COMMISSION
NATIONALE DE
L'INFORMATIQUE
ET DES LIBERTÉS

30e RAPPORT D'ACTIVITÉ 2009

ISBN : 978-2-11-008039-4

COMMISSION
NATIONALE DE
L'INFORMATIQUE
ET DES LIBERTÉS

30e RAPPORT D'ACTIVITÉ 2009

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

Sommaire

AU PROGRAMME 2010

CONCLUSION

ANNEXES

Avant-propos

Existe-t-il un exercice plus présomptueux que celui qui consiste à prétendre retracer, en quelques lignes, le travail accompli, avec dynamisme et passion, par 170 hommes et femmes, commissaires et collaborateurs, au service des libertés individuelles ?

Du moins peut-on, en quelques flashs, tenter de faire revivre les moments forts. Les bons et les moins bons…

Un bon moment pour nous que ce jour où notre Commission a vu son pouvoir de délivrer des labels enfin concrétisé dans la loi du 12 mai 2009 sur la simplification du droit. La loi du 6 août 2004 le prévoyait mais, faute de décrets d'application, ce projet n'avait pas pu se préciser. Un bon moment également, avec le renforcement du budget de notre Commission accordé par le Premier ministre, confirmant ainsi la tendance amorcée depuis 2004.

Moins bon moment, ce jour où un amendement Warsmann a mis, pendant quelques heures, ce même budget en péril…

Un moment ni bon ni mauvais, mais fort : la publication de notre rapport sur le STIC.

Une déception, enfin, de n'avoir pas convaincu la Commission chargée de réécrire le Préambule de la Constitution de 1958, de constitutionnaliser le droit à la protection des données personnelles.

Très grande satisfaction de constater que notre Commission est de plus en plus présente dans les grands débats de société, de plus en plus sollicitée par les pouvoirs publics, de plus en plus écoutée par nos concitoyens.

Je voudrais souligner également deux initiatives nouvelles engagées durant l'année 2009 et qui ont vocation à être pérennisées.

D'une part, nous avons rédigé et adressé à l'ensemble des élus locaux, soit environ 40 000 personnes, un guide des collectivités locales qui expose à la fois les règles et les enjeux « Informatique et Libertés » spécifiques à ces collectivités. Grand succès si l'on en juge par le nombre de contacts générés par cet envoi et, notamment, les centaines de maires qui nous ont fait connaître leur décision de doter leurs communes d'un « correspondant Informatique et Libertés ». Après les collectivités locales, notre cible prioritaire, en 2010, sera le milieu éducatif et surtout les jeunes élèves.

D'autre part, j'ai eu la joie – et l'honneur – de remettre le premier Prix de thèse de la CNIL couronnant un ouvrage contribuant à l'évolution de la doctrine « Informatique et Libertés » face aux nouveaux défis technologiques. Bien entendu, cette initiative sera renouvelée en 2010.

Enfin je rappelle au lecteur que notre rapport ne prétend pas être exhaustif mais bien mettre en lumière des tendances, des faits saillants, des inquiétudes – des angoisses aussi – et des espoirs ! Mais les équipes de notre Commission sont toujours, bien sûr, disponibles pour apporter les précisions et approfondissements qui pourraient être souhaités.

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

Le mot du secrétaire général

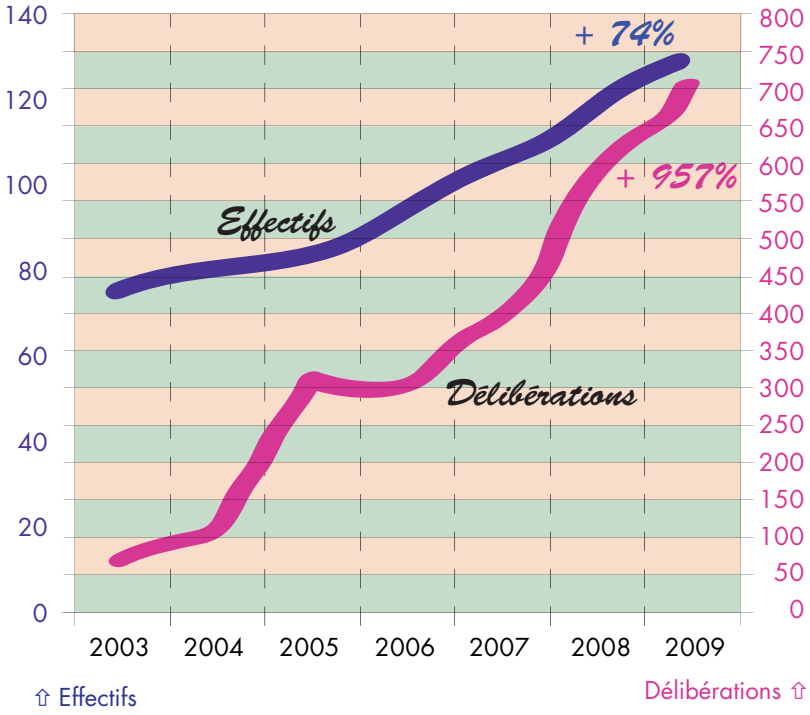
Bilan d'activité 2009

À l'heure du bilan, l'année 2009 m'apparait, avant tout, comme celle de la performance. Avec 719 délibérations (+23 % par rapport à 2008), 270 contrôles sur place (+24 % par rapport à 2008), notre Commission poursuit son développement mais, bien davantage encore, elle améliore son efficacité.

Cette efficacité accrue est d'abord le résultat de rationalisation de notre organisation engagée depuis 3 ans. C'est aussi, et surtout devrais-je dire, la conséquence la plus visible de l'investissement des équipes de la CNIL. Je tenais ici à les en remercier.

Ces efforts ont tous pour objectif l'amélioration du service rendu à l'usager. Trois faits marquants se sont produits en la matière en 2009.

Le premier est la réduction drastique des délais de délivrance des « récépissés » de déclarations. En effet, en 2007, un audit interne a révélé que ce délai moyen était de 13 mois, 25 % des récépissés étant délivrés après 24 mois alors même que la loi dispose qu'ils doivent l'être « sans délai ». En 2009, au prix d'une réorganisation débutée dès 2007, ce délai est désormais de trois semaines.



Le deuxième a été l'ouverture, en juillet 2009, d'un « extranet » dédié aux Correspondants informatique et libertés (CIL). Directement accessible depuis notre site, ce nouveau service offre une plateforme d'échanges privilégiés, des forums, des « questions-réponses », des modèles de formulaires, les supports de formation préparés

par les services de la CNIL. L'extranet est aujourd'hui utilisé par plus de 67% des CIL.

Le dernier consiste en la mise en ligne d'une nouvelle version de notre site internet. Structuré autour de publics cibles, offrant un moteur de recherche plus performant, des modèles de courriers actualisés, un fil d'actualité davantage fourni, ce nouveau site de la CNIL rencontre un réel succès puisque 2 millions de pages ont été vues en moyenne par mois en 2009, soit 2 fois plus qu'en 2008.

Toutefois, l'année 2009 ne saurait être évoquée sans qu'il soit fait état des décisions du 6 novembre du Conseil d'Etat annulant des sanctions prononcées par notre Commission au motif de l'irrégularité de la procédure de contrôle sur place. Fondées sur la jurisprudence de la Cour européenne des droits de l'Homme, ces décisions font que tous les éléments de preuve récoltés lors des 270 contrôles opérés en 2009 ne peuvent être légalement exploités. Près d'une année de travail des équipes de contrôleurs s'est ainsi trouvée réduite à néant, soit un coût significatif pour les deniers publics. Une réforme de la loi en cette matière est donc plus que nécessaire, impérieuse. Elle semble en bonne voie puisqu'une disposition en ce sens a été adoptée par le Sénat le 23 mars dernier.

Si 2010 devrait donc être l'année de la sécurisation juridique de nos procédures de contrôle, elle sera également, à mes yeux, celle de l'aboutissement et de l'audace.

Aboutissement des téléservices offerts par notre Commission tout d'abord. En effet, à l'heure où sont écrites ces lignes, notre site internet offre, enfin, la possibilité de procéder en ligne à une demande d'autorisation préalable qui, rappelons-le, constitue un régime juridique nouveau introduit par la loi du 6 août 2004 pour les fichiers les plus sensibles (biométrie, profilage, listes noires etc.). L'audace concerne le chantier de la labellisation. Depuis la loi du 13 mai 2009, notre Commission bénéficie, après 5 ans d'attente, de l'instrument juridique lui permettant de labelliser des produits informatiques ou des procédures, d'audit par exemple. Sur le fond, il s'agit pour nos équipes d'un nouveau métier, complexe, mêlant des considérations technologiques, juridiques et économiques. Notre objectif est de parvenir à modifier notre règlement intérieur cette année. Il s'agira ainsi de déterminer le cadre juridique de la mise en œuvre de ce nouveau pouvoir très attendu par nos entreprises qui y voient, à juste titre, un moyen de distinguer leur produit par leur « qualité » supérieure, puisque labellisée.

L'audace enfin est celle qui nous a conduits à engager une politique de communication institutionnelle sur les nouveaux espaces que sont les réseaux sociaux. Ainsi, au début 2010, la CNIL a ouvert son compte sur Facebook et Twitter. Sans cautionner pour autant la politique de collecte massive de données à laquelle se livrent ces sociétés commerciales, notre Commission a fait le choix d'utiliser ces moyens de communication en plein développement pour diffuser ses conseils et ses analyses aux utilisateurs. N'est-ce pas là le cœur de notre mission ?

