Élaboration d'un canevas législatif

En réponse à la demande de certains États de disposer d'un canevas législatif, et en vue de soumettre à la discussion un canevas francophone, les services de la CNIL ont élaboré un texte. Sa rédaction a été guidée par trois objectifs : favoriser le rapprochement des législations comme facteur contribuant à l'effectivité du droit sur le plan transfrontalier, lisibilité et flexibilité dans les méthodes de mise en œuvre.

À gauche, M. Vu Dinh Thuan, vice-ministre, Office du gouvernement du Vietnam, et AlexTürk, Sénat, 8 février 2006.

CENTRES D'APPELS DÉLOCALISÉS : COMMENT ASSURER LA PROTECTION DES DONNÉES ?

L'activité des centres d'appels est en plein développement et se situe à deux niveaux. Ils peuvent servir de point de contact avec les clients qui appellent afin d'obtenir une aide technique dite *hotline*, une commande de biens ou de services, ou encore une simple information. Par ailleurs, ils peuvent être utilisés par l'entreprise dans le cadre de son activité de prospection par exemple sur de nouveaux produits et services. Dans les deux cas, des traitements de données personnelles sont mis en œuvre et doivent donc respecter les règles de protection des données.

La Commission a donc décidé la mise en place d'un groupe de travail sur la problématique de la délocalisation de ces centres d'appels ainsi que de façon plus générale de l'externalisation informatique.

En effet, avec la baisse du coût des communications, la CNIL constate que les entreprises, les sociétés de service… et même l'État recourent de plus en plus à l'externalisation, hors Union européenne, de leurs moyens informatiques, en particulier dans des pays qui, le plus souvent, ne disposent pas de législation protectrice des données personnelles. Se pose alors 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.

Si les dossiers examinés par la CNIL sont évidemment très loin de refléter la réalité des échanges effectués, la Commission souhaite en effet sensibiliser l'ensemble des acteurs concernés au nécessaire respect de la loi. Elle a ainsi eu l'occasion de rappeler les conditions dans lesquelles doivent s'opérer de tels transferts pour être en conformité avec la loi. En effet, les entreprises qui font réaliser, hors Union européenne, des traitements de données doivent garantir un niveau de protection de ces données suffisant, soit en faisant adopter dans les contrats des clauses de protection des données conformes aux clauses types européennes soit en recourant à des règles internes contraignantes (préalablement soumises aux autorités de protection des données). Au-delà se pose la question de l'information des clients, des salariés… dont les données sont ainsi traitées dans des pays tiers et aussi des mesures prises pour assurer en local la formation des personnels et la sécurité des données.

De façon plus globale sur le plan international, les actions que mène actuellement la CNIL, en concertation avec ses homologues, tendent à montrer l'intérêt pour les pays tiers de se doter d'une loi spécifique de protection des données. Le développement des NTIC couplé à la convergence téléphone/Internet constitue un enjeu majeur du développement économique des pays notamment émergents et tant les gouvernements que les acteurs économiques des pays concernés doivent être conscients de la nécessité d'accompagner ce développement des règles de protection des données qui en sont le corollaire indispensable.

Le groupe de travail fera part de ses propositions à la fin de l'année 2007.

LES PRINCIPAUX DÉCRETS D'APPLICATION DEVANT ÊTRE SOUMIS POUR AVIS À LA CNIL EN 2007

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

* Création d'un traitement automatisé de données à caractère personnel des ressortissants étrangers (FNAD).

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

* Liste des traitements automatisés intéressant la sûreté de l'État, la défense, la sécurité publique.

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

Décrets d'application de la loi 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.

Décrets d'application de la loi relative à la prévention de la délinquance :

* Conditions dans lesquelles les candidats au service volontaire citoyen de la police nationale sont informés de la consultation des traitements automatisés mentionnés aux articles 21 et 23 de la présente loi.

* Dans le cadre du recensement prévu afin d'améliorer le suivi de l'obligation d'assiduité scolaire un décret précisera la liste des données à caractère personnel collectées, la durée de conservation de ces données, les modalités d'habilitation des destinataires ainsi que les conditions dans lesquelles les personnes intéressées peuvent exercer leur droit d'accès.

Décrets d'application de la loi relative à l'accès au crédit des personnes présentant un risque aggravé de santé :

* « À défaut d'accord, ou en cas de dénonciation, compromettant la mise en œuvre ou la pérennité du dispositif conventionnel, les conditions de collecte et d'utilisation et les garanties de confidentialité des données à caractère personnel de nature médicale sont fixées dans les six mois par décret en Conseil d'État, après avis de la Commission nationale de l'informatique et des libertés. »

Décrets d'application de la loi portant réforme des successions et des libéralités :

* Possibilité de création de traitements de données à caractère personnel permettant au GIE d'accomplir ses missions (notamment l'identification des propriétaires de biens fonciers et immobiliers en Corse).

Décrets d'application de la loi ratifiant l'ordonnance no 2005-1040 du 26 août 2005 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 et modifiant le code de la santé publique :

* Modalités d'élection par voie électronique.

* Choix de l'identifiant de santé ainsi que ses modalités d'utilisation.

Décrets d'application de l'ordonnance relative à la partie législative du code du sport :

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

Décrets d'application de la loi 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.

Décrets d'application de la loi portant engagement national pour le logement :

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

LA CNIL ET LES POUVOIRS PUBLICS

LA CNIL CONSULTÉE PAR LES PARLEMENTAIRES

Une première : la CNIL consultée sur une proposition de loi relative à la domiciliation

Si l'article 11 de la loi informatique et libertés prévoit que la CNIL est « *consultée sur tout projet de loi ou de décret relatif à la protection des données à l'égard des traitements automatisés* », cette disposition ne concerne pas les propositions de loi pouvant avoir un impact en cette matière.

Cet état du droit n'a pas empêché un député et un sénateur de saisir la Commission « pour avis », pour la première fois de son histoire, des dispositions d'une proposition de loi relative à la déclaration domiciliaire et déposée en termes identiques devant l'Assemblée nationale et le Sénat.

Ce texte, qui a donné lieu à de nombreux échanges et à deux réunions de travail avec ses auteurs, a également fait l'objet, au mois d'octobre, d'un débat en séance plénière de la Commission, qui s'est félicitée d'avoir été associée en amont à ces travaux parlementaires.

Questions à …

JEAN-MARIE COTTERET

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

Quelle est la raison d'être de cette proposition de loi ?

Ses auteurs, qui sont également élus locaux, soulignent les problèmes pratiques des maires pour – simplement – savoir qui sont leurs administrés et donc prendre en compte leurs besoins en termes d'infrastructures ou de services municipaux. Cette difficulté s'est accrue avec l'accélération des transferts de compétences dus à la décentralisation.

Pour y remédier, ces parlementaires proposent d'instituer une déclaration domiciliaire obligatoire et de faire du récépissé de cette déclaration l'unique justificatif de domicile. Prenant en compte les besoins des maires, la Commission a considéré qu'il était envisageable de faire du récépissé de cette déclaration un justificatif de domicile parmi d'autres, quand il est exigé.

Quelle est l'opinion de la CNIL sur ce sujet ?

Si le choix de la déclaration domiciliaire obligatoire a été fait par plusieurs États européens, l'établissement ou le changement de domicile n'est aujourd'hui, en France, soumis à aucune obligation déclarative – si l'on excepte le cas des étrangers devant être porteurs d'un titre de séjour et celui des trois départements d'Alsace-Moselle.

La Commission a souhaité définir les conditions dans lesquelles pourrait être mise en œuvre cette déclaration domiciliaire au regard des règles de protection des données.

Comment répondre au besoin légitime d'information des maires ?

L'instauration d'une obligation domiciliaire ne peut être envisagée comme la réponse unique à des problèmes très divers : certains nécessitent en effet une appréhension statistique globale de la population communale, d'autres une vision exacte de la composition des foyers, d'autres enfin une connaissance personnalisée des éléments d'identification et d'adresse de chaque administré.

Les maires ont déjà accès à un grand nombre de fichiers (fichiers de gestion communale, listes électorales, fichiers de communication, etc.) et de sources d'informations extérieures (listes des demandeurs d'emplois transmises par l'ANPE, informations statistiques fournies par l'INSEE, etc.). Dans la plupart des cas, leur bonne utilisation leur suffit à s'acquitter de leurs missions.

Il n'en demeure pas moins vrai, cependant, que les délais de transmission de certaines données, notamment les informations statistiques globales, pourraient être améliorés et que l'instauration d'une déclaration domiciliaire facultative pourrait, dans certains cas (inscription sur les listes électorales, recensement des jeunes en vue de la journée d'appel de préparation à la défense, redevance d'enlèvement des ordures ménagères…), permettre de solliciter les intéressés afin qu'ils s'acquittent de leur obligation, déclarative ou d'inscription.

En tout état de cause, la CNIL sera attentive au déroulement des travaux parlementaires concernant ce texte.

LES PROPOSITIONS DE LA CNIL AUX POUVOIRS PUBLICS

Étendre le principe du consentement préalable aux opérations de prospection politique

La Commission a été saisie au cours des années 2005 et 2006 de près d'une centaine de plaintes concernant l'utilisation de courriers électroniques à des fins de communication politique. En prévision des échéances électorales de 2007 et 2008, la Commission a adopté le 5 octobre 2006 une recommandation sur l'utilisation des fichiers par les partis politiques, notamment dans le cadre d'opérations de prospection.

Sur ce dernier point, la recommandation de la CNIL aborde la question de l'utilisation des moyens de prospection par voie électronique (courrier électronique, télécopieur et automates d'appel).

Si la loi sur la confiance dans l'économie numérique (LCEN) du 21 juin 2004 pose le principe selon lequel une opération de prospection directe, entendue au sens de commercial, est soumise au consentement préalable des personnes, le régime juridique applicable aux opérations de prospection à des fins politiques n'est, quant à lui, pas envisagé dans la LCEN.

L'importance de cette question, au regard des droits et libertés en cause, a conduit la Commission à attirer l'attention du Gouvernement sur la nécessité de trancher explicitement la question du régime juridique applicable aux opérations de prospection politique par voie électronique en étendant le principe du consentement préalable prévu par la loi aux opérations de prospection politique. On doit relever que le ministre de l'Intérieur a, dans un courrier adressé à la Commission en date du 12 décembre 2006, approuvé la position de la Commission en précisant toutefois qu'une telle modification législative ne devrait pas pouvoir intervenir avant le second semestre 2007.

Adopter une disposition législative pour anonymiser les décisions de justice diffusées sur Internet

La modification de la loi informatique et libertés par la loi du 6 août 2004 a conduit la CNIL à dresser un bilan de l'application de sa recommandation du 29 novembre 2001 relative à la diffusion de données personnelles sur Internet par les banques de données de jurisprudence.

Dans le cadre de ses travaux, la Commission a relevé la modification de la loi du 17 juillet 1978 par l'ordonnance du 6 juin 2005 qui a posé le principe général de l'anonymisation des documents publics avant leur réutilisation. Si le régime juridique défini par la loi du 17 juillet 1978 modifiée n'est pas applicable aux décisions de justice – ces dernières ne constituant pas des documents administratifs au sens de cette loi – le principe de l'anonymisation dans le cadre de la réutilisation d'informations publiques devrait, à tout le moins, s'appliquer aux bases de données jurisprudentielles qui contiennent des informations d'une nature particulière au regard de la protection de la vie privée des personnes concernées.

Ainsi, la Commission a estimé que les risques liés à la diffusion de bases de données de décisions de justice commandent l'adoption d'une disposition législative spécifique prévoyant l'anonymisation de celles-ci lors de leur diffusion par des moyens électroniques et, comme le lui permet l'article 114° b) de la loi du 6 janvier 1978 modifiée, a appelé l'attention du Gouvernement sur ce point.

Améliorer le fonctionnement du casier judiciaire

À l'issue des réflexions conduites par le groupe de travail constitué en son sein pour évaluer les difficultés de fonctionnement du casier judiciaire, la CNIL a formulé un certain nombre de propositions qu'elle a adressées au ministère de la Justice et au ministère de l'Intérieur au tout début de l'année 2007.

La Commission a ainsi proposé :

– qu'une réflexion soit menée afin que les contenus des extraits de casier judiciaire destinés respectivement aux juridictions et aux autorités administratives soient redéfinis. Par exemple, certaines condamnations figurant dans le bulletin destiné aux juridictions pourraient également être mentionnées dans celui destiné à l'administration afin de lui permettre d'accéder à des données complémentaires pour les enquêtes administratives relatives aux demandes d'agrément pour l'exercice de certains emplois. En effet, la CNIL a pu constater que, du fait de l'absence d'inscription des condamnations concernant les mineurs dans l'extrait de casier judiciaire dont elle peut avoir communication, l'autorité administrative se tourne vers les fichiers de police pour connaître les procédures en cours engagées à l'encontre des mineurs ;

– que les moyens des greffes correctionnels soient renforcés. Au cours de ses travaux, la CNIL a pu constater que le manque de moyens des greffes correctionnels avait des conséquences directes d'une part, sur la longueur des délais d'alimentation du casier judiciaire et d'autre part, sur l'insuffisance de la mise à jour des fichiers de police judiciaire ;

– que des mesures soient prises afin de mieux encadrer la consultation des fichiers de police judiciaire à des fins administratives. Il s'agirait de :

1. limiter dans le temps la possibilité de consulter ces fichiers en fonction de la nature de l'infraction ;

2. ajouter dans les cas d'effacement ou de mise à jour des fichiers de police judiciaire les classements en opportunité, le rappel à la loi et la composition pénale ;

3. rappeler aux préfets chargés de délivrer les agréments aux candidats à l'embauche dans le secteur du gardiennage et de la sécurité, la nécessité d'apprécier la situation de l'intéressé en fonction, notamment, de la nature de l'infraction et du type de poste occupé.

– que l'information des personnes concernées par les fichiers de police judiciaire, victimes et mises en cause soit renforcée. Ainsi, ces personnes devraient être avisées non seulement des conditions d'exercice de leur droit d'accès auprès de la CNIL, mais aussi de leur droit de s'adresser au procureur de la République territorialement compétent pour solliciter la mise à jour des informations les concernant. À cet égard, la CNIL rappelle que dans son avis rendu le 8 septembre 2005, elle avait déjà exprimé le souhait que toutes dispositions soient prises pour que les personnes concernées par les fichiers de police judiciaire soient clairement et précisément informées des conditions d'exercice de leur droit d'accès et de leur droit de demander, le cas échéant, que la qualification judiciaire des faits soit substituée à la qualification initiale telle qu'elle est enregistrée dans le fichier STIC.

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 restreinte chargée de prononcer des sanctions. Il a été élu vice-président du G29 en avril 2007.

Vice-président délégué

Guy ROSIER, conseiller maître honoraire à la Cour des comptes

Secteur : Affaires économiques

Membre de la CNIL depuis janvier 1999, Guy Rosier a été élu vice-président le 26 février 2004, puis vice-président délégué le 5 octobre 2004. Membre de droit de la formation restreinte.

Vice-président

François GIQUEL, conseiller maître honoraire à la Cour des comptes

Secteur : Sécurité

Membre de la CNIL depuis février 1999, François Giquel a été élu vice-président le 5 octobre 2004. Membre de droit de la formation restreinte.

Les membres (commissaires)

Hubert BOUCHET, membre du Conseil économique et social

Secteur : Travail

Hubert Bouchet est membre de la CNIL depuis novembre 1990, il a été vice-président délégué de février 1999 à août 2004. Il est membre élu de la formation restreinte.

Jean-Marie COTTERET, professeur émérite des universités

Secteurs : Collectivités locales, audiovisuel

Jean-Marie Cotteret est membre de la CNIL depuis janvier 2004.

Anne DEBET, professeur des universités

Secteur : Affaires sociales

Anne Debet est membre de la CNIL depuis janvier 2004. Elle est membre élu de la formation restreinte.

Emmanuel de GIVRY, conseiller à la Cour de cassation

Secteur : Gestion des risques et des droits

Emmanuel de Givry est membre de la CNIL depuis février 2004.

Georges de LA LOYÈRE, membre du Conseil économique et social

Secteur : Affaires internationales

Georges de La Loyère est membre de la CNIL depuis octobre 2004. Il est le représentant de la CNIL au sein du groupe de l'article 29 et des autorités de contrôle Europol et Schengen dont il est vice-président.

Francis DELATTRE, député du Val-d'Oise

Secteur : Affaires culturelles

Francis Delattre est membre de la CNIL depuis août 2002.

Patrick DELNATTE, député du Nord

Secteur : Justice

Patrick Delnatte est membre de la CNIL depuis août 2002.

Jean-Pierre de LONGEVIALLE, conseiller d'État honoraire

Secteur : Santé

Jean-Pierre de Longevialle est membre de la CNIL depuis décembre 2000.

Isabelle FALQUE-PIERROTIN, conseiller d'État, présidente du Conseil d'orientation et déléguée générale du Forum des droits sur l'Internet

Secteur : Libertés publiques

Isabelle Falque-Pierrotin est membre de la CNIL depuis janvier 2004. Elle y préside le groupe de travail sur l'administration électronique.

Didier GASSE, conseiller maître à la Cour des comptes

Secteur : Télécommunications et réseaux

Didier Gasse est membre de la CNIL depuis janvier 1999. Il est le représentant de la France au sein de l'autorité de contrôle Eurojust.

Philippe LEMOINE, président-directeur général de LaSer

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 restreinte.

Commissaires du gouvernement

Pascale COMPAGNIE

Catherine POZZO DI BORGO, adjointe

LES SERVICES AU 1er JUIN 2007

Président
Alex TÜRK
Secrétaire général
Yann PADOVA

SERVICE DE L'INFORMATION ET DE LA DOCUMENTATION
Chef de service
Edmée MOREAU
Information et documentation juridiques
Pascal PALUT
Sites web et intranet
Anne-Sophie JACQUOT
Louis RAMIREZ
Bibliothèque et documentation générale
N.

SERVICE DE LA COMMUNICATION EXTERNE ET INTERNE
Chef de service
Elsa TROCHET-MACÉ
Assistante Brigitte BARBARANT

DIRECTION DES AFFAIRES JURIDIQUES, INTERNATIONALES ET DE L'EXPERTISE	
Directeur : Sophie VULLIET-TAVERNIER	
Directeur adjoint : Sophie NERBONNE	
Assistance et secrétariat : Audrey BACQUIÉ	Chargé de mission : Clémentine VOISARD

SERVICE DE L'EXPERTISE INFORMATIQUE
Chef de service
Gwendal LE GRAND
Ingénieur expert en technologies de l'information
Thierry CARDONA
N.

SERVICE DES AFFAIRES JURIDIQUES
Chef de service
N.
Police-Défense-Affaires étrangères-Libertés publiques–Collectivités territoriales- Finances publiques- Administration électronique
Olivier LESOBRE Guillaume DELAFOSSE Valérie BEL N.
Travail-Santé-Social-Affaires culturelles
Daniéla PARROT Frédérique LESAULNIER Leslie BASSE Laurent LIM N.
Affaires économiques-Banque—Assurances- Commerce- Communications électroniques
Olivier COUTOR Vanessa YOUNES-FELLOUS Leslie BASSE Mathias MOULIN Johanna CARVAIS
Assistance et secrétariat
Barbara BAVOIL Nathalie DESMARAIS Valérie DISCA Brigitte HUGER Catherine MANDINAUD Eugénie MARQUES Brigitte SAGOT

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

Conseiller du Président pour la prospective et le développement
Marie GEORGES

Chargé de mission auprès du secrétaire général, questions budgétaires et financières
Patrick RIGAL

Secrétariat de la présidence et du secrétariat général
Odile BOURRE, chef du secrétariat
Halima GOUASMIA, Céline CORNE

DIRECTION DES RELATIONS AVEC LES USAGERS ET DU CONTRÔLE
Directeur : Florence FOURETS
Directeur adjoint : Jeanne BOSSI
Assistance et secrétariat : N.

DIRECTION DES RESSOURCES HUMAINES, FINANCIÈRES ET INFORMATIQUES
Directeur : Thierry JARLET
Adjoint au directeur, chef du service financier et logistique : David TRIVIÉ
Secrétariat de la direction : N.

Service des contrôles
Chef de service
N.
Auditeur Thomas DAUTIEU
Informaticiens contrôleurs
Julien DROCHON Michel GUEDRE Bernard LAUNOIS Judicaël PHAN
Assistance et Secrétariat
Nathalie JACQUES

Cellule Droit d'Accès Indirect
Responsable
Bérengère MONEGIER DU SORBIER
Assistance et secrétariat
Bertrande PIAT-TAMBAREAU N.

Service des plaintes
Chef de service
Norbert FORT
Banque-Crédit- Associations-Partis politiques-Libertés publiques
Xavier DELPORTE Michèle SAISI
Travail-Social-Sécurité sociale- Éducation nationale-Santé-Fiscal
Caroline PARROT-FRANCIS
Marketing- Assurances-Télécommunications-Internet-Logement
Odile JAMI
Assistance et Secrétariat
Anna BENISTI Véronique BREMOND Siré BARRY

Cellule Sanctions
Responsable
Guillaume DESGENS-PASANAU N.
Assistance et secrétariat
N.

Service d'orientation et de renseignement du public
Chef de service
Emilie PASSEMARD
Chargée d'études Fatima HAMDI
Responsable courrier Evelyne LE CAM
Téléconseillers
Françoise PARGOUD Véronique JENNEQUIN Wafae EL BOUJEMAOUI Merwann BENSIALI
Téléopératrices
Noëlle CHAUMETTE Malika KHELLAF Delphine LAUNOIS
Gestion informatique des formalités préalables
Responsable
Mireille LACAN
Opératrices de saisie
Sonia CUSTOS Carole GUIBOUT-CHATELAIN

Cellule Correspondants
Responsable
Inès ROGIC
Hervé GUDIN
Assistance et secrétariat
N.

Service des ressources humaines
Chef de service
Jean-Marc FERNANDES
Responsable gestion administrative Liliane RAMBERT
Secrétariat Anastasia TANFIN

Service financier et logistique
Chef de service
David TRIVIÉ
Comptabilité Sébastien BOILEAU Clarisse REB
Secrétariat voyages Véronique FOUILLET Coordonnateur Pierre RIHOUAY Huissiers Jérôme BROSSARD Akram KOUBAA Mickaël MERI Conducteurs Alain HOUDIN Joël LEPAGE Patrick MAHOUDEAU Entretien Félisa RODRIGUEZ

service de l'informatique interne
Chef de service
Hervé BRASSART
Informatique
Gilbert BENICHOU, ingénieur
Thierry CARDONA, ingénieur
Philippe MIMIETTE, administrateur réseaux
Sébastien BÉNARD, technicien développeur
Giuseppe GIARMANA, technicien bureautique et téléphonie

RÉFLEXIONS PROPOSÉES PAR ALEX TÜRK, président de la CNIL, à la conférence internationale des commissaires à la protection des données de Londres, novembre 2006.

Dans un peu moins de deux ans, nous allons fêter le 30e anniversaire de notre conférence internationale des commissaires à la protection des données. Si vous nous donnez votre accord, l'Allemagne et la France auront le grand plaisir de vous accueillir à Strasbourg puisqu'elles fêteront le même jour le 30e anniversaire de leurs lois fondamentales et de la création des autorités allemandes de protection des données personnelles et de la Commission nationale de l'informatique et des libertés.

Trente ans pour des institutions telles que les nôtres, est-ce vieux ? Est-ce jeune ? Disposons-nous du recul suffisant pour apprécier l'efficacité de notre action ? En vérité, le sens de la réponse à ces questions dépend moins du temps écoulé que de la succession des événements survenus durant cette période. Quels éléments communs entre l'activité de nos autorités de contrôle au début des années 1980 et celle que nous menons aujourd'hui ? Il n'est pas nécessaire d'être un expert pour désigner les facteurs déterminants de cette véritable révolution que nous connaissons depuis le début des années 1990 : Internet, téléphone portable, biométrie, puces RFID, Wi-Fi, nanotechnologies, etc.

Nous sommes ainsi confrontés à une **immense vague technologique** qui bouleverse, sur son passage, nos traditions juridiques, l'application de nos concepts et, pour finir, les grandes certitudes que nous pouvions encore entretenir, nous, autorités de protection des données, sur l'effectivité de notre action. Et voici que, peu après la tragédie du 11 septembre et des autres attentats terroristes survenus par la suite, est apparue une seconde vague que l'on pourrait qualifier de « **sécuritaire** » et qui a déclenché, depuis cinq ans, un mouvement profond, au sein des pouvoirs publics de nombreux États en faveur d'un accroissement des moyens d'action en matière de **lutte antiterroriste**.

Bien entendu, il ne s'agit, en aucune manière, de contester le bien-fondé même de ces politiques qui répondent aux attentes de nos concitoyens. Et d'ailleurs, ces dernières années, nos autorités de contrôle ont réagi avec un **grand sens de leurs responsabilités** aux différentes mesures antiterroristes prises par les autorités publiques. Mais cette **vague « sécuritaire », normative** cette fois, qui s'est traduite par la création ou l'extension de nombreux fichiers et la mise en place, au profit des autorités de police, de nouveaux moyens d'investigation dans les systèmes d'information, pourrait bien submerger nos autorités.

La philosophie même qui sous-tend l'existence de celles-ci est, en effet, mise en cause par la conjonction de ces deux vagues. Et l'on éprouve, souvent, un sentiment d'incompréhension lorsque l'on constate que nos autorités de contrôle, faute de moyens suffisants, ne peuvent accomplir correctement toutes leurs missions, piétinent face à l'émergence des nouvelles problématiques de protection des données, et se sentent parfois impuissantes face au déferlement de ces vagues alors qu'on attendrait de leur part, tout au contraire, un positionnement fort et un interventionnisme accru.

Dès lors, **une prise de conscience collective est nécessaire et urgente** si nous ne voulons pas faillir à notre mission.

Nous devons d'abord faire preuve de lucidité et tenter d'analyser les ressorts de ces deux vagues, à la fois technologique et normative, qui défient nos organisations. Il nous faut aussi, ensemble, proposer des réformes, des

stratégies coordonnées pour agir autrement, mieux, plus vite, plus fortement. Enfin, il nous faut déterminer les voies qui nous permettront d'accéder à une autre dimension, de façon à retrouver la place qui doit être la nôtre au service de la protection des données personnelles.

Prenons garde ! À défaut d'initiative de notre part, on pourra, un jour, dire de nous : « *La civilisation était en train de changer sous leurs yeux et ils n'ont rien vu venir ; un nouveau droit fondamental des hommes et des femmes vivant dans les sociétés modernes était en train d'être reconnu par les textes et ils n'ont rien fait pour le protéger.* »

I – DEUX VAGUES, UN TRIPLE DÉFI

A – La « vague technologique »

Il est impossible de formuler des solutions éventuelles à ces questions si on ne prend pas la peine de s'attacher à définir et à circonscrire les caractéristiques inhérentes au progrès technologique dans le domaine de la protection des données personnelles.

1 – Le facteur « accélération »

Phénomène bien connu, le progrès technologique s'avance en accélérant sans cesse. Les délais entre la découverte d'un phénomène et sa mise en œuvre technologique se raccourcissent et le temps de passage d'une innovation à une autre innovation, du développement d'un prototype à son déploiement industriel, se réduit sans cesse.

Ainsi, en 10 ans, Internet est devenu omniprésent : près d'un milliard d'internautes, soit 14,6 % de la population mondiale l'utilisent aujourd'hui [1]. Si l'accès à haut débit représente une première étape dans l'accélération de son usage, la deuxième étape, son accès depuis les mobiles, devrait rendre son usage rapidement incontournable.

Et il ne se sera écoulé que trois ans entre le moment où la technologie RFID a pu être développée à un stade industriel et celui où elle a été intégrée dans les documents de voyage, dans des cartes de paiement, des cartes d'accès, etc., et la réduction continue du coût de puces et des lecteurs assure la pérennité de ce développement.

Il est d'ores et déjà prévisible que l'impact des nanotechnologies, qui seront une réalité industrielle massive à échéance 2015, se manifestera encore plus rapidement que celui des RFID. Et on sait que, avec les nanotechnologies, les performances des futurs « ordinateurs quantiques » pourraient être plus élevées d'un facteur 10^9 (dix milliards de fois plus puissant) par rapport aux ordinateurs actuels. Ces chiffres vertigineux laissent imaginer l'ampleur de l'accélération technologique à venir.

Or le temps juridique est lui-même particulièrement lent à la fois parce que les normes et les concepts s'élaborent dans le respect des procédures démocratiques et parce que les enjeux sont de plus en plus complexes.

2 – Le facteur « globalisation »

Autre caractéristique du progrès technologique : ses effets sont marqués par une propension à s'universaliser, à se globaliser. Dans notre domaine, cela se traduit, bien sûr, par le formidable essor des délocalisations de traitements de données : l'émergence dans des pays jusqu'alors peu impliqués dans le traitement de l'information, d'activités de développement logiciel, de sous-traitance et de maintenance à distance. Évoquons également la maîtrise, par les États-Unis, des modes de traitement et d'organisation de l'information (systèmes d'exploitation, logiciels, outils de recherche…). De même, il est inutile d'insister sur les problématiques transfrontières qui s'attachent à ces phénomènes. Or notre droit, nos droits sont, par essence, étroits parce qu'ils s'inscrivent dans le cadre de territoires et de champs de compétences ordonnés et balisés.