Yann PADOVA

LES TEMPS FORTS DE L'ANNÉE 2009

PREMIER CONTRÔLE DU STIC

Un fichier de police judiciaire devenu un instrument d'enquêtes administratives

Officialisé par le décret n° 2001-583 du 5 juillet 2001, le STIC est un fichier national destiné à enregistrer les informations recueillies à partir des procédures établies par les services de la police nationale dans le cadre de leurs missions de police judiciaire. Il a pour finalité de *« faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs et l'exploitation des données à des fins de recherche statistique »*. Toutefois, la possibilité d'utiliser le STIC pour les enquêtes administratives a été introduite en 2001 et considérablement étendue en 2003 malgré les observations de la CNIL. Il peut être consulté à l'occasion du recrutement, de l'agrément ou de l'habilitation des personnels de professions très diverses. Ainsi en est-il, à titre d'exemple, des personnels de surveillance et de gardiennage, des personnes souhaitant travailler dans les zones aéroportuaires ou des agents de police municipale, des préfets, ambassadeurs, magistrats, etc. Mais c'est aussi le cas pour les demandes d'acquisition de la nationalité française ou pour une proposition à la Légion d'honneur.

Au total, la consultation du STIC à des fins d'enquête administrative est susceptible de concerner aujourd'hui plus d'un million d'emplois.

Un contrôle nécessaire avant l'entrée en vigueur d'Ariane

La Commission s'est prononcée sur les textes successifs intervenus pour encadrer ce fichier et a pu, à cette occasion, faire part de ses observations [1]. Elle exerce par ailleurs au quotidien les vérifications demandées par les intéressés eux-mêmes dans le cadre du droit d'accès indirect. Ce contrôle d'ensemble a permis d'effectuer un état des lieux, avant la mise en œuvre de la future application ARIANE (application de rapprochements, d'identification et d'analyse pour les enquêteurs) qui se substituera au STIC de la police nationale, et à JUDEX de la gendarmerie nationale. C'est ainsi que dix-neuf contrôles sur place ont été menés de juin 2007 à novembre 2008 (huit commissariats de police, trois services régionaux de police judiciaire, quatre tribunaux de grande instance, une direction régionale des renseignements généraux et trois préfectures). Ils ont permis, en interrogeant et contrôlant sur place les acteurs qui utilisent et interviennent dans le fonctionnement du STIC, de vérifier les modalités d'alimentation du fichier, les conditions et l'effectivité de sa mise à jour, les modalités d'accès et les mesures de sécurité existantes pour garantir la confidentialité des données qui y sont enregistrées.

En outre, un questionnaire portant sur le nombre d'affaires traitées, de classements sans suite, de décisions de relaxe, d'acquittement et de non-lieu, et de requalifications pénales rendus a été adressé aux trente-quatre tribunaux de grande instance représentant 50% de l'activité pénale de l'ensemble des TGI. Ce questionnaire a été complété pour trois TGI, par une interrogation précise à partir de cas nominatifs. Enfin, plusieurs questionnaires à caractère technique, assortis de requêtes informatiques, ont été adressés au ministère de l'Intérieur afin d'obtenir notamment des précisions sur la traçabilité des connexions au STIC.

Cette méthodologie, rigoureuse, permet à la Commission de disposer d'éléments nouveaux et précis dont la fiabilité n'a d'ailleurs pas été remise en cause par les deux ministères directement concernés.

Ce contrôle ne remet pas en cause la qualité des personnels participant au fonctionnement du STIC, mais souligne des problèmes le plus souvent liés à une inadéquation entre les moyens mis en œuvre par les ministères et les objectifs assignés à ce fichier de police. La CNIL a formulé **onze propositions** pour que son utilisation soit mieux contrôlée et plus sécurisée, afin de conforter l'exactitude et la mise à jour des informations enregistrées et largement consultées. Doivent être principalement relevées celles concernant :

1 Délibérations n° 98-97 du 24 novembre 1998, n° 00-064 du 19 décembre 2000, n° 2005-187 du 8 septembre 2005.

Le ministère de l'Intérieur, de l'Outre-mer et des Collectivités territoriales

Il s'agit de :
1. Mettre en œuvre une procédure pour sécuriser les opérations de saisie (mieux distinguer les victimes des personnes mises en cause) ;
2. Harmoniser les conditions d'enregistrement qui diffèrent d'un service régional de documentation criminelle (SRDC) à l'autre et engager une réflexion sur les conditions d'enregistrement des enfants de moins de 10 ans et les personnes âgées ;
3. Respecter les durées de conservation des informations dans les bases locales ;
4. Définir une politique de gestion des habilitations et des mots de passe plus stricte ;
5. Exploiter la traçabilité des accès au STIC pour mieux le sécuriser ;
6. Respecter les profils d'interrogation du fichier, en particulier en utilisant uniquement le profil administratif dans le cadre des enquêtes administratives (le non-respect des profils d'accès au STIC conduisant à donner accès de manière non justifiée à certaines informations, dont les conséquences peuvent s'avérer très préjudiciables pour les personnes concernées, en particulier quand le résultat de la consultation du STIC conditionne l'accès à un emploi) ;
7. Rendre obligatoire la vérification, par le préfet, qu'aucune décision judiciaire n'est intervenue devant conduire à l'effacement ou à la mise à jour de la fiche de la personne faisant l'objet d'une enquête administrative.

Le ministère de la Justice et des Libertés

8. Assurer la transmission des suites judiciaires au ministère de l'Intérieur en faisant une priorité de l'application CASSIOPÉE (application du ministère de la Justice permettant la gestion de l'ensemble de la chaîne pénale et l'échange d'informations avec le ministère de l'Intérieur).

Cette demande résulte du constat opéré par la CNIL de **l'absence quasi systématique de transmission par les parquets des suites judiciaires** nécessaires à la mise à jour du STIC (classements sans suite, acquittements, décisions de non-lieu, requalifications pénales). Or, les conséquences peuvent être très lourdes pour les personnes concernées par une enquête administrative : perte d'un emploi, refus d'embauche, impossibilité de passer un concours administratif, etc. **En 2007, 80% des classements sans suite pour insuffisance de charges ou infractions insuffisamment caractérisées n'ont pas été transmis par les TGI**.

Questions à …

Emmanuel de Givry

Conseiller honoraire
à la Cour de cassation
Vice Président délégué en charge
du secteur « Transports et assurance
des biens »

Quels sont les principaux enseignements du contrôle STIC opéré en 2007-2008 ?

À l'occasion de l'exercice du droit d'accès indirect aux fichiers de police intéressant la sûreté de l'État, la défense ou la sécurité publique, les magistrats membres de la CNIL dénonçaient régulièrement de sérieux dysfonctionnements dans l'alimentation et la gestion du STIC. Pour autant, il était souvent fait observer que cette appréciation était biaisée dans la mesure où elle se fondait sur les situations de personnes sollicitant la CNIL alors qu'elles se trouvaient dans des situations pour le moins délicates.

Les conclusions du premier contrôle approfondi du STIC effectué par la commission au titre des pouvoirs qu'elle tient de l'article 44 de la loi du 6 janvier 1978 modifiée, confirment de manière incontestable les lacunes dont est livrée l'analyse méthodique. Doit être à nouveau relevée que, trop souvent, des refus d'embauche ou d'habilitation conditionnant l'accès à un emploi sont pris à tort sur le fondement de données inexactes. C'est la raison pour laquelle est remarquée l'initiative prise par certains préfets qui, lorsque la consultation du STIC à des fins administratives font apparaître un enregistrement, s'attachent à compléter leurs informations par des contacts directs avec les parquets avant de se prononcer sur les demandes d'agrément.

Depuis la publication du rapport, le 20 janvier 2009, quelles suites a-t-il connu ?

À notre connaissance, le directeur des Affaires criminelles et des Grâces du ministère de la Justice a, dès le mois de février 2009, adressé un rappel aux procureurs généraux confirmant les insuffisances dans la mise à jour du STIC et leur a demandé de redoubler de vigilance compte tenu des conséquences humaines et sociales qui en résultent.

Par ailleurs, ce rapport, comme ceux qui l'avaient récemment précédé à l'initiative du ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales pour « mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés » n'a pu que souligner l'urgence d'achever l'application ARIANE, nouvelle base de données, qui devra remplacer le STIC et JUDEX, et faire de l'application CASSIOPÉE, outil de gestion de la chaîne pénale, une priorité de la chancellerie.

Sans lien direct avec la publication du rapport de la CNIL mais dans un contexte désormais marqué par les initiatives du Parlement en matière de fichiers de police à la suite de l'émotion suscitée par le fichier Edvige, l'année 2009 a été celle de la réalisation de deux importants rapports d'information : le premier, déposé par la commission des lois de l'Assemblée nationale, sur « les fichiers de police » avec pour rapporteurs Delphine Batho et Jacques-Alain Bénisti, le second, déposé au Sénat, relatif « au respect de la vie privée à l'heure des mémoires numériques » qui fait une large place à l'encadrement des fichiers de police sous la plume des sénateurs Yves Détraigne et Anne-Marie Escoffier.

Par ailleurs, relevons l'article 29 bis de la proposition de loi de simplification et d'amélioration de la qualité du droit adoptée en première lecture par l'Assemblée nationale le 2 décembre 2009 qui précise les finalités susceptibles de justifier la mise en œuvre de traitements à caractère personnel en matière de fichiers de police.

Et quelle sera la suite donnée par la CNIL ?

Conformément aux propositions formulées dans son rapport et dans le cadre des travaux législatifs qui leur donnent une résonance toute particulière, la CNIL saisira toutes les opportunités d'affirmer ses positions. Elle entend également autant que possible améliorer la qualité du dialogue avec les ministères concernés. Pour ce qui la concerne directement, elle a d'ores et déjà annoncé la réalisation d'un nouveau contrôle avant le 31 décembre 2011.

PUBLICITÉ CIBLÉE EN LIGNE : DES DONNÉES QUI VALENT DE L'OR

Vous venez de réserver un billet d'avion pour New York sur internet. Depuis, lorsque vous lisez votre quotidien en ligne, une publicité vous propose des locations de voiture pour cette ville à des tarifs intéressants. Ce n'est évidemment pas une coïncidence. C'est ce qu'on appelle de la publicité ciblée.