Quel constat en tirer pour la protection des données ? Face à des pays où le concept de protection des données est encore peu connu, sinon ignoré du système juridique, les instruments mis en place pour « contrôler » les flux transfrontières de données apparaissent à la fois bien dérisoires et peu compréhensibles.

Nous sommes bien évidemment, aujourd'hui, dans l'incapacité de contrôler, sur le plan international, les échanges de données. Il faut sans doute avoir le courage de reconnaître que nos règles de protection des données sont, en ce domaine, très largement inadaptées et que, de la même façon que l'informatique est aujourd'hui par nature communicante et sans frontières, la protection des données ne peut se concevoir que dans une dimension mondiale. Ceci suppose assurément d'élaborer, sur le plan international, un instrument juridique nouveau. Surtout, il nous faut, en amont, réfléchir à une adaptation (et non à une remise en cause) de nos concepts de base pour assurer une meilleure compréhension de ceux-ci (ainsi, la notion de donnée à caractère personnel, le concept de droit d'accès, etc.).

3 – Le facteur « ambivalence »

Toutes les réflexions menées dans le domaine de la philosophie du droit dans nos pays respectifs l'ont montré : il est vain de vouloir dissocier, parmi les effets du progrès technique, les aspects positifs et négatifs. Toute innovation technologique porte en elle « le bien et le mal » et renvoie

1. Sources : World Internet Statistics citées dans HS du *Monde* « Bilan du monde 2005 » paru en 2006.

aux usages que souhaitent en faire ses promoteurs [1] ou ceux à qui on remet le pouvoir de décision en la matière. Or le droit – c'est un élément intrinsèque à sa vocation – se doit d'être univoque et se trouve donc être bien souvent par nature, en inadéquation avec cette ambivalence du progrès technique.

La difficulté majeure vient de ce que, aujourd'hui, l'informatique est devenue une informatique de « confort » indispensable dans tous les actes de la vie quotidienne (pour se contacter, se localiser, s'informer, se sécuriser…). Mais nos concitoyens se préoccupent-ils de la traçabilité et de la surveillance potentielle de leurs déplacements, de leurs comportements, de leurs relations ? L'individu est-il pleinement conscient de cette ambivalence de la technique ? Force est de constater le peu de réactions de nos concitoyens vis-à-vis de ces questions. À qui la faute ? N'avons-nous pas notre part de responsabilité dans ce manque de vigilance citoyenne ?

4 – Le facteur « imprévisibilité »

Largement lié à la conjonction des trois caractéristiques précédentes, le développement parfois imprévisible de certains usages de l'outil informatique crée des situations de porte-à-faux pour ceux qui sont en charge de l'élaboration des normes et rend l'exercice de nos missions malaisé. C'est l'exemple du téléphone portable, qui aurait pu ne rester qu'un simple outil de communication, mais qui est également devenu un moyen de paiement et un outil de traçage et de géolocalisation des utilisateurs. De même, Internet, simple instrument d'information et de communication, peut se transformer en un redoutable système d'espionnage par le biais d'applications comme Google Earth, par exemple. Pouvait-on prévoir que l'on pourrait être identifié à distance par son passeport ou encore que l'on pourrait rechercher un passé judiciaire sur Internet « grâce » aux formidables capacités d'investigation dans la vie privée qu'offrent aujourd'hui les moteurs de recherche ?

5 – Le facteur « invisibilité » (invisibilité virtuelle/invisibilité physique ou réelle)

On est loin aujourd'hui du gros calculateur trônant dans « la » salle informatique… Le traitement de l'information est de plus en plus « invisible », impalpable, de moins en moins maîtrisable, que ce soit par les individus ou par nos autorités.

Ce facteur « invisibilité » est double :
– d'une part, la technologie tend à devenir invisible du fait du développement des traitements de données virtuelles réalisés à l'insu des personnes (c'est l'invisibilité virtuelle, liée aux processus) ;
– d'autre part, la technologie tend à devenir invisible du fait de son extrême miniaturisation (c'est l'invisibilité physique ou réelle).

Le premier facteur d'invisibilité résulte de la multiplication des traitements qui, s'ils sont effectués par des technologies visibles physiquement, sont toutefois réalisés à l'insu des personnes, si bien qu'ils sont, en pratique, pour celles-ci, parfaitement invisibles. Ce sont ces traitements qui permettent de tracer les personnes de manière virtuelle : traçabilité de leurs déplacements physiques dans les transports en commun, de leurs consultations sur Internet, de leurs communications téléphoniques et électroniques, etc.

L'indifférence de nos concitoyens à l'égard des enjeux de protection des données, le manque sinon l'absence de perception qu'ils ont des risques d'atteinte à leurs libertés individuelles par l'usage de telle ou telle technologie tiennent aussi sans doute à cette invisibilité croissante du traitement de l'information, à ces traces informatiques – actives ou passives – que chacun laisse désormais derrière soi.

Le second facteur d'invisibilité réside, lui, dans l'extrême miniaturisation de la technologie elle-même. Les téléphones portables, les ordinateurs, les assistants personnels diminuent en taille et en poids chaque année. La taille des puces diminue, tandis que leur durée de vie s'allonge et que les capacités de mémoire et les puissances de traitement des ordinateurs se développent.

Mais **une autre vague technologique pointe à l'horizon 2015, celle des nanotechnologies**, dont on nous promet des applications déconcertantes dans le domaine des systèmes d'information. Avec les nanotechnologies, la difficulté ne consistera plus à avoir conscience de l'existence d'un traitement, visible par ailleurs. Il ne sera même plus question d'avoir ou non conscience de l'existence d'un traitement : il sera devenu impossible de voir à l'œil nu que la technologie est présente dans un objet !

Avec la tendance à la virtualisation des traitements, nos concepts menaçaient déjà de voler en éclat : comment définir le responsable du traitement et la finalité avec le *data mining*, le lieu du traitement avec le *peer-to-peer* ? Quel sens cela a-t-il de définir aujourd'hui une durée de conservation ?… Mais de manière encore plus préoccupante, l'évolution vers l'invisibilité réelle de la technologie elle-même pourrait aboutir, à échéance de quelques années, à placer notre droit et nos autorités de contrôle dans une situation d'impuissance puisqu'il leur reviendrait d'encadrer et de contrôler des traitements effectués par le recours à une technologie invisible…

---

1. *Cf.* les propos ambigus tenus par les deux fondateurs de Google, Larry Page et Sergey Brin : *« Notre mission est d'organiser l'information du monde et de la rendre accessible à tous. »*

6 – Le facteur « irréversibilité »

Les évolutions liées au progrès technologique sont par nature irréversibles[1]. Nous ne vivrons plus jamais dans un monde sans ordinateurs, sans Internet, sans téléphones portables, sans identification biométrique, sans géolocalisation, sans vidéosurveillance. Bien au contraire, ces technologies ont tendance à s'imbriquer les unes dans les autres. Outre les problèmes majeurs que pose cette caractéristique d'irréversibilité à nos systèmes juridiques, elle doit probablement constituer, en termes d'intérêt général, le facteur le plus dangereux. Nous aurons l'occasion d'y revenir plus longuement en conclusion.

B – Les politiques de sécurité : la vague normative

Il s'agit, cette fois, d'un défi socio-juridique qui nous est lancé par l'ensemble des nouvelles législations et réglementations produites en matière de lutte antiterroriste des deux côtés de l'Atlantique. Ces politiques liées aux nouvelles exigences de sécurité publique ont abouti à la mise en place d'un maillage en matière d'utilisation de fichiers informatiques susceptibles de constituer un **choc de civilisation**.

Si l'on prend l'exemple de la France, les événements du 11 septembre se sont traduits par un renforcement des mesures de sécurité intérieure et de maîtrise des flux migratoires, même si notre pays est déjà doté, depuis 1986, d'une législation antiterroriste[2]. Plusieurs lois sont ainsi intervenues, depuis 2001, pour étendre la consultation des fichiers de police en particulier à des fins administratives (pour le recrutement à des emplois de sécurité, les décisions de naturalisations, l'octroi des titres de séjours des étrangers…), pour élargir sensiblement les possibilités d'accès par les autorités judiciaires et les services de police aux fichiers informatiques privés (et en particulier à ceux des opérateurs de communications, des cybercafés, des fichiers des compagnies aériennes) ou encore pour prévoir la création de nouveaux fichiers de police (par exemple, le fichier de domiciliation des délinquants sexuels), l'extension de fichiers existants (comme le fichier des empreintes génétiques), le développement de la vidéosurveillance ou encore la mise en place en tous points appropriés du réseau routier et autoroutier de dispositifs fixes ou mobiles de lecture des plaques minéralogiques et de prise des photographies des occupants des véhicules.

Ces différentes mesures, qui s'inscrivent dans le prolongement de la politique de lutte antiterroriste, ont, bien entendu, eu un impact certain sur la protection des données personnelles et on sait que les mesures adoptées en France ont connu leurs équivalents dans les autres pays.

Au niveau européen, les politiques de lutte contre le terrorisme ont donné un coup d'accélération au développement des bases de données sur les visas et de la seconde version du Système d'information Schengen (SIS II), à la rétention des données de trafic, au contrôle des listes de passagers aériens, etc. Elles ont également conduit nos gouvernements, *via* l'OACI, à soutenir l'incorporation de données biométriques dans les passeports et les documents de voyage.

Aux États-Unis, ces mêmes politiques ont conduit à l'adoption emblématique du Patriot Act – une loi de 342 pages ! – ratifié seulement un mois et demi après les attentats du 11 septembre. Cette loi, comme les divers programmes de surveillance ultérieurement mis en place par l'administration Bush, accorde des pouvoirs considérables aux autorités administratives américaines pour saisir et intercepter des documents, des communications téléphoniques et électroniques, pour interconnecter des fichiers, tout en limitant l'intervention de l'autorité judiciaire et en autorisant l'exécutif à ne pas publier ces mesures.

En outre, dans tous nos pays, une tendance se crée qui consiste à utiliser des bases de données de sociétés privées à des fins de lutte contre le terrorisme. Les affaires PNR et SWIFT sont caractéristiques de cette tendance.

Confrontées à une telle situation, les autorités de contrôle en matière de protection des données doivent éviter les pièges, dénoncer les illusions et combattre les mythes.

1 – Le piège du manichéisme

L'ensemble des autorités de contrôle nationales en charge de la protection des données reconnaît, bien évidemment, **la légitimité des politiques de lutte antiterroriste** mises en place dans leurs États respectifs. Et les accusations d'irresponsabilité qui sont parfois portées à leur égard en la matière sont inacceptables.

Les autorités de contrôle se situent en dehors du champ politique. On ne peut les confondre ni avec certaines associations militantes qui professent des opinions très engagées ni avec les autorités publiques en charge de la sécurité ou de la justice. Il serait si facile de stigmatiser les comportements de ces autorités de contrôle si elles versaient d'un côté ou de l'autre !

Au contraire, elles examinent les textes de niveau législatif ou réglementaire en recourant aux principes et aux instruments que les textes fondateurs de chaque pays leur ont confiés. Quelle est la finalité poursuivie par tel traitement de données dans une politique de lutte antiterroriste ? Y a-t-il adéquation entre l'objectif poursuivi et les moyens

---

1. Si l'on exclut, bien entendu, l'hypothèse de catastrophes naturelles majeures aboutissant à des destructions globales auquel cas, d'ailleurs, les réflexions ici menées se verraient *ipso facto* dépourvues de tout intérêt…
2. La France s'était dotée d'une telle législation après une première vague d'attentats en 1986 (loi du 9 septembre 1986). Celle-ci avait été renforcée par une seconde série d'attentats en 1995.

mis en œuvre ? Quel est le champ de garanties prévues pour assurer la confidentialité et le respect des droits des personnes ?, etc. Et c'est très exactement ce qu'attendent d'elles les citoyens des pays concernés : il s'agit d'éclairer leur propre analyse avantages/inconvénients qui doit leur permettre de **mesurer à quelles limitations de leurs droits individuels ils sont prêts à consentir pour accroître le niveau de sécurité publique**, et donc leur propre sécurité.

Les autorités de contrôle sont rompues à ce genre d'exercice et elles ne doivent donc pas se laisser entraîner dans le piège du manichéisme – à condition que les gouvernants veuillent bien leur délivrer les informations nécessaires pour leur permettre de formuler leur appréciation en pleine connaissance de cause ! Or, force est de constater, qu'en ces domaines, certes politiquement très délicats, nos autorités de contrôle peuvent éprouver parfois le sentiment de ne pas disposer de la part des autorités concernées de tous les éléments de contexte utiles. On imagine les motifs pour lesquels les autorités gouvernementales de l'ensemble des États peuvent ainsi être enclines à retenir l'information.

2 – Le risque de l'engrenage

Si l'on prend l'exemple des politiques de sécurité (mais nous pourrions en dire autant dans le domaine de la justice, de la politique sociale ou de la santé), on constate que, en pratique, dans aucun pays on n'a procédé par la mise en œuvre d'une loi fondamentale, suivie aussitôt d'un ensemble de textes d'application. Compte tenu de la complexité et de la sensibilité de ces questions, il est compréhensible que les pouvoirs publics de nos pays puissent être contraints de recourir à la pratique du train des lois successives.

Mais parfois il s'agit, en réalité, d'une **véritable stratégie de contournement** à l'égard des autorités de protection des données. Peu importe d'ailleurs car, du point de vue du comportement qui doit être le nôtre, cela ne change rien. Dans tous les cas, nous sommes confrontés au risque de l'engrenage juridico-politique.

Ce risque est le suivant. L'autorité de contrôle est saisie d'un projet de loi portant création d'un nouveau traitement. Conformément aux principes fondamentaux de finalité et de proportionnalité, elle formule un avis qui repose sur un équilibre à un instant donné et en admet la pertinence. Mais quelque temps plus tard, on lui soumet un nouveau projet de loi qui élargit le champ du traitement ou accroît sa puissance. Les promoteurs de ce second texte font valoir que l'autorité de contrôle ayant déjà donné un accord de principe au premier texte, on voit mal comment elle pourrait s'opposer à une simple extension, et ainsi de suite si nécessaire…

Ajoutons que le problème est rendu encore plus aigu par le fait qu'en la matière, 1 + 1 peut faire 3 ! On veut dire par là que la conjugaison des dispositions des deux textes produits peut créer une synergie telle que les risques engendrés à l'égard de la protection des droits individuels se multiplient au lieu de s'ajouter seulement.

Ce phénomène est parfaitement illustré par le développement progressif, selon des processus identiques, des fichiers nationaux d'empreintes génétiques en France et en Grande-Bretagne. Dans les deux cas, ces fichiers ont été créés dans un but spécifique : centraliser les empreintes génétiques de criminels sexuels condamnés afin de faciliter leur identification en cas de récidive. Puis, on a augmenté le nombre des personnes concernées, pas forcément de façon concomitante, ni dans le même texte. Ensuite, c'est la nature des infractions prises en compte qui est étendue. Enfin, on diversifie les situations des personnes vis-à-vis de la procédure pénale : s'agit-il d'une personne accusée ou simplement mise en cause ? Est-ce une personne seulement suspectée ? Y a-t-il des indices graves *et* concordants ? Ou s'agit-il d'indices graves *ou* concordants ? C'est ainsi qu'en quelques années, on est passé d'un fichier spécifique dédié à la prévention de la récidive des délinquants sexuels à un instrument général d'investigation au service de l'élucidation de quasiment toutes les affaires par la police judiciaire.

Comment réagir face à ce type d'engrenage législatif ? Question délicate surtout si l'on rappelle qu'elle se pose sur la toile de fond de l'irréversibilité des phénomènes décrits plus haut.

3 – L'illusion de « l'exemplarité »

Il s'agit là d'un autre risque qui présente quelques analogies avec le précédent mais qui concerne peut-être plus particulièrement les pays membres de l'Union européenne, représentant à eux seuls la moitié des États dans le monde disposant d'une autorité de contrôle et d'une loi de protection des données.

Par exemple, de nombreux pays en Europe disposent de fichiers nationaux de population et font usage d'un seul numéro d'identification, d'autres pays, tels que la France, ont fait des choix différents. Tel pays développe puissamment un système de traitement des empreintes génétiques qui devient une « référence » pour d'autres exécutifs. Tel autre développe de manière très significative le recours à la biométrie ou à la vidéosurveillance.

Or, les exécutifs nationaux, prenant appui sur ces exemples étrangers, ont bien souvent tendance à utiliser l'argument analogique suivant : « *Comment vous, autorité de contrôle, pouvez-vous vous opposer à tel ou tel développement de traitement alors que cela a été accepté dans tel autre pays ?* » On devine alors les problèmes d'harmonisation que cela pose et, en tout état de cause, on mesure à quel point il est **nécessaire de recourir à des raisonnements fondés sur la définition de dénominateurs communs**.

4 – Le mirage du fichier « remède miracle »

Nos autorités doivent ensuite se battre contre le mirage du « fichier, remède miracle ». On dit parfois que lorsque l'autorité publique est confrontée à un problème, elle crée une commission. Désormais, à cette propension s'ajoute un nouveau réflexe : la création d'un fichier !

Or nos autorités savent pertinemment que la création d'un fichier informatique ne règle pas tout. Il nous revient de **désacraliser le caractère supposé infaillible du fichier informatique**.

Combien de fois d'ailleurs nous sommes-nous prononcés sur des fichiers, supposés régler un problème, qui n'auront finalement jamais vu le jour ? Ainsi, en France, le législateur a prévu, en 1997, l'obligation de relever et de traiter les empreintes digitales des ressortissants sollicitant un titre de séjour en France. Près de dix ans après, ce fichier n'a toujours pas vu le jour ! Cela n'a pas empêché le législateur de modifier la loi pour étendre cette obligation aux demandeurs de visas, pour lesquels des expérimentations sont en cours. La réglementation européenne aura ici, sans aucun doute, contribué à l'accélération du processus.

Parfois également nos autorités se prononcent sur la création d'un fichier tout en sachant que celui-ci a des chances de ne pas être la réponse adaptée au problème que l'on cherche à régler. Ainsi, les exigences de transmission par les compagnies aériennes des données des passagers aux autorités américaines et les diverses mesures prises pour contrôler le déplacement des personnes ne sont-elles pas parfois disproportionnées, quand on sait que les mouvements terroristes ont désormais tendance à recruter en « local » et à user de moyens de déplacement plus discrets que l'avion… ?

Un dernier exemple illustrera encore de manière emblématique cette course, toujours inachevée, entre la création d'un nouveau fichier, son effet escompté en termes de sécurité et l'imprévisibilité des comportements humains les plus odieux. En France, le fichier judiciaire des infractions sexuelles recense les personnes condamnées pour des délits et des crimes sexuels et oblige celles d'entre elles ayant été le plus lourdement condamnées à se présenter tous les six mois au commissariat et à signaler tout changement de domicile. L'intérêt d'un tel fichier est indéniable car connaître la localisation de personnes dont la dangerosité est avérée, et qui se savent surveillées, peut contribuer à améliorer la prévention de la récidive. Or, ce fichier n'était pas encore entré en vigueur que, à la suite d'un fait divers particulièrement dramatique impliquant un récidiviste sexuel, plusieurs propositions de modifications ont été avancées afin d'obliger quasiment tous les délinquants sexuels à venir au commissariat non plus tous les six mois mais tous les trois mois, voire tous les mois. Ces propositions n'ont pas encore été suivies d'effet mais, une fois encore, le mythe du contrôle absolu par l'instrument informatique est à l'œuvre.

On le voit, croire que la création d'un fichier va permettre, en tant que telle, de résoudre un problème constitue trop souvent un leurre pour l'opinion publique.

5 – Le mythe du fichier infaillible et la problématique « majorité/minorité »

Les systèmes se développent et se perfectionnent sur le plan technologique. Ainsi, les traitements devenant de plus en plus performants, de moins en moins de personnes sont censées s'y trouver de manière non justifiée. Mais, de ce fait même, le problème est encore plus aigu pour les personnes qui figurent dans ces fichiers de manière indue, car tout portera à croire qu'il est impossible d'être dans ce fichier, aussi sophistiqué technologiquement, sans que cela soit justifié.

Sur le plan technique, il est impossible d'affirmer qu'un traitement de données peut être considéré comme fiable à 100 %. Il est donc indispensable, sur le plan éthique, de continuer à affirmer que **l'informatique peut être faillible** et de proscrire, tout particulièrement dans certains domaines tels que celui de la sécurité ou de la justice, la prise de décision automatique par ordinateur.

Comment dès lors faire prendre conscience aux exécutifs et aux législatifs que la création de fichiers, lorsqu'ils concernent potentiellement des millions de personnes, appelle au préalable une réflexion de fond et une évaluation à la fois de la mesure et de la technique utilisée ? L'exemple de la biométrie est sur ce point révélateur : considérée comme la panacée en matière d'identification et d'authentification, alors même qu'elle n'a jamais fait l'objet d'une évaluation officielle, concertée sur le plan international, la biométrie est aujourd'hui amenée à se développer massivement sans qu'aucune réflexion réelle n'ait été conduite sur les conséquences à l'égard des personnes des erreurs d'identification biométrique.

Pour conclure sur ces différents pièges, insistons sur le fait que **la problématique de sécurité présente toutes les caractéristiques d'un cheval de Troie**. Ce qui peut être finalement admis, dans ce domaine d'intervention, par les autorités de contrôle et les opinions publiques et individuelles peut devenir un précédent pour d'autres domaines d'action des fonctions régaliennes de l'État.

Si l'on n'y prend garde, il y a là, en germe, le risque de voir se vider de sa substance toute la philosophie qui sous-tend les textes fondamentaux en matière de protection des données personnelles.

C – Un troisième défi : la réputation de la protection des données et des autorités de contrôle

Au moins dans un certain nombre de pays, la protection des données et les autorités de protection des données ne jouissent pas de la réputation positive qu'elles méritent.

Les règles de protection des données peuvent être perçues comme complexes et difficiles à appliquer de manières cohérente, prévisible et réaliste. D'aucuns critiquent les

règles de protection des données comme trop abstraites et pas assez recentrées sur les dommages réels ou supposés – causés aux personnes ou à la société dans son ensemble – si ces règles ne sont pas observées. D'autres encore critiquent la manière dont ces règles sont interprétées ou mises en œuvre, ce qui les dissuade de se mettre en conformité ou d'investir dans des efforts de mise en conformité.

De telles perceptions négatives peuvent être celles d'hommes politiques, d'administrations, d'entreprises, des médias mais aussi de particuliers. Il est nécessaire de combattre ces perceptions, en démontrant l'importance pratique de la protection des données, en matérialisant la réalité des droits et libertés fondamentaux, et en reconsidérant certaines pratiques, si cela s'avère nécessaire.

II – LIGNES D'ACTION ET INITIATIVES

Pour faire face à de tels défis, il importe avant tout de reconsidérer nos méthodes d'action. Des initiatives germent ou existent sous l'impulsion de certains États à propos du rôle de la Conférence internationale, de l'OCDE à propos des instruments d'action des autorités de contrôle, de la Francophonie à propos de l'exigence d'une Convention internationale et de l'inventaire des moyens d'action des États… Tout cela concourt au même objectif et pourrait emprunter deux axes principaux.

Les autorités de contrôle doivent réfléchir ensemble :

– d'une part, à la manière de rendre plus efficace leur action,

– d'autre part, à faire reconnaître celle-ci de manière institutionnelle sur le plan international.

A – Les instruments

1 – La capacité d'expertise, de prospective et d'intervention dans le champ technologique

Face à ces deux vagues qui menacent de nous submerger, il nous faut trouver un **second souffle**. Il est crucial et urgent de développer et d'affûter nos capacités d'expertise et de prospective. Notre crédibilité se joue en ce moment même chaque fois que nous allons devant l'opinion publique pour exprimer notre point de vue face aux projets développés par les pouvoirs publics et le secteur privé.

Au-delà, l'expertise technique nécessaire pour apprécier les enjeux du développement de telle ou telle technologie devient de plus en plus pointue. Ces enjeux nécessitent un suivi permanent qui s'avère de plus en plus difficile à réaliser pour les autorités de protection des données. Force est de constater qu'aujourd'hui nos autorités sont plus présentes sur le terrain juridique que technique et que la protection des données « souffre » de son image trop juridique. **Or la crédibilité de nos institutions est et sera de plus en plus liée à notre capacité à comprendre et à anticiper les développements technologiques**. C'est un enjeu de taille pour les autorités de contrôle, mais il n'est pas concevable que se développent des techniques telles que le *peer-to-peer*, des applications comme Google Earth ou le Customer Experience Improvement Program de Microsoft sans que nous ne procédions, de façon coordonnée et concertée, à l'expertise de leurs potentialités. Le *peer-to-peer* signifie la libre circulation de quantités illimitées d'informations entre des acteurs situés en tout point de la planète, sans qu'il soit possible d'encadrer, sur le plan juridique, les échanges d'information en question. Google Earth, dans sa forme actuelle, constitue le socle idéal pour mettre en place des applications de géolocalisation d'une efficacité de plus en plus redoutable. Enfin, pour ceux qui ont accepté de participer aux programmes d'amélioration de ses logiciels, Microsoft reçoit, à Seattle, toutes les informations qu'il a jugé nécessaire de recueillir sur la façon d'utiliser ses logiciels (quand, comment, à quelle fréquence, etc.), construisant ainsi un profil détaillé de ses utilisateurs.

Pour analyser toutes ces nouveautés, est-il nécessaire chaque fois d'inventer ce qui existe déjà ? Nos autorités de contrôle ne sont-elles pas capables de mettre en place des structures de coordination nécessaires pour élaborer **des stratégies de division du travail entre les autorités**, en fonction de leurs expériences, de leurs responsabilités, de leurs moyens et des enjeux qui sont les leurs ?

Face aux puissances planétaires, économiques, créatives et financières que sont Microsoft ou Google, il est aujourd'hui indispensable et urgent de repenser notre mode d'expertise, de coordonner, en ce domaine, nos actions, de développer et de mettre en commun notre savoir technologique. Cela suppose aussi et surtout de réfléchir aux relations que nous souhaitons et devons entretenir avec la communauté des chercheurs et les industriels des technologies de l'information et de la communication.

2 – Évaluer notre efficacité et adapter nos pratiques

Le dialogue régulier et fructueux qui existe entre l'ensemble des autorités de contrôle permet de très vite toucher du doigt l'un des paradoxes qui aujourd'hui obère notre efficacité globale.

Prenons l'exemple de l'Union européenne. L'ensemble des 25 États de l'Union européenne s'est donné un corpus de règles communes dans le cadre de la directive de 1995, et nombre de ces États travaillent ensemble sur les

questions de protection des données depuis vingt ans. Pourtant, dès que l'on observe de plus près les pratiques des uns et des autres, issues de leurs textes de référence, on se trouve devant une mosaïque, une incroyable diversité.

Alors que toutes les autorités ont la même vocation, les mêmes missions à accomplir, défendent les mêmes principes, elles disposent de pouvoirs et utilisent des moyens parfois totalement différents les uns des autres. Certains pays mettent l'accent en forte priorité sur la politique de contrôle et de sanction, parmi ceux qui en disposent, d'autres privilégient le rôle des correspondants à la protection des données, d'autres encore donnent la primauté aux procédures de déclaration. Et d'autres pays enfin s'efforcent de développer une stratégie généraliste.

Probablement, certains de ces mécanismes sont plus efficaces que d'autres. Personne n'en sait rien. Probablement, certains de ces mécanismes sont complémentaires des uns et des autres. Personne n'en sait rien.

Il est donc absolument nécessaire de procéder à une **évaluation complète et sans fard de cette diversité dans l'utilisation des moyens d'action** pour en tirer des enseignements permettant d'améliorer les résultats des autorités concernées.

Mais cela passera alors par la remise en cause de pratiques de fonctionnement et aussi, parfois, par des revendications tendant à faire évoluer les législations en vigueur.

B – Nécessité d'une reconnaissance institutionnelle

Pour porter ces messages et ces actions vis-à-vis des responsables des États concernés mais aussi pour prolonger notre politique d'action, d'information et de dialogue à l'égard des pays qui entreprennent aujourd'hui une réflexion sur leur niveau de protection des données, nous devons, le plus rapidement possible, parvenir à une reconnaissance institutionnelle et donc à une existence internationale plus forte.

1 – Structuration de la conférence internationale

La conférence internationale des commissaires à la protection des données doit devenir le fer de lance de l'action de nos autorités sur le plan international. Pour ce faire, nos autorités ont besoin d'en structurer le fonctionnement, pour la rendre plus visible et plus efficace. Une réflexion est indéniablement nécessaire pour en assurer la viabilité et proposer des améliorations de fonctionnement. **Il convient dès lors de soutenir avec vigueur la résolution très opportune proposée en ce sens par nos collègues néo-zélandais.**

Peut-être est-il déjà possible, à ce stade, d'évoquer quelques pistes de réflexion, quelques objectifs. À court terme, nous devrons sans doute réfléchir à la manière dont nos conférences doivent permettre, plus que cela n'a été possible jusqu'à présent, la discussion et la remontée d'idées de portée concrète, **dans un but avoué d'harmonisation de nos pratiques et d'adoption de positions communes**. À moyen terme, il nous faudra trouver le moyen de faire vivre notre conférence tout au long de l'année, et plus seulement deux ou trois jours par an, élaborer un plan d'action, un programme de communication… Notre conférence devra également se donner les moyens d'être considérée sur le plan international comme un interlocuteur privilégié pour les initiatives internationales ayant une incidence sur le droit de la protection des données. Cela impliquera sans doute, à terme, de la doter d'un **secrétariat permanent**. La tâche est donc importante, et elle est urgente.