Il existe de nombreuses techniques de publicité ciblée en ligne. Dans le cas le plus simple, la publicité est basée sur les données que l'internaute a lui-même fournies pour s'inscrire sur un site internet (âge, sexe, adresse, etc.). Dans d'autres cas, la publicité ciblée est déterminée à partir des mots-clés que l'internaute saisit dans son moteur de recherche et de sa localisation. Celle-ci peut être obtenue, par exemple, à partir de l'adresse IP ou dans le cas de l'internet mobile, en utilisant l'identifiant d'antenne auquel le téléphone est connecté ou même sa position GPS.

Dans les cas les plus sophistiqués, la publicité ciblée est basée sur un suivi du comportement de l'internaute lors de sa navigation sur Internet. Cette technique de suivi fait généralement appel à des « cookies traceurs ».

Le modèle économique de nombreuses sociétés phares d'internet est basé sur la fourniture de services apparemment « gratuits » pour l'internaute, mais financés majoritairement, sinon exclusivement, par la publicité.

Le marketing ciblé est ainsi devenu l'un des éléments essentiels de l'économie numérique, de plus en plus gourmande en données personnelles. Avec le développement de la géolocalisation (fonctionnalités GPS incluses dans les téléphones couplées avec un accès à internet), la publicité sera à l'avenir ciblée au plus près de l'internaute.

Ces évolutions font craindre notamment un « profilage » systématique des internautes, qui plus est, à leur insu, ainsi qu'un risque de commercialisation des profils individuels entre les fournisseurs de contenus et les annonceurs. Dans cette logique marchande, l'internaute est alors considéré comme un « client » qui cède ses données personnelles en contrepartie d'un service rendu. Comme dans toute relation commerciale, il devrait alors avoir la possibilité à tout moment de retirer ses données personnelles s'il ne souhaite plus bénéficier du service qui lui est proposé. Or ce n'est pas toujours le cas.

Dans son rapport, rendu public en mars 2009, la CNIL fait le point sur les différentes techniques de publicité en ligne, sur les risques d'atteinte à la vie privée et les parades possibles.

Comment ça marche ?

La publicité ciblée

Comment est-il possible de connaître les centres d'intérêt ou les caractéristiques d'un internaute ?

L'internaute a fourni des informations sur lui (son âge, son sexe, sa localisation...) en s'inscrivant sur un service. On pourra alors le classer dans une catégorie marketing : par exemple « jeune urbain » ou « senior ».
L'internaute a saisi un mot-clé pour effectuer une recherche sur le moteur de recherche. L'analyse de ses informations permet d'obtenir des indices sur ses centres d'intérêt supposés et ainsi de déterminer la publicité qui sera affichée sur son écran. Son adresse IP pourra aussi permettre de déduire sa localisation et éventuellement la langue pratiquée.
La dernière technique consiste à observer le comportement de l'internaute sur une période plus ou moins longue, les sites qu'il a visités, les mots-clés utilisés, pour en déduire son profil et lui proposer des publicités adaptées.

Questions à …

Bernard Peyrat

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

Quel est le problème principal que pose la publicité ciblée en ligne aujourd'hui ?

Le principal reproche que l'on peut faire à l'encontre des mécanismes de publicité ciblée en ligne, c'est leur manque de transparence et l'absence d'information fournie aux internautes. D'ailleurs, de nombreux internautes ignorent totalement que leur comportement en ligne est épié par des régies publicitaires.

Pourtant, il est légitime de se poser certaines questions simples : Quelles données sont collectées ? Ces données incluent-elles des données sensibles (par exemple médicales, religieuses ou autres) ? Qui collecte ces données ? Combien de temps sont-elles conservées ? Avec qui ces données sont-elles partagées ?

Peut-on s'opposer à la publicité ciblée en ligne ?

Oui, tout internaute a le droit de s'opposer à ce type de publicité. Mais il faut souligner qu'aujourd'hui ce droit s'exerce de manière imparfaite. En premier lieu, il faut évidemment être clairement informé de ce droit pour pouvoir l'exercer, ce qui n'est pas toujours le cas puisque les internautes ignorent même souvent jusqu'à l'identité de la société qui affiche les publicités. En second lieu, les mécanismes permettant d'exercer ce droit ne sont pas toujours simples. Par exemple, de nombreuses régies publicitaires utilisent un « cookie » pour matérialiser le fait que l'internaute s'est opposé à la publicité ciblée. Or les internautes les plus sensibilisés à la protection de leurs données personnelles ont tendance à effacer régulièrement leurs « cookies » ce qui a pour conséquence d'effacer également la marque de leur opposition à recevoir de la publicité ciblée.

Quelles évolutions peut-on imaginer pour l'avenir ?

Dans le sillage de la publication de notre rapport public de février 2009 sur la publicité ciblée, notre Commission s'est engagée dans une réflexion sur ce sujet avec ses homologues européens. Ce travail devrait aboutir en 2010 à la publication d'un avis du G29 matérialisant notre position commune.

La CNIL a également engagé un dialogue avec divers acteurs de la publicité ciblée en ligne, soit directement, soit au travers d'organisations comme le Forum des droits sur l'internet, afin de réfléchir à la mise en place de bonnes pratiques au sein de cette industrie.

On peut en outre noter que des acteurs importants comme Google et Yahoo ! ont récemment mis en œuvre un certain nombre d'innovations afin d'offrir des plateformes de publicité ciblée plus transparentes et plus respectueuses des droits des internautes.

Enfin, il faut souligner que le législateur européen s'est saisi avec détermination de la question lors de la refonte en décembre 2009 du « paquet télécoms ». Le nouveau texte, qui doit être transposé en droit français au plus tard en mai 2011, devrait notamment obliger les régies publicitaires à obtenir le consentement préalable des internautes avant la mise en place de mécanisme de traçage basés sur les cookies. C'est un progrès qui serait bénéfique à tous.

CASSIOPÉE : CONSTELLATION OU NÉBULEUSE ?

Plusieurs critiques ont été adressées à l'institution judiciaire, ces dernières années, en ce qui concerne les retards pris dans l'informatisation des tribunaux et l'hétérogénéité des applications informatiques déployées dans les juridictions pénales. En effet, les applications pénales existantes actuellement dans les tribunaux de grande instance ont été développées dans les années 1980 à partir de technologies aujourd'hui vieillissantes et incompatibles entre elles. De plus elles ne couvrent pas l'ensemble du processus pénal. Ainsi de nombreuses juridictions ne disposent pas d'informatique de gestion des scellés ou de l'exécution des peines. Afin de répondre à ces difficultés, le ministère s'est lancé dans un programme de réforme dont les axes majeurs passent par le développement des nouvelles technologies et notamment la numérisation et la dématérialisation des procédures pénales, afin de permettre l'amélioration du traitement des dossiers (que ce soit en termes de délais ou de fiabilité des informations) ainsi que la fluidité des transmissions entre les différents acteurs du procès.

Le fichier CASSIOPÉE (Chaîne applicative supportant le système d'information orienté pénale et enfants), s'inscrit dans un plan de développement des nouvelles technologies dans les juridictions et constitue l'un des chantiers majeurs de la politique de modernisation du fonctionnement de l'institution judiciaire.

Une première étape de ce programme a été réalisée avec le traitement de gestion électronique de documents intitulé « Numérisation des procédures pénales » (NPP). La CNIL s'est prononcée sur ce dispositif qui a été déployé en 2008. Toutes les juridictions du premier comme du second degré, ont été dotées à cet effet de matériels leur permettant de numériser l'ensemble des pièces des procédures pénales.

CASSIOPÉE constitue la seconde étape de cette dématérialisation. La CNIL a rendu en mars 2009 un avis sur cette application destinée à mettre en œuvre le bureau d'ordre national automatisé des procédures judiciaires (prévu à l'article 48-1 du Code de procédure pénale). Ce traitement a pour objet l'enregistrement d'informations et de données à caractère personnel relatives aux procédures judiciaires au sein des tribunaux de grande instance. Il est accessible par les magistrats, les greffiers et les personnes habilitées pour les assister. Les procédures judiciaires concernées sont les procédures pénales, d'assistance éducative, civiles et commerciales, et celles relevant du juge des libertés et de la détention. Il permet d'assurer la gestion des audiences, l'élaboration des décisions des juridictions de jugement et des pièces associées, la gestion des voies de recours, la gestion des requêtes, la gestion des scellés et des objets en gardiennage.

Au sein des services pénaux d'un tribunal de grande instance, seul le service de l'application des peines dispose de son propre système, partagé avec l'administration pénitentiaire. Il s'agit du traitement APPI (Application des peines-probations et insertion) qui a pour objet le suivi des personnes faisant l'objet d'une mesure judiciaire en matière d'application des peines. Notre Commission s'est prononcée sur ce dispositif en octobre 2009. Compte tenu de la nécessaire continuité de la chaîne pénale, en particulier entre la phase de jugement et celle d'exécution des peines, il est prévu une interconnexion de CASSIOPÉE avec ce logiciel.

La Commission devrait également être saisie très prochainement d'une refonte du logiciel GIDE (Gestion informatisée des détenus en établissement) utilisé par les personnels des établissements et des services pénitentiaires. Cette application aura vocation à être interconnectée avec le logiciel APPI.

Questions à …

Claire Daval

Avocat
Commissaire en charge du secteur «Justice»

Sur quels points la Commission a-t-elle appelé l'attention du ministère dans son avis sur le traitement CASSIOPÉE ?

Dans son avis de mars 2009 notre Commission a souligné que le déploiement de cette application au sein des juridictions était un projet particulièrement ambitieux qui s'inscrivait dans un contexte délicat marqué par de profondes mutations. En effet, l'inflation des réformes (réforme de la carte judiciaire, réformes de l'instruction, de la justice des mineurs…) ainsi que le nombre croissant de procédures, peuvent laisser craindre des risques de dysfonctionnement lors du déploiement de CASSIOPÉE.

La Commission a également rappelé son attachement à la mise en œuvre de mesures de sécurités fortes et appropriées et a souligné la nécessité de mettre en place, le plus rapidement possible, les dispositifs nécessaires pour assurer le chiffrement du fichier compte tenu de la sensibilité des données enregistrées et du grand nombre de personnes habilitées à y accéder.

L'application CASSIOPÉE peut-elle jouer un rôle dans la mise à jour des fichiers d'antécédents judiciaires ?

La Commission a relevé à plusieurs reprises que la mise à jour des fichiers d'antécédents judiciaires n'était pas satisfaisante. En effet, le respect des dispositions prévues par l'article 3 du décret n° 2001-583 du 5 juillet 2001 portant création du STIC, c'est-à-dire la transmission par le procureur de la République de certaines suites judiciaires concernant des personnes mises en cause, notamment en cas de décision de relaxe, d'acquittement, de non-lieu ou encore de classement sans suite pour insuffisance de charge, s'avère difficile en l'état des modalités actuellement mises en œuvre (envoi d'une « fiche navette » renseignée manuellement). Dès lors, l'interconnexion de CASSIOPÉE avec la future application ARIANE, qui a vocation à se substituer aux fichiers STIC et JUDEX en les mutualisant, pourra jouer un rôle important dans la mise à jour de ces fichiers. En effet, CASSIOPÉE adressera directement à ce fichier les suites judiciaires données aux affaires enregistrées, ce qui devrait permettre d'améliorer leur mise à jour.

LE VOTE ÉLECTRONIQUE SOUS CONTRÔLE

Le recours au vote électronique, essentiellement par internet, se développe. Ce vote à distance diffère du vote électronique réalisé à partir de machines à voter utilisées pour des scrutins nationaux. Actuellement, le vote à distance par internet n'est possible que pour les scrutins qui offraient déjà la possibilité de voter par correspondance. La majorité des étapes sont les mêmes que lors d'un vote papier : l'élaboration des listes électorales et des candidats, l'ouverture et la fermeture du scrutin, l'élection d'un bureau de vote (président et assesseurs) et enfin le dépouillement du vote. Le bon déroulement d'un tel vote s'appuie sur la confiance apportée à un dispositif complexe et pouvant être ressenti comme opaque.

Dans la mesure où l'électeur ne pourra pas vérifier visuellement que tout se passe correctement, les garanties de sécurité apportées par le système informatique sont déterminantes. La CNIL a donc adopté une recommandation en juillet 2003 qui s'apparente à un guide de bonnes pratiques. Cette recommandation précise les garanties à respecter, notamment les conditions techniques permettant d'assurer le secret du scrutin, le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales et la surveillance effective du vote. Outre l'examen des dossiers de formalités préalables, la CNIL effectue régulièrement des contrôles de dispositifs de vote électronique, afin de s'assurer du respect de ces principes.

En quoi consiste le contrôle de la CNIL ?

Au cours de l'année 2009, la CNIL a effectué des contrôles d'élections électroniques organisées par des organismes privés et des ministères (élections prud'homales et de l'Ordre des infirmiers). Ces contrôles furent également l'occasion de vérifier les dispositifs de vote proposés par les différents prestataires du marché.

Lors de ces contrôles, les équipes de la CNIL se rendent dans le bureau de vote, généralement le premier jour du scrutin et lors de la clôture du vote électronique. Elles se rendent également dans les locaux du prestataire hébergeur, pour examiner le dispositif de vote utilisé.

La CNIL vérifie les conditions du scellement physique et logique de l'urne électronique, afin de détecter toute modification du dispositif de vote et d'empêcher toute manipulation des bulletins. Elle examine s'il existe, ou non, des moyens de connexion au dispositif de vote durant le scrutin. Elle vérifie ensuite si les différents programmes constitutifs du dispositif de vote utilisé ont été expertisés dans leur intégralité, en faisant notamment des copies de documents et de fichiers informatiques comme le lui permet la loi. Enfin, la Commission examine les moyens mis en œuvre pour s'assurer de l'identité des votants et du secret des votes.

Des constats et des sanctions

Ces contrôles ont permis de mettre en évidence l'insuffisance des garanties apportées par les dispositifs de vote, en termes de sécurité et de confidentialité des données.

Ainsi, la Commission a sanctionné plusieurs organismes ayant procédé à des votes par voie électronique. En effet, certains principes de la loi « Informatique et Libertés », rappelés dans sa recommandation n'avaient pas été respectés et notamment : l'interdiction de toute connexion au dispositif de vote durant le scrutin, l'assurance que la version expertisée du dispositif de vote était bien celle utilisée et le correct scellement de l'intégralité du dispositif de vote.

Ces contrôles témoignent de l'importance que la Commission attache aux opérations de vote électronique qui doivent être aussi sûres et démocratiques que les élections traditionnelles.

Questions à …

Isabelle Falque-Pierrotin

Conseiller d'État,
Vice-Président en charge du secteur « Vie citoyenne et collectivités locales »

Quels sont les principaux enseignements que l'on peut retenir des contrôles des élections organisées par voie électronique ?

Le constat majeur est le suivant : aucun dispositif de vote électronique ne respecte l'intégralité des recommandations de la CNIL. Si certaines solutions ont été améliorées, il n'en demeure pas moins que de nombreux progrès doivent encore être effectués pour garantir le secret du scrutin et la sincérité des opérations électorales. Par exemple, il a ainsi parfois été constaté que l'urne n'était pas correctement scellée et qu'elle n'était pas toujours sous le contrôle du bureau de vote. De surcroît, l'identité des votants n'était pas toujours garantie.

Quelles ont été les mesures prises par la CNIL à la suite de ces constats ?

Outre les observations qu'elle adresse aux responsables de traitements, c'est-à-dire les organisateurs des élections, la CNIL dialogue régulièrement avec les différents prestataires impliqués dans le développement de solutions de vote électronique. Elle révisera d'ailleurs prochainement sa recommandation en la matière.

En quoi consistera la révision de la recommandation ?

Globalement, la recommandation émise par la CNIL en 2003 est toujours d'actualité. C'est pourquoi, avant de procéder à cette révision, elle envisage d'auditionner différents acteurs concernés tels que des responsables de traitements, des chercheurs et des prestataires. Cette révision prendra principalement la forme d'une mise à jour pour tenir compte des dernières évolutions technologiques et des constats effectués lors des contrôles de la CNIL.

DES FICHIERS DE RENSEIGNEMENT MIEUX ENCADRÉS ET PLUS CONTRÔLÉS

Plus d'un an après l'abandon du fichier EDVIGE, le Gouvernement a publié, à l'automne dernier, deux décrets visant à remplacer les fichiers des ex-renseignements généraux. Ces décrets, pris après avis de la CNIL, concernent respectivement un fichier relatif à la prévention des atteintes à la sécurité publique et un fichier ayant trait aux enquêtes administratives liées à la sécurité publique.

La mise en œuvre de ces fichiers s'accompagne d'un certain nombre de garanties des droits et libertés des citoyens. À cet égard, la CNIL a pris une part importante à la définition de ce cadre juridique de référence.

Le fichier de prévention des atteintes à la sécurité publique

Les conditions de traitement des données « sensibles » ont été précisées, conformément aux demandes réitérées de la CNIL. Ainsi, seul l'enregistrement de données portant sur « l'activité » (information objective) politique, philosophique, religieuse ou syndicale des personnes est rendu possible et non plus celui des « opinions » (information subjective). En outre, seules pourront être enregistrées dans le fichier les informations tenant aux « *signes physiques particuliers et objectifs* » et à l' « *origine géographique* », ces dernières ne pouvant faire apparaître directement ou indirectement l'origine raciale ou ethnique des personnes

Questions à ...

Jean-Marie Cotteret

Professeur émérite des universités
Commissaire en charge du secteur « Police nationale et sûreté de l'Etat »

Quel regard portez-vous sur ces nouveaux fichiers, qui remplacent les anciens fichiers des renseignements généraux ?

En premier lieu, on ne peut que se féliciter de ce que le Gouvernement ait pris en compte les recommandations de la CNIL et décidé de créer deux fichiers distincts là où le projet initial consistait en la mise en œuvre d'un fichier unique comportant plusieurs finalités. Ces deux fichiers seront soumis aux règles du contrôle sur place opéré par la CNIL.

En second lieu, il convient de souligner que les textes qui encadrent le fonctionnement de ces fichiers ont été publiés, au même titre que les avis de la CNIL qui s'y rapportent. Le Gouvernement a ainsi fait droit à la demande de la Commission en ce sens.

Il importe de relever aussi que les accès aux fichiers feront l'objet de mesures de traçabilité strictes, lesquelles permettront, le cas échéant, à la CNIL d'opérer une vérification effective de l'utilisation de ces fichiers. Enfin, ils feront tous deux l'objet d'un rapport annuel portant sur les activités de vérification, de mise à jour et d'effacement des données enregistrées. Ce rapport annuel indiquera également les procédures suivies afin que les données enregistrées soient en permanence exactes au regard des finalités des fichiers.

Enfin, on doit se réjouir de ce qu'il n'est désormais plus question d'enregistrer de données ayant trait à la santé ou à la vie sexuelle des personnes, comme cela avait été initialement envisagé. Il n'est plus question non plus de recourir à un quelconque fichage des personnalités issues des mondes politique, syndical ou associatif.

De quoi s'agit-il ?

Les fichiers liés à la sécurité publique

Ces fichiers sont les outils de travail de la direction centrale de la sécurité publique. Le premier est un fichier de renseignement destiné à prévenir les atteintes à la sécurité publique. Il concerne ainsi les phénomènes de « violences urbaines » ou les phénomènes de violence relevés dans les stades, par exemple. Le second vise à faciliter la réalisation des enquêtes administratives auxquelles doivent se soumettre les personnes qui souhaitent pouvoir exercer telle ou telle activité liée à la sécurité publique (agents de sécurité, par exemple).

concernées. Le décret précise également que les « *signes physiques particuliers et objectifs* » doivent être uniquement entendus comme des « *éléments de signalement des personnes* ». Enfin, il ne sera pas possible de sélectionner dans le fichier une catégorie particulière de personnes à partir de ces seules données.