2 – Élaboration d'une Convention internationale

Par la **déclaration de Montreux**, nos autorités appelaient au développement d'une **Convention universelle de protection des données**. Cette initiative doit être soutenue, portée par nos autorités en parallèle du renforcement de la conférence internationale.

Cette Convention devrait être une grande déclaration de droits, consacrant la reconnaissance **d'un droit universel à la protection des données et à la vie privée**. Sous la forme d'un instrument juridiquement contraignant, elle doit reprendre et mettre en valeur tous les travaux effectués en matière de protection des données jusqu'à nos jours, sur le plan mondial.

Elle devra constituer également un outil indispensable à la collaboration entre autorités de contrôle, notamment dans les affaires sensibles de portée internationale, et permettre d'œuvrer pour le renforcement de leurs capacités, à se concerter face à l'accélération des nouvelles technologies. Elle favorisera des activités d'accompagnement aux démarches législatives, réglementaires et institutionnelles nécessaires à la mise en œuvre du droit à la protection des données.

Une longue marche sera sans nul doute nécessaire pour faire en sorte qu'une telle convention soit élaborée sous l'égide de l'organisation internationale compétente. Nous devons toutefois réaliser que nous avons parfois accès à des champs d'influence immenses qui peuvent être autant d'appuis pour faire avancer le projet. Je pense par exemple aux organisations régionales et aux zones linguistiques espagnole, francophone, lusophone, sans oublier le Commonwealth. Et **il reviendra à chacune de nos autorités de faire progresser cette idée et de la soutenir auprès de son gouvernement et**

des organisations auxquelles elle appartient[1], en fonction bien sûr de nos positionnements institutionnels respectifs et, éventuellement, après coordination avec les autres autorités compétentes en matière de protection des données au niveau national.

III – POUR UNE NOUVELLE STRATÉGIE DE COMMUNICATION

Nous devons, de manière urgente, concevoir et mettre en œuvre une nouvelle stratégie de communication, chacun en ce qui nous concerne mais également sur le plan international.

Cette nouvelle stratégie doit être conçue à la fois comme une fin et comme un moyen.

A – Un objectif : communiquer

La communication doit être conçue d'abord comme un objectif prioritaire. Est-il concevable, par exemple, que dans les pays de l'Union européenne où l'on inscrit le droit à la protection des données parmi les droits fondamentaux imprescriptibles tels que la liberté d'aller et venir ou la liberté de la presse[2], l'immense majorité de nos concitoyens n'ait aucune conscience d'en être titulaires ? Or nous ne disposerons jamais d'assez de moyens pour nous interposer entre chacun d'entre eux et leurs gouvernants respectifs. Dès lors, nous devons nous engager dans des **actions pédagogiques puissantes et, à long terme, visant à les informer de l'existence et du contenu de ces droits et à créer le réflexe de la protection des données personnelles**. Nos concitoyens devraient refuser de transiger sur leurs droits à la protection des données comme ils refuseraient de le faire pour la liberté de réunion ou la liberté de la presse.

Or tel n'est pas le cas, loin de là ! Nous avons donc à engager un immense effort de pédagogie et il peut nous arriver de défendre le droit des individus, si l'on ose dire, malgré eux. Toute la population est ainsi concernée, le citoyen en tant que tel, les salariés des entreprises, les fonctionnaires des administrations, etc.

Mais deux catégories doivent être visées en priorité :

– il s'agit d'abord des élus nationaux et locaux qui ont, par nature, une responsabilité particulière en la matière et dont l'information doit être améliorée ;

– en second lieu, il faut s'adresser aux jeunes générations qui, bien souvent, font preuve d'une grande indifférence vis-à-vis de ces questions tant elles sont habituées à manipuler ces nouvelles technologies au fur et à mesure qu'elles font l'objet d'usages publics. Chacun comprend que l'usage précoce de cette technologie, dépourvue de référence aux principes de la protection des données personnelles, ne favorise pas l'accès des jeunes à une **citoyenneté de l'informatique et des libertés**. Il faut donc **agir dans le secteur éducatif** le plus tôt possible. Si l'on osait risquer cette image : il faut faire en sorte que, dès l'instant où un enfant pose le doigt, pour la première fois, sur un clavier d'ordinateur, il intègre à son apprentissage l'impératif de la protection des données.

B – Un levier d'action : communiquer

Les réflexions qui précèdent montrent combien il est important et urgent de doter les autorités de moyens d'action supplémentaires et de leur assurer une reconnaissance sur le plan international.

Seules les organisations assurant une communication fondée sur des **thèmes largement accessibles au grand public** et tournés vers l'ensemble des médias disposeront de la **puissance nécessaire pour être entendues par les opinions publiques et donc par les États et la communauté internationale**. C'est à cette condition qu'ils pourront obtenir ces moyens d'action indispensables. Ceci passe probablement par une professionnalisation de la fonction de la communication au sein de nos autorités.

CONCLUSION

Nos autorités de contrôle occupent une place singulière et sans précédent au sein de l'organisation des pouvoirs publics de nos États respectifs. Nous ne sommes pas des législateurs mais certains d'entre nous peuvent émettre des réglementations à caractère contraignant. Nous ne sommes pas des sociétés de consultants mais nous nous honorons d'exercer, avant tout, un rôle de conseil auprès des acteurs de l'informatique et de nos concitoyens. Enfin, nous ne sommes pas des juridictions, mais certaines de

---

1. À titre d'exemple, l'action de la CNIL a mené les chefs d'État et de gouvernement de la Francophonie à appeler, dans la déclaration adoptée à l'issue de leur sommet de Bucarest, les 28 et 29 septembre 2006, à l'intensification des travaux nécessaires à l'adoption de législations et réglementations de protection des données, et, conscients de l'accroissement de la circulation de données personnelles au-delà des frontières, à marquer leur intérêt pour examiner l'opportunité d'élaborer un instrument international garantissant le droit des personnes à la protection des données à caractère personnel.
2. *Cf.* l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

nos autorités peuvent prendre des sanctions. En réalité, notre mission consiste à rechercher en permanence, au nom de la société, **un équilibre entre les impératifs de sécurité publique ou du développement économique, d'une part, et d'autre part, les exigences de la protection de la vie privée et des données personnelles**.

L'extrême difficulté de notre tâche réside dans le fait que nous devons définir la légitimité et les ressorts de cet équilibre en nous projetant cinq à dix ans plus tard. Nous devons éclairer le chemin que s'apprête à parcourir notre civilisation dans les usages qu'elle fait de l'informatique et **prévenir les dérives éventuelles** engendrées par la création de tel ou tel traitement de données. Et il est très difficile, alors même que nous savons que le résultat peut s'avérer catastrophique pour nos libertés, de se faire entendre lorsqu'il s'agit d'alerter nos concitoyens et nos gouvernants de menaces éventuelles. Les éléments mis en place par tel ministère vont s'ajouter à d'autres éléments, se conjuguer, se combiner pour créer des synergies et aboutir à des situations échappant à notre contrôle. Et le risque serait qu'un jour, on constate que notre civilisation est totalement engluée. Les responsables seront alors tout désignés et l'on comptera parmi eux les autorités de contrôle…

C'est pourquoi une piste intéressante consisterait à réfléchir à un thème qui pourrait être développé en commun par l'ensemble des autorités permettant de mettre chacun face à ses responsabilités et de sensibiliser fortement nos concitoyens. Il s'agirait, par analogie avec le thème du capital naturel de notre planète mise en danger par la pollution issue de l'activité humaine, de reprendre la notion de capital à préserver.

Chaque homme et l'humanité dans son ensemble sont à la fois détenteurs et responsables d'un capital. De même qu'on ne peut pas agir impunément en matière de protection de l'environnement, nous devons être extrêmement vigilants dans notre domaine, à l'égard de toute avancée technologique non maîtrisée comme de toute mise en œuvre de normes nouvelles consenties plus ou moins consciemment, parce que **ce capital de garantie de nos libertés et de notre identité peut alors être amputé ou menacé dans son existence même**.

Et il ne se renouvellera pas précisément en raison du **phénomène d'irréversibilité des effets du progrès technologique**.

Il y a donc là une **situation d'urgence** qu'il s'agit d'exposer à nos concitoyens.

LISTE DES DÉLIBÉRATIONS ADOPTÉES PAR LA CNIL EN 2006

NUMÉRO DATE	OBJET
2006-001 12 janvier 2006	Délibération portant avis sur le projet d'arrêté du ministre de l'Économie, des Finances et de l'Industrie modifiant l'arrêté du 5 avril 2002 portant création par la direction générale des impôts d'un traitement automatisé d'informations nominatives, dénommé « Accès au dossier fiscal des particuliers » (ADONIS)
2006-002 12 janvier 2006	Délibération portant refus d'autorisation de la mise en œuvre par la société Air Promotion Group d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux
2006-003 12 janvier 2006	Délibération portant refus d'autorisation de la mise en œuvre par le cabinet Breese-Derambure et Majerowicz d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux
2006-004 12 janvier 2006	Délibération portant refus d'autorisation de la mise en œuvre par la Société du marché d'intérêt national d'Avignon (SMINA) d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux
2006-005 12 janvier 2006	Délibération portant refus d'autorisation de la mise en œuvre par la clinique de Goussonville d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle des horaires des employés
2006-006 12 janvier 2006	Délibération portant autorisation de mise en œuvre par le lycée de la vallée de Chevreuse d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2006-007 12 janvier 2006	Délibération portant autorisation de mise en œuvre par le lycée Thierry Maulnier d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2006-008 12 janvier 2006	Délibération portant autorisation de mise en œuvre par le conseil général du Tarn-et-Garonne d'un système d'information géographique exploitant les données cadastrales
2006-009 19 janvier 2006	Délibération portant autorisation de mise en œuvre par le conseil général du Val-de-Marne d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place à titre expérimental d'un observatoire social des publics accueillis en circonscription d'actions sanitaires et sociales, dénommé « ISIS » (informations statistiques sur l'insertion sociale)
2006-010 19 janvier 2006	Délibération portant autorisation d'une expérimentation présentée par le GIE Groupama TPG ayant pour finalité d'accéder, sous forme anonymisée, à l'information sur les défauts visuels des assurés figurant sur les demandes de prises en charge

2006-011 24 janvier 2006	Délibération portant mise en demeure
2006-012 24 janvier 2006	Délibération portant mise en demeure
2006-013 24 janvier 2006	Délibération portant mise en demeure
2006-014 24 janvier 2006	Délibération portant mise en demeure
2006-015 24 janvier 2006	Délibération portant mise en demeure
2006-016 24 janvier 2006	Délibération portant mise en demeure
2006-017 24 janvier 2006	Délibération portant mise en demeure
2006-018 24 janvier 2006	Délibération portant mise en demeure
2006-019 2 février 2006	Délibération portant autorisation unique de certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit
2006-020 2 février 2006	Délibération portant refus d'autorisation de mise en œuvre par la SOFRES d'un traitement automatisé de données nominatives destiné à permettre la réalisation d'un sondage d'opinion téléphonique en vue d'objectiver, de mesurer et d'analyser l'état de l'opinion de la communauté juive de France
2006-021 2 février 2006	Délibération portant autorisation de la mise en œuvre par la Caisse d'allocations familiales de la Seine-Saint-Denis d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès aux locaux par reconnaissance des empreintes digitales
2006-022 2 février 2006	Délibération portant autorisation de la mise en œuvre par la banque Finama d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès aux locaux informatiques par reconnaissance des empreintes digitales
2006-023 2 février 2006	Délibération portant autorisation de la mise en œuvre par la SCM Imagerie médicale Jeanne d'Arc d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2006-024 2 février 2006	Délibération portant autorisation de la mise en œuvre par la société TAGG informatique d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité d'une part le contrôle de l'accès aux locaux, et d'autre part, le contrôle des horaires
2006-025 2 février 2006	Délibération portant autorisation de la mise en œuvre par la société Total S.A. d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux passes d'étages et aux clés des locaux à risques
2006-026 2 février 2006	Délibération portant autorisation de la mise en œuvre par la société Armatis S.A. d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux locaux

2006-027 2 février 2006	Délibération portant autorisation de la mise en œuvre par la société Gonesdis d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux locaux
2006-028 2 février 2006	Délibération portant autorisation de la mise en œuvre par la SNC Armatis Île-de-France d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès aux locaux
2006-029 2 février 2006	Délibération portant autorisation de mise en œuvre par le CHU de Grenoble d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un système d'information hospitalier destiné à permettre le partage de l'information « patient » entre les professionnels de l'établissement chargés de sa prise en charge et permettant la communication et l'échange de données vers et depuis la plate-forme régionale de santé Rhône-Alpes
2006-030 2 février 2006	Délibération portant autorisation de mise en œuvre par le réseau de l'association MGADDOC d'un traitement de données à caractère personnel ayant pour finalité la prise en charge médico-psycho-sociale des patients en difficulté avec des substances psycho-actives sur le département du Loir-et-Cher
2006-031 2 février 2006	Délibération portant autorisation de mise en œuvre par le collège Roland Garros d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2006-032 21 février 2006	Délibération portant mise en demeure
2006-033 21 février 2006	Délibération portant mise en demeure
2006-034 21 février 2006	Délibération portant mise en demeure
2006-035 21 février 2006	Délibération portant mise en demeure
2006-036 21 février 2006	Délibération portant mise en demeure
2006-037 21 février 2006	Délibération portant mise en demeure
2006-038 21 février 2006	Délibération portant mise en demeure
2006-039 21 février 2006	Délibération portant mise en demeure
2006-040 21 février 2006	Délibération portant mise en demeure
2006-041 21 février 2006	Délibération portant mise en demeure
2006-042 23 février 2006	Délibération portant avis sur le traitement de données à caractère personnel mettant en œuvre un dispositif de vote électronique pour les élections à l'Assemblée des Français de l'étranger du 18 juin 2006
2006-043 23 février 2006	Délibération portant refus d'autorisation de mise en œuvre par le GIE 50 d'un traitement automatisé de données à caractère personnel portant sur l'utilisation du numéro de sécurité sociale à des fins de « gestion de la relation client en mode multi-canal »