Par ailleurs, les données ne pourront être conservées dans le fichier plus de dix ans. Il s'agit là d'une avancée considérable, à mettre au crédit de la CNIL, dans la mesure où jusqu'alors aucune durée de conservation n'avait été précisée. En outre, la CNIL a obtenu du Gouvernement qu'il prévoit une durée spécifique de trois ans s'agissant des données relatives aux mineurs.

Le fichier relatif aux enquêtes administratives liées à la sécurité publique

Ce fichier se présente comme un simple répertoire des enquêtes administratives liées à la sécurité publique, associé à un mécanisme de gestion électronique de documents. Il concerne les enquêtes administratives liées soit aux emplois publics participant à l'exercice des missions de souveraineté de l'État, soit aux emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit aux emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit à l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit à l'utilisation de matériels ou produits présentant un caractère dangereux. Ainsi, comme demandé par la CNIL, les enquêtes administratives liées à l'instruction des demandes d'acquisition de la nationalité française ou à la délivrance et au renouvellement des titres relatifs à l'entrée et au séjour des étrangers ou à la nomination et la promotion dans les ordres nationaux ne seront pas concernées.

Les catégories de données à caractère personnel susceptibles de faire l'objet d'un enregistrement dans le fichier ont été considérablement réduites. Il n'est plus question d'enregistrer directement dans le fichier des données touchant aux « *activités publiques* », au « *comportement* », au « *déplacement* » ou à l' « *environnement* » des personnes, ni même des « *informations patrimoniales* » les concernant ou des données relatives à leurs « *antécédents judiciaires* ». En ce qui concerne les données « sensibles », leur enregistrement sera désormais prohibé.

Enfin, les données pourront être conservées pendant une durée maximale de cinq ans à compter de leur enregistrement dans le fichier. À cet égard, le point de départ de la durée de conservation a été à la fois reconsidéré et précisé par rapport au projet initial, conformément aux recommandations de la CNIL.

LA LUTTE CONTRE LA FRAUDE FISCALE ET SOCIALE

Évadés fiscaux : création du fichier EVAFISC

Les conditions de la mise en œuvre par l'administration fiscale du fichier EVAFISC ont été examinées le 12 novembre 2009 par la Commission.

Ce fichier s'inscrit dans le cadre de la politique de lutte contre la fraude fiscale conduite par les pouvoirs publics. Il comporte des informations relatives aux comptes bancaires détenus hors de France par des personnes physiques ou morales.

La finalité de ce fichier est d'enregistrer des données se rapportant à des risques de fraude sur la base d'informations obtenues par l'administration fiscale dans le cadre de ses missions légales (par exemple obtenues en exerçant son droit de communication prévu par les articles L. 96 A et L. 101 du Livre des procédures fiscales ou lors d'enquêtes ou de contrôles).

Dans son avis, la Commission a estimé que les finalités poursuivies par l'administration fiscale en créant le fichier « Evafisc », à savoir la prévention, la recherche, la constatation ou la poursuite d'infractions pénales et de manquements fiscaux, étaient légitimes.

En outre, la Commission s'est assurée auprès du ministère que les données figurant dans ce fichier font l'objet d'un contrôle systématique permettant de vérifier leur exactitude. Elle a également demandé que des vérifications régulières soient effectuées dans ce fichier, afin d'éviter d'éventuelles erreurs d'homonymie. Par ailleurs, les données enregistrées étant conservées pour une durée de dix ans, la Commission a demandé qu'un mécanisme de purge automatique soit mis en place.

La CNIL a également pu vérifier que ne seront rendus destinataires des informations contenues dans le fichier « Evafisc » que les agents habilités de la direction nationale des enquêtes fiscales.

Compte tenu de la nature de ce fichier, ayant notamment pour finalité la poursuite de manquements fiscaux et d'infractions pénales, les droits d'accès et de rectification s'exercent de manière indirecte auprès de la CNIL.

Le répertoire national de la protection sociale (RNCPS)

La loi du 21 décembre 2006 a prévu la création d'un répertoire national commun aux organismes de sécurité sociale, aux caisses assurant le service des congés payés, ainsi qu'à Pôle emploi. La création de ce répertoire poursuit trois objectifs : une simplification des démarches pour les assurés, une productivité accrue pour l'administration, et une meilleure efficacité de la lutte contre la fraude.

Le législateur a fixé les principales caractéristiques du RNCPS. Il a en particulier prévu qu'il comporte le numéro de sécurité sociale et l'adresse des assurés. Le répertoire permet également de connaître l'affiliation des assurés ainsi que la nature des prestations servies par les différents organismes (pension d'invalidité, retraite, indemnité chômage, etc.). Ce fichier ne contient cependant aucune information relative à d'éventuelles fraudes avérées.

Un décret en Conseil d'État, pris après avis de la CNIL, était nécessaire pour déterminer les modalités de gestion et d'utilisation de ce répertoire. C'est sur ce décret qu'a porté l'avis de la CNIL rendu le 30 avril 2009 après une instruction très approfondie du dossier.

Le RNCPS est un répertoire centré sur l'aide à la décision qui vient en complément de l'examen de la situation effectuée au cas par cas par un agent pour chaque assuré. Aucune décision ne peut être prise du simple fait de l'utilisation de ce répertoire. Le RNCPS permet toutefois de détecter les éventuels cumuls de prestations incompatibles et les prestations auxquelles un assuré pourrait prétendre et dont il ne bénéficie pas. La consultation du RNCPS n'entraîne aucune mise à jour automatique des données du répertoire ou du système d'information des organismes concernés.

Compte tenu de la sensibilité des fichiers ainsi constitués et du nombre très important de personnes susceptibles d'accéder au RNCPS, la CNIL a considéré que le suivi et le contrôle des habilitations constituaient un point essentiel pour garantir la sécurité et la confidentialité des données.

Elle a notamment veillé à ce que soient mis en œuvre :
– une traçabilité des accès au RNCPS couplé à un mécanisme d'alerte en cas de consultation anormale ou massive du répertoire ;
– un suivi très strict de la gestion des habilitations par les organismes utilisant le RNCPS ;
– des mécanismes de consultation sécurisés (saisie obligatoire du NIR et du nom de l'assuré pour chaque requête).

La CNIL a également veillé à ce que l'information des personnes notamment sur leurs droits d'accès et de rectification soit la plus complète possible (mention sur les sites internet et les formulaires des organismes, information affichée dans les lieux d'accueil du public, publication de documents d'information, information à l'occasion de l'envoi de courriers aux assurés).

Enfin, un bilan annuel sur le RNCPS doit être adressé à la CNIL. Ce bilan fera apparaître notamment les résultats obtenus en matière de contrôle et de lutte contre la fraude et de simplification des démarches pour les assurés.

Questions à …

Philippe Gosselin

Député de la Manche
Commissaire en charge du secteur « Questions fiscales et sociales »

Comment fonctionne le RNCPS ?
Le RNCPS est un répertoire à l'architecture technique innovante qui permet de connaître, en tant que de besoin, les données relatives aux prestations servies aux assurés par l'ensemble des organismes concernés, sans les conserver dans une base centrale.
Aucune donnée relative aux prestations ou à l'adresse des personnes n'est conservée ou centralisée dans le répertoire. Les organismes continuent d'héberger dans leurs propres systèmes d'information les données relatives aux prestations des assurés.

Quelles sont les données qui seront transmises par les organismes de sécurité sociale ou Pôle emploi ?
Le répertoire permet de connaître le nom des organismes de sécurité sociale auxquels un individu est ou a été rattaché dans les cinq dernières années et les droits et prestations qui lui sont servis sur cette période.
Ces données sont transmises par les organismes partenaires en temps réel. Elles ne comportent aucune information relative aux montants des droits et prestations perçus par un assuré, à sa situation familiale ou son état de santé.

Qui peut accéder au RNCPS ?
Certains organismes sont chargés de mettre en commun leurs données et d'alimenter le répertoire (organismes dits « contributeurs »). Il s'agit :
– des organismes chargés d'un régime obligatoire de sécurité sociale ;
– des caisses assurant le service des congés payés ;
– Pôle emploi.
D'autres organismes n'ont qu'un accès en consultation au répertoire (organismes dits « lecteurs »). Il s'agit :
– des organismes de la branche recouvrement (URSSAF) ;
– des collectivités territoriales et des centres communaux d'action sociale aux seules fins de vérifier les conditions d'accès à l'aide sociale.
L'administration fiscale n'est pas autorisée à consulter le RNCPS.

LES FICHIERS UTILISÉS EN MATIÈRE D'IMMIGRATION : TOUJOURS PLUS ?

Si l'année 2009 a été marquée par de larges débats publics et politiques en matière d'immigration, les fichiers utilisés dans le cadre de la gestion administrative des étrangers ont connu d'importantes évolutions cette année. Ainsi, la plupart des fichiers existants ont fait l'objet de modifications, et de nouveaux traitements informatiques ont été créés.

Le fichier OSCAR (outil de statistique et de contrôle de l'aide au retour)

Ce fichier, prévu par la loi du 20 novembre 2007 relative à la maîtrise de l'immigration, à l'intégration et à l'asile, est un dispositif biométrique qui enregistre les empreintes digitales des bénéficiaires d'une aide au retour (les étrangers résidant en France et qui souhaitent retourner dans leur pays d'origine en contrepartie d'une aide financière). Notre Commission, qui n'avait pas été saisie de la disposition législative ayant créé ce fichier, a été très attentive aux modalités précises de son fonctionnement. Elle a notamment demandé que les données biométriques de ces étrangers soient effacées du fichier si l'aide au retour leur a été refusée, qu'elles ne soient utilisées qu'à la seule fin de déterminer si une personne a déjà bénéficié d'une telle aide, et qu'elles ne soient pas accessibles aux services de l'OFII (Office français de l'immigration et de l'intégration) ou aux services préfectoraux en vue d'identifier ces personnes.