2006-044 23 février 2006	Délibération portant refus d'autorisation de mise en œuvre par la société Vie Plus d'un traitement automatisé de données à caractère personnel portant sur l'utilisation du numéro de sécurité sociale à des fins de gestion de la relation client dans le cadre de la souscription de contrats retraite individuelle et collective
2006-045 23 février 2006	Délibération portant refus d'autorisation de mise en œuvre par la société Volkswagen finances d'un traitement automatisé de données à caractère personnel ayant pour finalité l'utilisation du numéro de sécurité sociale à des fins de détection d'incohérence dans les demandes de crédit
2006-046 23 février 2006	Délibération portant refus d'autorisation de mise en œuvre par la société Montalivet Gestion d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des données des dossiers de recouvrement de créances pour le compte d'autrui
2006-047 23 février 2006	Délibération portant autorisation de la mise en œuvre par la société ALIS d'un traitement automatisé de données à caractère personnel ayant pour finalité principale la gestion des abonnés
2006-048 23 février 2006	Délibération portant refus d'autorisation de la mise en œuvre par la société ALIS d'un traitement automatisé de données à caractère personnel relatif au suivi des clients en infraction
2006-049 23 février 2006	Délibération portant autorisation de mise en œuvre par le lycée Maurice Ravel d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2006-050 23 février 2006	Délibération portant autorisation de mise en œuvre par le Réseau ferré de France d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2006-051 23 février 2006	Délibération portant autorisation de mise en œuvre par la banque BCP d'un traitement automatisé de données à caractère personnel ayant pour finalité l'établissement d'un score lors d'une demande de crédit d'un client particulier ou d'un prospect
2006-052 23 février 2006	Délibération portant autorisation de mise en œuvre par la Caisse Régionale du Crédit Agricole Mutuel du Midi d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en œuvre d'un outil d'aide à la décision lors de l'octroi d'un prêt habitat ou consommation (score)
2006-053 23 février 2006	Délibération portant autorisation de mise en œuvre par la société Disponis d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des financements des crédits aux particuliers
2006-054 23 février 2006	Délibération annulée
2006-055 23 février 2006	Délibération portant refus d'autorisation de mise en œuvre par MFP Services d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion de la relation client
2006-056 2 mars 2006	Délibération décidant la dispense de déclaration des traitements mis en œuvre par les collectivités territoriales et les services du représentant de l'État dans le cadre de la dématérialisation du contrôle de légalité
2006-057 2 mars 2006	Délibération portant refus d'autorisation de mise en œuvre par l'Association générale de prévoyance militaire (AGPM) d'un traitement automatisé de données à caractère personnel ayant pour finalité l'utilisation du numéro de sécurité sociale à des fins de gestion des dossiers d'indemnisation des victimes d'accidents de la circulation
2006-058 2 mars 2006	Délibération portant autorisation de la mise en œuvre par l'Établissement public administratif Euroméditerranée d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle d'accès aux locaux et le contrôle des horaires des employés

2006-059 2 mars 2006	Délibération portant autorisation de la mise en œuvre par la SCM Imagerie Rouen-Elbeuf-Le Neubourg d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2006-060 9 mars 2006	Délibération portant mise en demeure
2006-061 9 mars 2006	Délibération portant mise en demeure
2006-062 9 mars 2006	Délibération portant mise en demeure
2006-063 9 mars 2006	Délibération portant mise en demeure
2006-064 9 mars 2006	Délibération portant mise en demeure
2006-065 16 mars 2006	Délibération portant avis sur un projet de décret modifiant le décret n° 2005-556 du 27 mai 2005 portant création à titre expérimental d'un traitement automatisé de données à caractère personnel relatives à des passagers de l'aéroport Roissy-Charles de Gaulle
2006-066 16 mars 2006	Délibération portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public
2006-067 16 mars 2006	Délibération portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés
2006-068 16 mars 2006	Délibération portant autorisation de la mise en œuvre par la société Assistance totale en maintenance (ATM) d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2006-069 16 mars 2006	Délibération portant autorisation de la mise en œuvre par la société Brisach SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle des horaires
2006-070 16 mars 2006	Délibération portant autorisation de la mise en œuvre par la société Sagem Défense Sécurité d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2006-071 16 mars 2006	Délibération portant autorisation de la mise en œuvre par la société La Mesta Chimie fine SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2006-072 16 mars 2006	Délibération portant autorisation de mise en œuvre par la communauté de communes du Pays du Roi Morvan d'un traitement ayant pour finalité la mise en place d'un SIG à partir des données relatives à l'assainissement non collectif
2006-073 16 mars 2006	Délibération portant autorisation de mise en œuvre par la communauté d'agglomération du Beauvaisis d'un traitement ayant pour finalité la mise en place d'un SIG à partir des données relatives à l'assainissement non collectif
2006-074 16 mars 2006	Délibération portant autorisation de mise en œuvre par le conseil général du Gers d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données cadastrales

2006-075 16 mars 2006	Délibération portant autorisation de mise en œuvre par la direction départementale de l'équipement du Tarn-et-Garonne d'un traitement automatisé de données à caractère personnel comportant d'un SIG à partir des données cadastrales
2006-076 16 mars 2006	Délibération portant autorisation de mise en œuvre par la société Projep (ex-Leval 15) d'un traitement automatisé de données à caractère personnel ayant pour finalité l'aide à la décision (score)
2006-077 21 mars 2006	Délibération portant approbation d'une convention de partenariat avec la Haute Autorité de lutte contre les discriminations et pour l'égalité
2006-078 21 mars 2006	Délibération portant refus d'autorisation de mise en œuvre par le conseil représentatif des institutions juives de France d'un traitement automatisé de données à caractère personnel destiné à constituer un échantillon de sondage à partir d'un tri sur la consonance du nom des intéressés susceptible de faire apparaître leurs opinions religieuses
2006-079 21 mars 2006	Délibération portant avis sur la demande d'agrément présentée par la société D3P, candidate à l'hébergement du dossier médical personnel dans le cadre de son expérimentation
2006-080 21 mars 2006	Délibération portant avis sur la demande d'agrément présentée par la société France Telecom, candidate à l'hébergement du dossier médical personnel dans le cadre de son expérimentation
2006-081 21 mars 2006	Délibération portant avis sur la demande d'agrément présentée par la société inVita, candidate à l'hébergement du dossier médical personnel dans le cadre de son expérimentation
2006-082 21 mars 2006	Délibération portant avis sur la demande d'agrément présentée par le GIE Santeos, candidat à l'hébergement du dossier médical personnel dans le cadre de son expérimentation
2006-083 21 mars 2006	Délibération portant avis sur la demande d'agrément présentée par la société Thales-Cegedim, candidate à l'hébergement du dossier médical personnel dans le cadre de son expérimentation
2006-084 21 mars 2006	Délibération portant avis sur la demande d'agrément présentée par le groupement Santénergie, candidat à l'hébergement du dossier médical personnel dans le cadre de son expérimentation
2006-085 21 mars 2006	Délibération concernant un projet d'arrêté portant création d'un système informatisé de fabrication et de gestion des titres de voyage (PHILEAS) et modifiant l'arrêté du 30 mars 2005 relatif au système informatique de traitement des données relatives aux Français établis hors de France
2006-086 21 mars 2006	Délibération portant autorisation de mise en œuvre du traitement Télé@ctes par la direction générale des impôts visant à la dématérialisation des échanges entre le notariat et les conservations des hypothèques
2006-087 21 mars 2006	Délibération portant autorisation de mise en œuvre par la direction générale des impôts des modifications apportées au fichier informatique des données juridiques sur les immeubles (FIDJI) par la création de l'application Télé@ctes
2006-088 21 mars 2006	Délibération portant autorisation de mise en œuvre par la direction générale des impôts des modifications apportées à la Banque nationale de données patrimoniales (BNDP) par la création de l'application Télé@ctes
2006-089 21 mars 2006	Délibération portant autorisation unique de traitements de données à caractère personnel aux fins d'exercice des activités notariales et de rédaction des documents des offices notariaux
2006-090 21 mars 2006	Délibération portant autorisation de mise en œuvre par l'Institut de recherche et documentation en économie de la santé (IRDES) de l'Enquête Santé Protection Sociale (ESPS) 2006
6 avril 2006	Délibération portant autorisation de mise en œuvre par l'institut géographique national d'un traitement automatisé de données à caractère personnel visant à mettre en œuvre le référentiel à grande échelle
2006-092 6 avril 2006	Délibération portant autorisation de mise en œuvre par le lycée Paul Augier d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité la gestion de l'accès à la demi-pension

2006-093 6 avril 2006	Délibération portant autorisation de mise en œuvre par le collège Gérard Philipe d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2006-094 6 avril 2006	Délibération portant autorisation de mise en œuvre par le collège Louisa Paulin d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité la gestion de l'accès à la demi-pension
2006-095 6 avril 2006	Délibération portant autorisation de mise en œuvre par le lycée Henri Matisse d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité la gestion de l'accès à la demi-pension
2006-096 6 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Alsatel S.A. 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 et à la salle informatique
2006-097 6 avril 2006	Délibération portant autorisation de la mise en œuvre par la société APELEM d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2006-098 6 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Carrefour d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès à certains locaux
2006-099 6 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Diagnostic Medical Systems (DMS) d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2006-100 27 avril 2006	Délibération portant avis sur un projet de décret relatif à l'allocation temporaire d'attente
2006-101 27 avril 2006	Délibération portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail
2006-102 27 avril 2006	Délibération portant autorisation unique de mise en œuvre de dispositifs biométriques 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 aux locaux sur les lieux de travail
2006-103 27 avril 2006	Délibération portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire
2006-104 27 avril 2006	Délibération portant avis sur le projet d'arrêté présenté par le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, et créant un traitement de données à caractère personnel relatif aux espaces numériques de travail « ENT »
2006-105 27 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Neuf Telecom d'un traitement automatisé de données à caractère personnel relatif à la prévention des impayés
2006-106 27 avril 2006	Délibération portant autorisation de mise en œuvre par le lycée Léon Chiris d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2006-107 27 avril 2006	Délibération portant autorisation de mise en œuvre par l'OGEC Sainte-Marie/Saint-Vincent d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire

2006-108 27 avril 2006	Délibération portant autorisation de mise en œuvre par l'ensemble scolaire catholique Rochois Sainte-Marie/Sainte-Famille d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire
2006-109 27 avril 2006	Délibération portant autorisation de la mise en œuvre par le Service départemental Incendie et Secours de la Haute-Corse d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés
2006-110 27 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Centre Taxis Services d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé des infractions au Code de la route
2006-111 27 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Copagly d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé des infractions au Code de la route
2006-112 27 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Franco Taxis d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé des infractions au Code de la route
2006-113 27 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Nord Ouest Taxis d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé des infractions au Code de la route
2006-114 27 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Omnia Taxis d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé des infractions au Code de la route
2006-115 27 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Taxitel d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé des infractions au Code de la route
2006-116 27 avril 2006	Délibération portant autorisation de la mise en œuvre par la société Copagau d'un traitement automatisé de données à caractère personnel relatif à l'identification des conducteurs dans le cadre de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé des infractions au Code de la route
2006-117 27 avril 2006	Délibération portant mise en demeure
2006-118 27 avril 2006	Délibération portant mise en demeure
2006-119 27 avril 2006	Délibération portant mise en demeure
2006-120 27 avril 2006	Délibération portant mise en demeure
2006-121 27 avril 2006	Délibération portant mise en demeure

2006-122 27 avril 2006	Délibération portant mise en demeure
2006-123 27 avril 2006	Délibération portant mise en demeure
2006-124 27 avril 2006	Délibération portant mise en demeure
2006-125 27 avril 2006	Délibération portant mise en demeure
2006-126 27 avril 2006	Délibération portant mise en demeure
2006-127 27 avril 2006	Délibération portant mise en demeure
2006-128 27 avril 2006	Délibération portant mise en demeure
2006-128 27 avril 2006	Délibération portant mise en demeure
2006-129 9 mai 2006	Délibération portant avis sur les modifications des traitements de la direction générale des impôts rendues nécessaires par la généralisation du processus de préremplissage des déclarations de revenus, quel qu'en soit le support
2006-130 9 mai 2006	Délibération décidant de la dispense de déclaration des traitements relatifs à la gestion des membres et donateurs des associations à but non lucratif régies par la loi du 1er juillet 1901
2006-131 9 mai 2006	Délibération portant autorisation de mise en œuvre par l'unité 525 de l'Institut national de la santé et de la recherche médicale (INSERM) d'une banque d'ADN et d'ARN de patients présentant une athérosclérose coronarienne
2006-132 9 mai 2006	Délibération portant autorisation de mise en œuvre par l'unité 525 de l'Institut national de la santé et de la recherche médicale (INSERM) d'une banque d'ADN et d'ARN de patients présentant une athérosclérose coronarienne
2006-133 9 mai 2006	Délibération portant autorisation de la mise en œuvre par la société Sodebo reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès à certains locaux
2006-134 9 mai 2006	Délibération portant autorisation de la mise en œuvre par la Caisse d'allocations familiales de la Seine-Saint-Denis reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès aux locaux
2006-135 9 mai 2006	Délibération portant autorisation de la mise en œuvre par la société Visual 102 reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès à un site de tournage
2006-136 9 mai 2006	Délibération portant autorisation de la mise en œuvre par la banque Finama reposant sur la reconnaissance des empreintes digitales ayant pour finalité le contrôle des accès logiques au poste de travail
2006-137 9 mai 2006	Délibération portant autorisation de la mise en œuvre par la direction départementale de l'équipement du Val-de-Marne comportant un système d'information géographique à partir des données cadastrales
2006-138 9 mai 2006	Délibération décidant de la dispense de déclaration des traitements constitués à des fins d'information et de communication externe

2006-139 10 mai 2006	Délibération portant avertissement
2006-140 10 mai 2006	Délibération clôturant un dossier
2006-141 10 mai 2006	Délibération portant mise en demeure
2006-142 10 mai 2006	Délibération portant mise en demeure
2006-143 10 mai 2006	Délibération portant mise en demeure
2006-144 10 mai 2006	Délibération portant mise en demeure
2006-145 10 mai 2006	Délibération portant mise en demeure
2006-146 23 mai 2006	Délibération portant avis sur les dispositions de l'article 3-I du troisième projet de loi de simplification du droit (PLS3) relatif à la communication d'informations détenues par les organismes de sécurité sociale chargés de la gestion d'un régime obligatoire de sécurité sociale
2006-147 23 mai 2006	Délibération fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés
2006-148 23 mai 2006	Délibération portant autorisation de mise en œuvre par le Syndicat départemental d'assainissement autonome de Meurthe-et-Moselle (SDAA 54) d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales et d'assainissement non collectif
2006-149 23 mai 2006	Délibération portant autorisation de mise en œuvre par la Société française Donges-Metz (SFDM) d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2006-150 23 mai 2006	Délibération portant autorisation de mise en œuvre par la communauté de communes « Au pays de la Roche-aux-Fées » (CCPRF) d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales et d'assainissement non collectif
2006-151 30 mai 2006	Délibération portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel
2006-152 30 mai 2006	Délibération portant avis sur un projet de décret relatif aux réquisitions télématiques ou informatiques
2006-153 30 mai 2006	Délibération portant refus d'autorisation de la mise en œuvre par la société Rothschild & Compagnie Banque d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux
2006-154 30 mai 2006	Délibération portant refus d'autorisation de la mise en œuvre par la société Rothschild & Compagnie d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux
2006-155 30 mai 2006	Délibération portant refus d'autorisation de la mise en œuvre par la société Rothschild & Compagnie Gestion d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux

2006-156 30 mai 2006	Délibération portant refus d'autorisation de la mise en œuvre par la société Rothschild Gestion d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux
2006-157 30 mai 2006	Délibération portant refus d'autorisation de la mise en œuvre par la société Murano Urban Resort d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux chambres de l'hôtel
2006-158 30 mai 2006	Délibération portant autorisation de la mise en œuvre par la société La Mesta Chimie Fine SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux
2006-159 30 mai 2006	Délibération portant autorisation de la mise en œuvre par la banque BBVA d'un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre le blanchiment de capitaux et le financement du terrorisme
2006-160 8 juin 2006	Délibération portant avis sur un projet de loi autorisant l'approbation du protocole additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, fait à Strasbourg le 8 novembre 2001
2006-161 8 juin 2006	Délibération portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les pharmaciens à des fins de gestion de la pharmacie
2006-162 8 juin 2006	Délibération portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les biologistes à des fins de gestion du laboratoire d'analyses de biologie médicale
2006-163 8 juin 2006	Délibération portant autorisation de mise en œuvre par la communauté d'agglomération de l'Artois d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2006-164 8 juin 2006	Délibération portant autorisation de mise en œuvre par la communauté d'agglomération de Saint-Brieuc d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2006-165 8 juin 2006	Délibération portant autorisation de mise en œuvre par la communauté de communes du Montreuillois d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un système d'information géographique à partir des données relatives à l'assainissement non collectif
2006-166 13 juin 2006	Délibération portant habilitation de certains agents de la CNIL pour procéder à des vérifications
2006-167 13 juin 2006	Délibération portant avis sur le projet de loi relatif à la prévention de la délinquance
2006-168 13 juin 2006	Délibération portant avis sur un projet de décret pris pour l'application, à titre expérimental, de l'article L. 625-3 du code de l'entrée et du séjour des étrangers et du droit d'asile
2006-169 13 juin 2006	Délibération portant autorisation de la mise en œuvre par la société Omer Telecom Limited d'un traitement automatisé de données à caractère personnel relatif à la prévention des impayés
2006-170 26 juin 2006	Délibération portant autorisation de mise en œuvre par l'Institut national des études démographiques (INED) d'une enquête intitulée « Intégration des secondes générations en Europe »

2006-171 26 juin 2006	Délibération portant avis sur un projet d'arrêté relatif à l'expérimentation du placement sous surveillance électronique mobile
2006-172 26 juin 2006	Délibération portant autorisation de la mise en œuvre par la société Sanofi Chimie d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès logiques au système d'information
2006-173 28 juin 2006	Délibération portant sanction
2006-174 28 juin 2006	Délibération portant sanction
2006-175 28 juin 2006	Délibération portant mise en demeure
2006-176 28 juin 2006	Délibération portant avertissement
2006-177 28 juin 2006	Délibération portant mise en demeure
2006-178 28 juin 2006	Délibération portant mise en demeure
2006-179 28 juin 2006	Délibération portant mise en demeure
2006-180 28 juin 2006	Délibération portant mise en demeure
2006-181 28 juin 2006	Délibération portant mise en demeure
2006-182 28 juin 2006	Délibération portant mise en demeure
2006-183 28 juin 2006	Délibération portant mise en demeure
2006-184 28 juin 2006	Délibération portant mise en demeure
2006-185 28 juin 2006	Délibération portant mise en demeure
2006-186 6 juillet 2006	Délibération décidant la dispense de déclaration de certains traitements automatisés de données personnelles ayant pour finalité la tenue, l'utilisation et la communication des listes d'initiés
2006-187 6 juillet 2006	Délibération portant autorisation de mise en œuvre par le GIE GE Money outre-mer d'un traitement automatisé de données à caractère personnel ayant pour finalité la prévention de la fraude dans le domaine du crédit
2006-188 6 juillet 2006	Délibération portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion du contentieux lié au recouvrement des contraventions au Code de la route et l'identification des conducteurs dans le cadre du système de contrôle automatisé des infractions au Code de la route
2006-189 6 juillet 2006	Délibération portant autorisation de mise en œuvre par la Société lyonnaise de transports en commun (SLTC) d'un traitement automatisé de données à caractère personnel dénommé « Main courante du PC sécurité » et ayant pour finalité le recueil et la centralisation de toutes les informations relatives à la sécurité du réseau de transport en commun lyonnais

2006-190 6 juillet 2006	Délibération portant refus d'autorisation de mise en œuvre par l'Observatoire régional des études supérieures (ORES) de Lille Nord-Pas de Calais d'une étude sur les parcours des inscrits dans l'enseignement supérieur de la région
2006-191 6 juillet 2006	Délibération portant autorisation de mise en œuvre par l'Agence française de lutte contre le dopage d'un traitement automatisé de données à caractère personnel pour gérer la délivrance des autorisations d'usage à des fins thérapeutiques de produits ou de procédés interdits par la réglementation en matière de lutte contre le dopage
2006-192 6 juillet 2006	Délibération portant autorisation de mise en œuvre par le conseil général de la Loire d'un traitement modifiant la gestion du revenu minimum d'insertion
2006-193 6 juillet 2006	Délibération portant autorisation de mise en œuvre par la direction départementale de l'équipement de Seine-et-Marne d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2006-194 6 juillet 2006	Délibération portant autorisation de mise en œuvre par le conseil de développement du Pays Pyrénées-Méditerranée d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2006-195 6 juillet 2006	Délibération portant autorisation de mise en œuvre par la communauté de communes Aurence-Glane d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales et des données relatives à l'assainissement non collectif
2006-196 14 septembre 2006	Délibération portant sur l'habilitation de certains agents de la CNIL à procéder à des vérifications
2006-197 14 septembre 2006	Délibération portant avis sur le projet d'arrêté portant modification de l'arrêté du 29 août 1991 relatif au traitement informatisé du fichier national transfrontière
2006-198 14 septembre 2006	Délibération portant avis sur le projet d'arrêté portant création, à titre expérimental, d'un traitement automatisé de données à caractère personnel relatives aux passagers, enregistrées dans le système de contrôle des départs des transporteurs aériens
2006-199 14 septembre 2006	Délibération portant avis sur le projet de décret en Conseil d'État fixant, à titre expérimental, les modalités de transmission au ministère de l'Intérieur des données relatives aux passagers par les transporteurs aériens
2006-200 14 septembre 2006	Délibération portant avis sur les projets de décret et d'arrêté relatifs aux modalités de vote électronique pour l'élection des délégués du personnel et du comité d'entreprise
2006-201 14 septembre 2006	Délibération portant autorisation de la mise en œuvre par le conseil général des Bouches-du-Rhône d'un traitement automatisé de données à caractère personnel pour la gestion du système d'équipement billettique du réseau départemental d'autocars
2006-202 14 septembre 2006	Délibération portant autorisation de mise en œuvre par la SNCF d'un traitement automatisé de données à caractère personnel pour la gestion des abonnements TAPAS (forme billetterie ou forme billettique) souscrits par des voyageurs du réseau ferroviaire régional
2006-203 14 septembre 2006	Délibération portant autorisation de mise en œuvre par l'association Le cheval bleu d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un dossier minimum partagé dans le cadre d'un réseau santé mentale précarité
2006-204 21 septembre 2006	Délibération prononçant une sanction
2006-205 21 septembre 2006	Délibération prononçant une sanction
2006-206 21 septembre 2006	Délibération prononçant une sanction

2006-207 21 septembre 2006	Délibération prononçant une sanction
2006-208 21 septembre 2006	Délibération portant avertissement
2006-209 21 septembre 2006	Délibération portant mise en demeure
2006-210 21 septembre 2006	Délibération portant mise en demeure
2006-211 21 septembre 2006	Délibération portant mise en demeure
2006-212 21 septembre 2006	Délibération portant mise en demeure
2006-213 21 septembre 2006	Délibération portant mise en demeure
2006-214 21 septembre 2006	Délibération portant mise en demeure
2006-215 21 septembre 2006	Délibération portant mise en demeure
2006-216 28 septembre 2006	Délibération portant sur l'habilitation de certains agents de la CNIL à procéder à des vérifications
2006-217 28 septembre 2006	Délibération portant autorisation de la mise en œuvre par Aéroport de Paris SA d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité d'assurer la confidentialité et la protection des données stockées dans un ordinateur portable
2006-218 28 septembre 2006	Délibération portant avis sur le projet de décret modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004
2006-219 28 septembre 2006	Délibération portant avis sur le projet de décret pris pour l'application des I et II de l'article 6 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
2006-220 28 septembre 2006	Délibération portant avis sur un projet de loi autorisant la ratification du traité signé le 27 mai 2005, à Prüm, entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché du Luxembourg, le Royaume des Pays-Bas et la République d'Autriche, relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale
2006-221 28 septembre 2006	Délibération portant autorisation d'un traitement automatisé d'observation sociale statistique des agents du ministère de l'Équipement, des Transports, de l'Aménagement du territoire, du Tourisme et de la Mer
2006-222 28 septembre 2006	Délibération portant autorisation de l'expérimentation par la société CORA d'un traitement automatisé de données à caractère personnel ayant pour finalité d'assurer une protection contre la fraude par chèque bancaire

2006-223 5 octobre 2006	Délibération portant avis sur le projet de décret modifiant le système national des permis de conduire, le fichier national des immatriculations, modifiant le décret n° 2004-1266 du 25 novembre 2004 créant un traitement relatif aux ressortissants étrangers sollicitant la délivrance d'un visa et modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, en application de l'article 9 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
2006-224 5 octobre 2006	Délibération portant avis sur un projet de décret en Conseil d'État relatif à la carte d'assurance maladie et modifiant le code de la sécurité sociale
2006-225 5 octobre 2006	Délibération portant autorisation de mise en œuvre par la communauté de communes de la Haute-Saintonge d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2006-226 5 octobre 2006	Délibération portant autorisation de mise en œuvre par la communauté de communes de la région de Pons d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2006-227 5 octobre 2006	Délibération portant autorisation de la mise en œuvre par la Régie des transports marseillais (RTM) d'un traitement automatisé de données à caractère personnel relatif aux infractions à la police des services publics de transports terrestres
2006-228 5 octobre 2006	Délibération portant recommandation relative à la mise en œuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives, de fichiers à des fins de communication politique
2006-229 5 octobre 2006	Délibération relative aux traitements automatisés de données à caractère personnel mis en œuvre par les partis ou groupements à caractère politique, les élus ou les candidats à des fonctions électives à des fins de communication et modifiant la délibération n° 91-118 du 3 décembre 1991 (NS-034 modifiée)
2006-230 17 octobre 2006	Délibération dispensant de déclaration les traitements mis en œuvre par les comités d'entreprises ou d'établissements, les comités centraux d'entreprises, les comités de groupe ou les comités interentreprises ou les délégués du personnel pour la gestion de leurs activités sociales et culturelles
2006-231 17 octobre 2006	Délibération portant avis sur le projet de décret en Conseil d'État portant création de l'application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA)
2006-232 17 octobre 2006	Délibération autorisant la mise en œuvre par la société L'Oréal SA d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité l'identification des personnes à l'occasion de la signature de documents électroniques
2006-233 26 octobre 2006	Délibération autorisant la mise en œuvre par l'Inspection générale des finances d'une interconnexion temporaire entre les fichiers de la Direction générale des impôts et ceux de divers organismes de sécurité sociale ayant pour finalité de déterminer le taux national d'anomalie de calcul de la prime pour l'emploi
2006-234 26 octobre 2006	Délibération autorisant la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES) du ministère de la Santé et des Solidarités à mettre en œuvre les traitements automatisés de données à caractère personnel nécessaires à la réalisation d'une enquête statistique auprès des demandeurs de l'allocation aux adultes handicapés
2006-235 9 novembre 2006	Délibération portant autorisation unique de mise en œuvre par les organismes de location de véhicules de traitements automatisés de données à caractère personnel ayant pour finalité la gestion de fichiers de personnes à risques
2006-236 9 novembre 2006	Délibération autorisant la branche loueurs du Conseil national des professions de l'automobile (CNPA) à mettre en œuvre un fichier central de personnes présentant un risque contractuel

2006-237 9 novembre 2006	Délibération portant avis sur les projets de décret en Conseil d'État et d'arrêté relatifs à l'expérimentation du vote électronique pour les élections prud'homales de 2008
2006-238 9 novembre 2006	Délibération autorisant l'Institut de recherche et de documentation en économie de la santé (IRDES) à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité l'étude des facteurs conjoncturels et structurels associés aux indemnités journalières et aux consommations de soins associées aux arrêts de travail
2006-239 9 novembre 2006	Délibération autorisant la mise en œuvre par la Caisse nationale du régime social des indépendants d'un traitement de contrôle des prestations servies au titre de l'assurance maladie aux bénéficiaires d'exonération du ticket modérateur pour les affections de longue durée
2006-240 9 novembre 2006	Délibération autorisant la mise en œuvre par la société anonyme Électricité de Strasbourg d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales
2006-241 16 novembre 2006	Délibération autorisant l'Institut national de la statistique et des études économiques à mettre en œuvre les traitements automatisés de données à caractère personnel nécessaires à la réalisation d'une enquête statistique obligatoire sur les accidents du travail, les maladies professionnelles, les handicaps et les problèmes de santé de longue durée liés au travail et à l'exploitation de ses résultats
2006-242 16 novembre 2006	Délibération autorisant l'Institut national de la statistique et des études économiques à mettre en œuvre les traitements automatisés de données à caractère personnel nécessaires à la réalisation d'une enquête statistique obligatoire sur les accidents du travail, les maladies professionnelles, les handicaps et les problèmes de santé de longue durée liés au travail et à l'exploitation de ses résultats
2006-243 16 novembre 2006	Délibération autorisant la modification de deux traitements automatisés de données à caractère personnel mis en œuvre par la société Cetelem ayant respectivement pour finalité la lutte contre les tentatives d'obtentions irrégulières de crédit et la gestion des comptes clients
2006-244 16 novembre 2006	Délibération autorisant la modification de deux traitements automatisés de données à caractère personnel mis en œuvre par la société Cofinoga ayant respectivement pour finalité la lutte contre les tentatives d'obtentions irrégulières de crédit et la gestion des comptes clients
2006-245 23 novembre 2006	Délibération prononçant une sanction
2006-246 23 novembre 2006	Délibération portant avertissement
2006-247 23 novembre 2006	Délibération portant mise en demeure
2006-248 23 novembre 2006	Délibération portant mise en demeure
2006-249 23 novembre 2006	Délibération portant mise en demeure
2006-250 23 novembre 2006	Délibération portant mise en demeure
2006-251 23 novembre 2006	Délibération portant mise en demeure
2006-252 23 novembre 2006	Délibération portant mise en demeure
2006-253 23 novembre 2006	Délibération portant mise en demeure