L'application RMV2 (Réseau mondial visas)

Une refonte complète du système RMV2 (Réseau mondial visas), qui enregistre les données issues des documents fournis lors du dépôt du dossier de demande de visa, a été entreprise. L'arrêté du 24 novembre 2009, pris après avis de la CNIL, doit ainsi permettre la mise en place du *Visa Information System*, en même temps qu'il élargit l'accès aux informations aux préfectures, aux services des douanes et à la direction centrale du renseignement intérieur. Il a également permis le recours à des prestataires extérieurs pour collecter les dossiers de demande de visa et enregistrer ces informations dans RMV2, ce sur quoi notre Commission s'est montrée très réservée, eu égard aux possibilités de captation de données par ces prestataires ou par les autorités des pays dans lesquels les visas sont délivrés.

De quoi s'agit-il ?

VIS (VISA INFORMATION SYSTEM)

Le VIS est destiné à améliorer la mise en œuvre de la politique commune en matière de visas, en permettant la mise en commun et l'échange entre États membres de l'Union européenne de données relatives aux demandes de visas Schengen qui leur sont adressées. Le système repose sur une base centrale européenne reliée aux systèmes nationaux. Il 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 Schengen, soit à terme, environ cent millions d'individus.

Le fichier FNAD (Fichier des non-admis)

Il s'agit d'un système biométrique qui enregistre notamment les empreintes digitales des étrangers contrôlés à la frontière et ne remplissant pas les conditions d'entrée requises. Créé pour deux ans en 2007 et limité à la frontière de l'aéroport de Roissy, l'expérimentation du FNAD a été reconduite pour deux ans. Notre Commission a obtenu que cette expérimentation soit rigoureusement évaluée, afin que l'intérêt de ce fichier, qui ne permet que d'identifier les personnes commettant une nouvelle infraction aux règles d'entrée sur le territoire, soit plus clairement établi avant d'envisager une généralisation à l'ensemble du territoire national.

Les fichiers relatifs aux demandeurs d'asile

Ces fichiers doivent faire l'objet de garanties spécifiques, car les dossiers de demande d'asile contiennent des données très sensibles, comme les opinions politiques et religieuses des personnes, ou leurs origines ethniques.

Le ministère de l'Immigration a ainsi créé le traitement DN@ qui vise à améliorer la gestion des centres d'accueil des demandeurs d'asile (CADA), en enregistrant des données permettant le suivi individualisé des personnes qui y sont prises en charge. L'avis de notre Commission a permis que ne soient pas enregistrées de données relatives à la protection sociale ou à la santé de ces personnes, et a exigé une procédure de désignation et d'habilitation individuelle pour tous les destinataires des informations et notamment l'OFII (Office français de l'immigration et de l'intégration), les services de l'asile du ministère de l'Immigration et les préfectures, afin que seuls les agents directement en charge de l'accueil des demandeurs d'asile aient accès aux données enregistrées dans DN@.

L'administration n'est pas seule à enregistrer des informations sur les demandeurs d'asile. Notre Commission a ainsi autorisé la CIMADE, association de défense des droits des étrangers intervenant notamment dans les centres de rétention administrative, à mettre en œuvre deux traitements informatiques, afin de gérer les dossiers des étrangers assistés dans ses permanences et dans les centres de rétention. Elle s'est montrée particulièrement attentive aux mesures de sécurité entourant le fonctionnement de ces fichiers (modalités d'accès aux données, traçabilité des actions, etc.), à la durée de conservation des informations, qui ne peut excéder un an, ainsi qu'aux modalités d'information des personnes et d'exercice des droits d'opposition, d'accès et de rectification ou de suppression des données qui les concernent.

Questions à …

Sébastien Huyghe

Député du Nord
Commissaire en charge du secteur « Identité, défense et affaires étrangères »

En quoi ont consisté les principales évolutions des fichiers informatiques utilisés dans le cadre de la gestion de l'immigration ?

Tout d'abord, des adaptations juridiques et techniques des fichiers existants ont été entreprises, notamment afin de prendre pleinement en compte les nouvelles attributions du ministère chargé de l'Immigration. De même, la refonte des missions de l'OFII, ex-ANAEM, a logiquement donné lieu à des ajustements des fichiers informatiques utilisés par cet office. Des initiatives européennes ont également nécessité des adaptations des fichiers nationaux utilisés en la matière, comme par exemple la mise en œuvre du *Visa Information System* (VIS) qui regroupera à terme les photographies, les empreintes digitales, ainsi que l'ensemble des données renseignées dans les dossiers de demande, de tous les demandeurs de visa à destination de l'Union européenne.

En second lieu, les conditions d'utilisation de certains fichiers ont été modifiées, notamment en élargissant les possibilités d'accès aux principaux fichiers d'étrangers afin de permettre un plus grand partage des données entre les autorités compétentes. Cet élargissement concerne au premier chef les services du ministère chargé de l'Immigration, mais également les services des douanes dans le cadre de leurs missions de contrôle aux frontières, les services préfectoraux, l'OFII ou encore, dans certains cas, les services antiterroristes.

Enfin, de nouveaux fichiers relatifs aux étrangers, expressément prévus par les lois votées en matière d'immigration ces dernières années ou répondant à de nouveaux besoins exprimés par l'administration, ont été mis en œuvre cette année. Dans l'ensemble, ces nouveaux fichiers confirment la tendance, déjà observée depuis plusieurs années, à recourir de plus en plus aux identifiants biométriques, et en particulier aux empreintes digitales des étrangers dans le cadre de la gestion administrative de l'immigration.

LES RÉSEAUX SOCIAUX ET LE DROIT À L'OUBLI

Facebook, Myspace, Linkedin, Copainsdavant, les réseaux sociaux sur internet, sont source de nouveaux enjeux en termes de protection de la vie privée. Ils offrent, certes, des services innovants et généralement gratuits, mais en contrepartie d'une collecte massive de données personnelles pour une utilisation commerciale.

Or le développement fulgurant des réseaux sociaux concerne directement la vie privée des internautes du fait de la très grande quantité de contenus déposée par les utilisateurs et de la coexistence d'univers personnels et professionnels sur les mêmes plateformes.

De nombreuses questions se posent donc, notamment sur l'information des personnes, l'utilisation des données par des tiers, le paramétrage par défaut des outils de gestion de la vie privée, ou encore les possibilités de quitter définitivement ces réseaux en supprimant son compte.

L'avis du G29

Compte tenu des enjeux, le G29 (groupe des CNIL européennes) a précisé les règles applicables aux réseaux sociaux dans son avis du 12 juin 2009. Cet avis affirme l'applicabilité du droit européen de protection des données aux réseaux sociaux, même quand leur siège se trouve hors d'Europe. De manière générale, les grands réseaux sociaux américains ne partagent pas cette analyse même s'ils font quelques efforts pour respecter la plupart des principes de protection des données. Notons que Linkedin est celui qui est allé le plus loin puisqu'il a effectué toutes les formalités déclaratives auprès de la CNIL.

Les CNIL européennes demandent également à ces acteurs de :

– définir des paramètres par défaut limitant la diffusion des données des internautes à leur insu ;
– mettre en place des mesures pour protéger les mineurs ;
– supprimer les comptes qui sont restés inactifs pendant une longue période ;
– permettre aux personnes, même si elles ne sont pas membres des réseaux sociaux, de bénéficier d'un droit de suppression des données qui les concernent ;
– proposer aux internautes d'utiliser un pseudonyme, plutôt que leur identité réelle ;
– mettre en place un outil accessible aux membres et aux non-membres, sur la page d'accueil des réseaux sociaux, permettant de déposer des plaintes relatives aux atteintes à la vie privée.

Pour faire un premier bilan de la mise en œuvre de son avis, le G29 a notamment organisé des auditions de certains réseaux sociaux, dont Facebook, lors de sa séance plénière de décembre 2009.

Les contrôles de la CNIL

En 2008 et 2009, la CNIL a effectué plusieurs contrôles auprès des principaux réseaux sociaux français. Les constats relevés sont les suivants :
– les outils pour gérer le niveau de visibilité des données sont difficilement accessibles ;
– les paramètres par défaut permettent généralement une visibilité complète du profil des membres ainsi qu'un référencement par les moteurs de recherche ;
– les personnes qui ne font pas partie du réseau ne sont pas toujours informées quand elles sont identifiées sur une photo de groupe ;
– les mentions d'information ne sont pas suffisamment visibles, principalement lorsque des données « sensibles » sont collectées ;
– les mesures pour protéger les mineurs sont parfois inexistantes ;
– des politiques de modération peuvent être mises en œuvre (filtrage par mots-clés ou zones géographiques ou à la suite d'un signalement par un utilisateur ou les autorités judiciaires), ce qui peut entraîner la désactivation, le gel ou la suppression de comptes utilisateurs, voire bloquer l'accès au réseau social ;
– la publicité peut être ciblée en fonction de l'âge, du sexe et de l'adresse IP de l'internaute sans que celui-ci ait moyen de s'y opposer ;
– les durées de conservation ne sont pas systématiquement définies et sont parfois excessives ;
– les demandes de suppression de données de la part d'internautes sont souvent prises en considération ;
– les mesures de sécurité sont globalement satisfaisantes, à l'exception des mesures prises pour assurer la sécurité des réquisitions judiciaires.

M É M O

43 % des Français estiment que leur vie privée est insuffisamment protégée sur les réseaux sociaux (échantillon IFOP de 1 000 personnes de 18 ans et plus, décembre 2009)

Questions à …

Alex Türk

Sénateur du Nord
Président de la CNIL

Pourquoi la CNIL est-elle préoccupée par le développement d'internet ?