2006-254 30 novembre 2006	Délibération autorisant la mise en œuvre par la direction régionale du service médical Languedoc-Roussillon (DRSM) d'un traitement automatisé de données à caractère personnel ayant pour finalité le suivi du contentieux technique entre le service médical et les professionnels de santé
2006-255 30 novembre 2006	Délibération autorisant la mise en œuvre par la direction régionale du service médical Midi-Pyrénées (DRSM) d'un traitement automatisé de données à caractère personnel ayant pour finalité le suivi des contrôles médicaux et l'analyse de l'activité des professionnels de santé
2006-256 30 novembre 2006	Délibération portant autorisation de la mise en œuvre par la société CGBC d'un traitement automatisé de données à caractère personnel relatif à la prévention des impayés
2006-257 5 décembre 2006	Délibération portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les collectivités locales ou leurs groupements à des fins de gestion de l'urbanisme ou du service public de l'assainissement non collectif (et pouvant comporter un système d'information géographique)
2006-258 5 décembre 2006	Délibération autorisant l'Institut national de veille sanitaire à modifier le système de notification obligatoire du VIH/sida
2006-259 5 décembre 2006	Délibération autorisant la mise en œuvre par la société ALIS d'un traitement automatisé de données à caractère personnel relatif au suivi des clients en infraction
2006-260 5 décembre 2006	Délibération autorisant la mise en œuvre par la société Télé2 Mobile d'un traitement automatisé de données à caractère personnel relatif à la prévention des impayés
2006-261 30 novembre 2006	Délibération portant avis sur un projet de décret en Conseil d'État relatif à l'enregistrement, à la conservation et au traitement par le greffe du tribunal de grande instance de Paris et les agents diplomatiques et consulaires des données à caractère personnel relatives à la formation, la modification et la dissolution du pacte civil de solidarité et abrogeant les décrets n° 99-1090 et 99-1091 du 21 décembre 1999
2006-262 5 décembre 2006	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 de Bagnères-de-Bigorre Loisirs SAS
2006-263 5 décembre 2006	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 GIE Casinos Conseil et Service
2006-264 5 décembre 2006	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 Amneville Loisirs SAS
2006-265 5 décembre 2006	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 Cagnes-sur-Mer Loisirs Sas
2006-266 5 décembre 2006	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 de Luc-sur-Mer
2006-267 5 décembre 2006	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 Le Grau-du-Roi Loisirs SAS
2006-268 5 décembre 2006	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 Dunkerque Loisirs SAS

2006-269 5 décembre 2006	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 Pau Loisirs SAS
2006-270 5 décembre 2006	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 Neris Loisirs SAS
2006-271 5 décembre 2006	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 Roscoff Loisirs SAS
2006-272 5 décembre 2006	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 St-Gervais Loisirs SAS
2006-273 5 décembre 2006	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 Pougues Loisirs SAS
2006-274 5 décembre 2006	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 Sète Loisirs SAS
2006-275 5 décembre 2006	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 Valras-Plage Loisirs
2006-276 5 décembre 2006	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 Villers-sur-Mer Loisirs SAS
2006-277 5 décembre 2006	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 Yport Loisirs SAS
2006-278 5 décembre 2006	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 Argelès-Gazost Loisirs SAS
2006-279 14 décembre 2006	Délibération prononçant une sanction
2006-280 14 décembre 2006	Délibération portant mise en demeure
2006-281 14 décembre 2006	Délibération prononçant une sanction
2006-282 14 décembre 2006	Délibération prononçant une sanction
2006-283 14 décembre 2006	Délibération portant mise en demeure
2006-284 14 décembre 2006	Délibération portant mise en demeure
2006-285 14 décembre 2006	Délibération portant mise en demeure

2006-286 14 décembre 2006	Délibération portant mise en demeure
2006-287 14 décembre 2006	Délibération portant mise en demeure
2006-288 14 décembre 2006	Délibération portant mise en demeure
2006-289 14 décembre 2006	Délibération portant mise en demeure
2006-290 14 décembre 2006	Délibération prononçant une sanction
2006-291 14 décembre 2006	Délibération portant mise en demeure
2006-292 21 décembre 2006	Délibération portant avis sur le projet d'arrêté portant modification de l'arrêté du 15 mai 1996 modifié relatif au fichier des personnes recherchées (FPR)
2006-293 21 décembre 2006	Délibération portant avis sur un projet de décret en Conseil d'État relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique
2006-294 21 décembre 2006	Délibération autorisant la mise en œuvre par l'association de Lutte contre la piraterie audiovisuelle (ALPA) d'un traitement de données à caractère personnel ayant pour finalité principale la recherche des auteurs de contrefaçons audiovisuelles
2006-295 21 décembre 2006	Norme simplifiée n° 54 relative aux traitements automatisés de données à caractère personnel mis en œuvre par les opticiens lunetiers pour la gestion de leur activité professionnelle
2006-296 21 décembre 2006	Délibération autorisant la mise en œuvre par la commission bancaire 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 contenu de clés USB
2006-297 21 décembre 2006	Délibération autorisant la mise en œuvre par la banque Accord d'un traitement automatisé de données à caractère personnel pour la prévention des risques de fraude à l'utilisation de la carte bancaire
2006-298 21 décembre 2006	Délibération autorisant la mise en œuvre par l'autorité de contrôle des assurances et des mutuelles (ACAM) d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au contenu des clés USB
2006-299 21 décembre 2006	Délibération autorisant la mise en œuvre par l'association du Pays de Langres d'un traitement automatisé de données à caractère personnel comportant un système d'information géographique à partir des données cadastrales

Mesures de simplification décidées en 2006

4 normes simplifiées destinées à alléger les formalités déclaratives des pharmaciens, des biologistes et des opticiens lunetiers ainsi que des organismes qui « géolocalisent » des véhicules utilisés par leurs employés.

5 dispenses de déclaration exonérant de toute formalité déclarative :

– les traitements mis en œuvre dans le cadre de la dématérialisation du contrôle de légalité ;

– les traitements constitués à des fins d'information ou de communication externe ;

– les traitements de gestion des membres et donateurs des associations à but non lucratif ;

– certains traitements visant la tenue, l'utilisation et la communication des listes d'initiés ;

– les traitements des comités d'entreprises ou des délégués du personnel pour la gestion de leurs activités sociales et culturelles.

8 autorisations uniques auxquelles peuvent se conformer d'autres traitements de même nature :

– aide à l'évaluation et à la sélection des risques en matière de crédit ;

– activités notariales ;

– contrôle d'accès et gestion des horaires et de la restauration sur les lieux de travail par la reconnaissance du contour de la main ;

– contrôle de l'accès aux lieux de travail par la reconnaissance de l'empreinte digitale lorsqu'elle est enregistrée sur un support individuel ;

– contrôle d'accès au restaurant scolaire grâce à la reconnaissance du contour de la main ;

– gestion du contentieux lié au recouvrement des contraventions au Code de la route et à l'identification des conducteurs dans le cadre du système de contrôle automatisé des infractions au Code de la route ;

– gestion des fichiers de personnes à risques mis en œuvre par les organismes de location de véhicules ;

– gestion de l'urbanisme ou du service public de l'assainissement non collectif mis en œuvre par les collectivités locales ou leurs groupements ;

1 avis sur un acte réglementaire unique auquel peuvent se rattacher les traitements de données personnelles relatifs aux espaces numériques de travail « ENT ».

LISTE DES ORGANISMES CONTRÔLÉS EN 2006

ASSURANCE COMPLÉMENTAIRE SANTÉ

AGF

AVIVA

AXA

C

GROUPAMA

MAAF SANTÉ

MACIF MUTUALITÉ

MAPA

MGEN

PRÉVIADE-MUTOUEST

BANQUE

BNP PARIBAS

GIE FÉDÉRAL SERVICE (BANQUE CRÉDIT MUTUEL)

LE CRÉDIT LYONNAIS

BIOMÉTRIE

CENTRE DE REMISE EN FORME CAM

DÉPARTEMENT DE RECHERCHES ARCHÉOLOGIQUES DE MARSEILLE

DIRECTION RÉGIONALE DES AFFAIRES CULTURELLES D'AIX-EN-PROVENCE

HÔTEL KUBE

HÔTEL MURANO URBAN RESORT

HÔTEL VERLAIN

LYCÉE PROFESSIONNEL PRIVÉ MARCEL LAMY

MAGIC FORM

RÉSIDENCE MASSÉNA (ASSOCIATION PARME)

COLLECTIVITÉS LOCALES

MAIRIE DE MONTPELLIER

CENTRE COMMUNAL D'ACTION SOCIALE DE MONTPELLIER

COMMUNAUTÉ D'AGGLOMÉRATION DE MONTPELLIER

MAIRIE DE LUXEUIL-LES-BAINS

MAIRIE D'ORLÉANS

COMMERCE

CENTRE LECLERC (ST DENIS-LES-SENS)

CENTRE LECLERC – COLANDIS (LANNION)

CENTRE LECLERC – PERLANDIS (LANNION)

IDENTICAR

ISORAMA (PARIS) : INTER CONFORT

ISORAMA (BOULOGNE-BILLANCOURT) : PRO DÉCOR

KYRIS

LE POINT DE VUE

RESTAURANT ALCAZAR

ÉNERGIE

EDF-GDF SERVICES (MONTPELLIER)

IMMOBILIER

AGENCE ALTICE

ESPACIMMO

INTERNET

CONSEIL BUREAUTIQUE SERVICE

E-NOV DÉVELOPPEMENT

IMPACT NET

SOCIÉTÉ KELPROF

JUSTICE

SCP AYNÉ JEAN-LUC – DURROUX BRUNO – LANCON LUC

SCP ELDIN DANY – BAUDIA PIERRE – GUILLEMAIN BRIGITTE

SCP LE DOUCEN ALAIN – CANDON PATRICK

SCP NEKADI JEAN-MARIE – PEYRACHE THIERY – DUMAS JEAN-MARC

MARKETING COMMERCIAL

Constructeurs automobiles

AUDI

GARAGE AUDI BAUER

CITROËN

STÉ AUTOMOBILES CITROËN

CAPGEMINI

STÉ COMMERCIALE AUTOMOBILE

STÉ DAP CITROËN

DAIMLERCHRYSLER FRANCE

FIAT

GROUPE FIAT

GARAGE HESS

FORD

FORD FRANCE AUTOMOBILES SAS

GENERAL MOTORS FRANCE

PEUGEOT

PEUGEOT SA

FILIALES PEUGEOT PARIS

PEUGEOT BOTZARIS PARIS

RENAULT

RENAULT

DIFATLANTIC

TOYOTA

TOYOTA FRANCE

PROFESSIONNELS DU MARKETING

ARK-DATA

ASDO ÉTUDES

BIS MEDIA

CONSO LISTS

DATEXIA DIRECT

GROUPE I-MEDIA

H-CONSULTANTS

I BASE

MEDIA PRISME

NETÉTUDES

NETNOE

PHONE CONTACT

WANADOO DATA

XPEDITE SYSTEMS

VENTE PAR CORRESPONDANCE

LA REDOUTE

SOCIÉTÉ SFC

RECOUVREMENT DE CRÉANCES

SOCIÉTÉ DRE

SOCIÉTÉ SOFINOR

SANTÉ
EXPÉRIMENTATION DU DOSSIER MÉDICAL PERSONNEL

D3P

CENTRE HOSPITALIER D'ANNECY

NATEXIS ALTAIR (LOGNES)

RÉSEAU SANTÉ SOCIAL (RUEIL-MALMAISON)

FRANCE TELECOM

CENTRE HOSPITALIER D'ARMENTIÈRES

FRANCE TELECOM (PARIS)

INVITA

HÔPITAL EUROPÉEN GEORGES POMPIDOU (PARIS)

INTRACALL CENTER (AMIENS)

INVITA (PARIS)

JET MULTIMEDIA (VÉLIZY-VILLACOUBLAY)

SANTENERGIE

BULL (TRELAZE)

NOUVELLES CLINIQUES NANTAISES

SANTEOS

ATOS WORLDLINE (BLOIS ET SECLIN)

RÉSEAU DIABÈTE PICARDIE (AMIENS)

THALES

CENTRE HOSPITALIER UNIVERSITAIRE DE STRASBOURG

THALES INFORMATION SYSTEMS (MALAKOFF)

SÉCURITÉ

AGENCE PAVAILLON

AGENCE TOURANGELLE ENQUÊTES ET RECHERCHES

GROUPE PROFIL FRANCE

SOCIÉTÉ B & M

SYSTÈME D'INFORMATION SCHENGEN (SIGNALEMENTS FONDÉS SUR L'ARTICLE 99 DE LA CONVENTION)

SPORT

FÉDÉRATION FRANÇAISE D'ÉQUITATION

GROUPEMENT HIPPIQUE NATIONAL

TÉLÉCOMMUNICATIONS

BOUYGUES TELECOM

FRANCE TELECOM

FREE

LE NUMÉRO

LES PAGES JAUNES

NEUF TELECOM

TRANSPORT

DISPOSITIF NAVIGO

RATP

GROUPEMENT D'INTÉRÊT ÉCONOMIQUE COMUTITRES

EXPERIAN

LASER CONTACT

TELETECH INTERNATIONAL

STUDIO MATAMORE

TRAVAIL

BATENBORCH INTERNATIONAL

DISNEYLAND RESORT PARIS

CAPFOR

GROUPE RICHELIEU CONSULTANTS

ROBERT HALF INTERNATIONAL FRANCE

SERVICE INNOVATION GROUP FRANCE

TYCO HEALTHCARE FRANCE

VIDÉOSURVEILLANCE

AUTOROUTES DU NORD ET DE L'EST DE LA FRANCE

AUTOROUTES PARIS RHIN RHÔNE

AUTOROUTES SUD DE LA FRANCE

HÔTEL VERLAIN

PHARMACIE LA BOÉTIE CHAMPS-ÉLYSÉES

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 restreinte

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 restreinte ». 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, 15, 23, 24, 26, 28, 39, 47, 55, 57, 58, 60, 62, 64, 66, 69, 71, 72, 73, 79.

© Fotolia : p. 11, 13, 14, 15, 25, 27, 55, 63, 66, 71, 74.

© Tralalere 2007 : p. 56.