Le monde est désormais entré dans la période du Web 2.0. Les nouvelles applications qui en découlent, et notamment les réseaux sociaux, font exploser le nombre d'informations personnelles accessibles sans limitation de durée sur internet. Les photos de soirées arrosées ou de vacances en maillot de bain sont mises en ligne sur Facebook. Des plaisanteries plus ou moins douteuses, des opinions politiques, des préférences sexuelles, des relations privées sont affichées sur des blogs. Les films personnels sont diffusés sur des sites vidéo – de plus en plus souvent à l'insu des personnes concernées.
Nous ne cessons d'exposer notre vie privée au vu et au su de tous, sans avoir conscience des risques que cela fait courir à chacun d'entre nous dans la vie réelle. Ces préoccupations sont d'autant plus vives qu'elles concernent au premier chef les jeunes générations.

Quelles peuvent être les conséquences des traces que nous laissons sur internet ?

La diffusion de ces informations sur le réseau peut avoir des conséquences désastreuses : nombre de professionnels (ressources humaines, compagnies d'assurances, recherche de personnes disparues…) utilisent désormais des données extraites d'internet pour vérifier, compléter ou valider des dossiers de candidats, de salariés ou de clients.
Dès lors, comment réagir lors d'un entretien d'embauche quand votre interlocuteur vous avoue qu'il doute que vos opinions politiques, affichées sur Facebook, soient compatibles avec les valeurs de l'entreprise ? Comment gérer les conséquences, sur sa vie personnelle, d'une condamnation judiciaire reprise sur un site internet, sans limitation de durée, alors même qu'une publication par voie papier n'aurait eu qu'un effet ponctuel et que le casier judiciaire prévoit l'effacement, au bout d'un certain temps, des condamnations ?
Ou encore, comment éviter qu'un bailleur refuse de louer un appartement à un jeune professionnel quand il aura trouvé sur lui des preuves d'une vie étudiante agitée, mais révolue ?

Que signifie la notion de droit à l'oubli numérique ?

Il est inacceptable et dangereux que l'information mise en ligne sur une personne ait vocation à demeurer fixe et intangible, alors que la nature humaine implique, précisément, que les individus changent, se contredisent, bref, évoluent tout naturellement.
Il en va, pour tous, de la protection de la liberté d'expression et de la liberté de pensée, mais aussi du droit de changer d'avis, de religion, d'opinions politiques, la possibilité de commettre des erreurs de jeunesse, puis de changer de vie.
C'est pourquoi notre Commission se félicite du débat qui s'ouvre actuellement en France sur ce sujet, qui souligne avec force le caractère fondamental du « droit à l'oubli ».

BON À SAVOIR

Faire supprimer une page web contenant des informations personnelles

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

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

LA CNIL EN ACTION

PROTÉGER

La CNIL protège vos droits

En 2009, la CNIL a reçu **4 265 plaintes** pour non-respect de la loi « Informatique et Libertés », soit un chiffre quasi identique à celui de l'année précédente (4 244).

Ce volume important de plaintes – la CNIL en reçoit aujourd'hui deux fois plus qu'il y a dix ans – montre que les particuliers, qu'ils soient salariés, usagers des services publics, clients d'entreprises ou « prospects », sont de plus en plus soucieux de défendre leurs droits « Informatique et Libertés ».

La CNIL est là pour les y aider.

C'est ainsi que les personnes peuvent notamment trouver sur www.cnil.fr des dossiers thématiques, des questions-réponses et des modèles de courriers pour exercer plus facilement leurs droits.

Un « mode d'emploi » a également été mis en ligne, en 2009, pour informer le grand public de la possibilité d'adresser une plainte à la CNIL, des modalités à suivre et de la façon dont les plaintes sont traitées (rubrique *« vos libertés » – « la CNIL à vos côtés »).*

Toujours dans le but d'améliorer le service à l'usager, un courrier d'information est désormais adressé à chaque plaignant, à réception de son dossier, pour qu'il puisse mieux suivre le traitement de sa plainte.

Enfin, les personnes qui ne parviennent pas à se faire radier d'un fichier de publicité (droit d'opposition) ou qui ne peuvent pas obtenir copie de leurs données enregistrées dans un fichier (droit d'accès) pourront bientôt adresser leur plainte en ligne, grâce à un nouveau téléservice qui leur sera proposé sur le site internet de la CNIL au premier semestre 2010.

Les secteurs les plus concernés par les plaintes en 2009 sont : *banque-crédit, prospection commerciale, internet/télécoms, travail.* Cinq cas concrets permettent d'illustrer l'action régulatrice de la CNIL face aux difficultés rencontrées par des particuliers.

Une caméra trop indiscrète

Une déléguée syndicale saisit la CNIL d'une plainte à la suite de l'installation de caméras de vidéosurveillance dans son entreprise.
Deux des caméras filmeraient la badgeuse ainsi que le couloir menant à la salle de pause et au local syndical.
La CNIL adresse un courrier à l'employeur, qui avait déclaré son dispositif en 2006, pour lui rappeler que la vidéosurveillance ne doit pas être disproportionnée et ne peut pas visualiser les locaux syndicaux et leur accès.
L'employeur répond à la CNIL qu'il a décidé de modifier l'orientation de la première caméra afin qu'elle ne filme plus la badgeuse.
La seconde caméra, filmant le couloir menant à la salle de pause et au local syndical, est retirée.
L'intervention de la CNIL a ainsi permis de faire respecter le droit des salariés à ne pas être placés sous surveillance sans raison.

Un bon payeur mal récompensé

Monsieur Y. rembourse son prêt par anticipation en adressant à la société de crédit deux chèques à quelques semaines d'intervalle.
Quatre ans plus tard, la société prélève sur le compte bancaire de Monsieur Y. une première mensualité, puis une deuxième.
Monsieur Y. demande alors à sa banque de faire opposition aux prochains prélèvements. Deux mois plus tard, Monsieur Y. reçoit une lettre émanant de la société de crédit lui demandant de régulariser ses deux échéances impayées. Monsieur Y. explique en vain à cette société qu'il a remboursé son crédit par anticipation quatre ans auparavant.
Le mois suivant, Monsieur Y. est inscrit au Fichier national des Incidents de remboursement des Crédits aux Particuliers (FICP). Ce fichier recense les incidents de remboursement lié au crédit et a pour conséquence de ne pas pouvoir souscrire un crédit. Monsieur Y. saisit la CNIL qui demande à la société de crédit des explications sur le cas de Monsieur Y.
La société reconnaît alors son erreur.
En effet, le premier chèque avait été enregistré comme un règlement anticipé « partiel » et affecté sur le capital restant dû.
Le deuxième chèque avait été enregistré comme un « payé d'avance » sur les échéances à venir des quatre prochaines années. Les prélèvements avaient donc été suspendus durant cette période.
Puis les prélèvements avaient repris, à tort, à l'issue de cette période de quatre ans.
Grâce à l'intervention de la CNIL, la société fait immédiatement lever l'inscription de Monsieur Y. au FICP qui l'empêchait d'obtenir tout nouveau crédit.

Des cours « gratuits » qui coûtent chers

Monsieur K. recherche des cours d'espagnol pour son enfant et souscrit une formule payante sur un site proposant des cours particuliers. Cette formule comprend un mois d'accès gratuit à un site d'aide à l'apprentissage des mathématiques.
Quelques mois plus tard, Monsieur K. a la surprise de constater que deux prélèvements sur son compte bancaire ont été effectués par une société qui lui est inconnue. Il s'aperçoit, par la suite, que le mois d'accès gratuit, offert dans le cadre de la formule achetée sur le site de cours particuliers, s'est prolongé sous forme d'un abonnement payant.
Monsieur K. n'a pourtant jamais sollicité les services de cette société et n'a pas communiqué les données bancaires utilisées pour débiter son compte.
Indigné par ces pratiques, il demande à la CNIL d'intervenir.
La CNIL signale au responsable du site de cours particuliers que ses clients ne disposent pas d'informations claires sur les formules d'abonnement proposées en ligne.
Ils ignorent en effet qu'elles intègrent automatiquement l'accès au service d'une société partenaire facturé mensuellement au-delà du premier mois.
Grâce à l'intervention de la CNIL, les clients de ce site sont désormais informés par une fenêtre spécifique de l'existence de ce service additionnel et de la transmission de leurs coordonnées à son partenaire aux fins de facturation, s'ils décident d'y souscrire.

Droit à l'oubli

Monsieur X, ancien militaire à la recherche d'un emploi a eu la mauvaise surprise de découvrir qu'il était qualifié de « bastonneur » sur un blog d'anciens élèves de son lycée. Il a fait savoir au contact de ce blog qu'il avait adressé une plainte à la CNIL et qu'il souhaitait exercer son droit d'opposition conformément à l'article 38 de la loi Informatique et libertés. Il a finalement obtenu gain de cause.

Street View s'invite chez vous !

Monsieur et Madame B. découvrent sur internet que le module « Street View » de l'application « Google Maps » permet d'accéder à des vues de leur domicile.
Ils sont stupéfaits de constater que ce service de Google diffuse des vues de l'intérieur de leur propriété sur lesquelles on aperçoit leur fille âgée de quatre ans en sous-vêtements.
Considérant ces vues comme attentatoires à leur vie privée et dangereuses pour la sécurité de leur fille, Monsieur et Madame B. utilisent le formulaire mis en place par Google pour demander leur suppression.
N'obtenant pas satisfaction, ils saisissent la CNIL qui intervient directement auprès de Google France. Google indique en réponse que les vues concernées ont été supprimées.

Aspirer des annonces immobilières, ça peut coûter cher !

Des personnes qui ont passé des annonces sur des sites spécialisés de particuliers ont été surprises d'être démarchées par des « partenaires » de la société DIRECTANNONCES. Surtout, elles ont constaté qu'elles étaient dans l'impossibilité de s'opposer à figurer dans le traitement mis en œuvre par DIRECTANNONCES. Un contrôle de la CNIL a permis de constater que la société DIRECTANNONCES « aspirait » des annonces immobilières sur des sites internet dédiés à des particuliers, en vue de les compiler dans des « piges » et de les vendre.
La Commission a considéré que de telles pratiques étaient déloyales vis-à-vis des particuliers annonceurs, puisqu'ils n'étaient pas informés de la collecte et de la vente de leur annonce et, par conséquent, ils ne pouvaient pas s'y opposer.
Compte tenu des faits constatés, la formation contentieuse de la CNIL a prononcé, le 26 février 2009, une sanction pécuniaire d'un montant de 40 000 euros à l'égard de la société DIRECTANNONCES. Depuis, DIRECTANNONCES a pris des mesures pour se conformer à la loi et pour permettre aux personnes de s'opposer à la diffusion de leurs données.

Effacement du profil génétique

Monsieur A. est condamné à dix-huit mois de prison en mai 2003 et exécute sa peine. Il s'étonne d'être convoqué par la police, en janvier 2009, pour subir un prélèvement de salive afin d'inscrire son profil génétique dans le fichier national automatisé des empreintes génétiques (FNAEG). Monsieur A. interroge la CNIL sur la légalité de la procédure suivie et notamment sur le délai séparant sa condamnation de cette convocation.
La CNIL interroge alors le ministère de la Justice. S'agissant de Monsieur A., elle rappelle que le Code de procédure pénale prévoit que le prélèvement destiné à alimenter le FNAEG doit intervenir dans le délai maximal d'un an à compter de l'exécution de la peine (jusqu'en novembre 2005 dans son cas).
Le ministère explique en réponse que l'expédition tardive de cette convocation à Monsieur A. est due à une erreur matérielle et que ce prélèvement n'aurait jamais dû être effectué.
Le procureur compétent sollicite donc l'effacement du profil génétique de Monsieur A. du FNAEG.

Gros plan sur ...

Un nouveau partenariat avec le Contrôleur général des lieux de privation de liberté (CGLPL)

La CNIL et le CGLPL, autorités indépendantes, ont décidé de s'apporter un concours mutuel dans la protection des droits fondamentaux des personnes privées de liberté (personnes incarcérées, hospitalisées d'office, placées en centre de rétention administrative ou en centre éducatif fermé, etc.).

La convention de partenariat signée le 2 décembre 2009 prévoit notamment des échanges d'informations.

Lorsque le Contrôleur général, à l'occasion de la visite d'un lieu de privation de liberté ou de l'examen d'une saisine, aura connaissance de fichiers ou traitements informatiques contraires à la loi « Informatique et Libertés », il communiquera à la CNIL les informations nécessaires à son action.

Réciproquement, lorsque la CNIL, à l'occasion de l'instruction d'une plainte, d'un dossier de déclaration ou d'un contrôle, aura connaissance de faits ou de situations susceptibles de porter atteinte aux droits fondamentaux de personnes privées de liberté, elle communiquera au Contrôleur général les informations nécessaires à son action.

La réforme du crédit à la consommation et ses incidences sur le FICP (Fichier national des incidents de remboursement des crédits aux particuliers)

Assurant la transposition de la directive sur le crédit à la consommation du 23 avril 2008 et réformant la procédure de traitement du surendettement, le projet de loi portant réforme du crédit à la consommation actuellement examiné par les assemblées parlementaires comporte plusieurs améliorations du système en vigueur. Il a vocation à définir de façon rigoureuse les conditions d'utilisation et de communication des données contenues dans le FICP.

Ce projet de loi redéfinit les finalités du fichier, prévoit la réduction de la durée d'inscription au FICP des personnes confrontées à des difficultés financières ponctuelles qui respectent leurs engagements, complète la liste de ses destinataires et améliore l'information et l'exercice des droits d'accès et de rectification des personnes qui y sont inscrites. Il instaure également, avant toute signature du contrat de crédit, un contrôle renforcé de la situation du demandeur de crédit et rend obligatoire la consultation par le prêteur du FICP. Celle-ci constitue un élément d'appréciation de la solvabilité de l'emprunteur parmi l'ensemble des éléments d'information dont dispose le prêteur.

L'accélération de la mise à jour des données mises à la disposition des établissements de crédit sera fixée par voie réglementaire. Cet aménagement sera de nature à faciliter le traitement des réclamations des personnes inscrites au fichier. Il y aura, à bref délai, généralisation de la consultation et de la mise à jour en temps réel des données enregistrées dans ce fichier. La CNIL avait en effet, à de nombreuses occasions, attiré l'attention des pouvoirs publics sur les dysfonctionnements du FICP au vu du nombre de plaintes qu'elle reçoit à ce sujet (10% du total des plaintes par an).

De quoi s'agit-il ?

Le FICP

Le Fichier national des incidents de remboursement des crédits aux particuliers a été instauré par une loi du 31 décembre 1989. Sa création participe d'un dispositif d'ensemble de prévention du surendettement, s'inspirant des dispositions applicables aux entreprises en difficulté. Sa gestion a été confiée à la Banque de France.

Le FICP permet d'informer les banques et organismes de crédit, dans le cadre de la gestion du risque de crédit, sur les personnes qui rencontrent des difficultés dans le remboursement d'un crédit. Il comporte les nom, prénom, date et lieu de naissance du débiteur, la nature de l'incident de paiement, le nom de l'organisme ayant procédé à l'inscription, les informations relatives aux procédures de règlement de surendettement et la date de radiation présumée.

Sont inscrites dans ce fichier les personnes qui n'ont pas payé deux mensualités consécutives de leur crédit ou qui sont débiteurs d'un montant du double d'une mensualité ; les personnes qui sont poursuivies en justice pour défaut de paiement ou, lorsqu'il y a déchéance du terme, après une mise en demeure infructueuse ; les personnes qui sont redevables d'une somme d'au moins 500 € depuis plus de soixante jours et qui n'ont pas répondu à une mise en demeure de leur créancier et les personnes qui ont déposé un dossier de surendettement auprès de la Banque de France. Les personnes inscrites dans le fichier ne peuvent pas obtenir de crédit.

De quoi s'agit-il ?

Bâle II

Les établissements financiers ont l'obligation de mettre en place un système de notation des clients afin d'évaluer le risque financier attaché à chacun d'eux. Cette obligation résulte de la directive sur les fonds propres réglementaires transposée par plusieurs arrêtés du 20 février 2007. Il s'agit d'un système de cotation permanente attachée à un client, personne physique, et qui a vocation à être utilisé dans les relations avec le client. Cette logique se différencie des systèmes de «credit scoring » qui ne sont mis en œuvre que pour une opération unique.

Questions à ...

Jean-Paul Amoudry

Sénateur de la Haute-Savoie
Commissaire en charge du secteur «Banques et crédit»

En quoi a consisté la redéfinition des finalités du FICP ?
La finalité principale du fichier est de fournir aux prêteurs un élément d'appréciation sur la solvabilité des personnes qui sollicitent un crédit à des fins non professionnelles. Le fichier devra impérativement être consulté avant toute souscription d'un contrat de crédit au nom des seules personnes qui sollicitent le crédit, afin d'apporter une aide à l'évaluation de leur solvabilité.
Le FICP pourra aussi être utilisé pour calculer la notation individuelle de risque de crédit, dite « note Bâle II » des clients, dans l'optique prudentielle dégagée par le nouvel accord Bâle II.
Enfin, il pourra fournir un élément d'appréciation à l'occasion des décisions d'attribution d'un moyen de paiement, dans un souci de renforcement de l'efficacité du FICP pour lutter contre le surendettement et déterminer les moyens de paiement les plus adaptés à la situation des clients.

Combien de temps les informations seront-elles conservées ?
Le dispositif envisagé simplifie et renforce la cohérence des règles applicables aux données du FICP. Il aura pour effet de réduire très significativement la durée d'inscription au FICP dans le cadre d'un plan de surendettement. Les règles de conservation applicables aux signalements liés au surendettement des personnes seront uniformisées, quelle que soit la mesure adoptée (plan de redressement amiable ou procédure de rétablissement personnel).
La durée de conservation de dix ans applicable à ces inscriptions correspondra à un maximum pour les personnes qui font successivement l'objet d'un plan conventionnel de redressement puis d'une recommandation de la commission de surendettement. Une radiation anticipée sera possible à l'expiration d'un délai de cinq ans si les mesures ont été exécutées sans incident.

Comment sera facilité l'exercice des droits d'accès et de rectification pour les personnes inscrites ?
Il est prévu d'abandonner l'interdiction actuellement en vigueur de toute délivrance par écrit d'informations sur le contenu du fichier. En effet, cette interdiction a fréquemment été perçue par les intéressés comme une gêne à l'exercice de leurs droits d'accès et de rectification. Les personnes inscrites au FICP pourront obtenir communication, notamment par écrit, des données les concernant qui y sont enregistrées.
La Commission sera très attentive à éviter tout risque de détournement de finalité des informations contenues dans le FICP, compte tenu des expériences étrangères en matière de fichiers de solvabilité et des pratiques avérées de demandes de certificats de non-inscription à d'autres fichiers bancaires. De telles demandes proviennent par exemple de bailleurs, d'agences immobilières ou encore d'employeurs, toutes personnes qui ne sont pas habilitées à consulter le fichier mais souhaitent disposer de certificats de solvabilité, ce qui aggraverait encore l'exclusion économique et sociale des personnes inscrites au FICP.

Le droit d'accès indirect aux fichiers de police

En 2009, la CNIL a reçu **2217 demandes de droit d'accès indirect. Ces demandes concernent en général plusieurs fichiers et nécessitent en conséquence de nombreuses vérifications.** Par exemple pour les fichiers de police judiciaire, les magistrats de la CNIL effectuent des vérifications dans le fichier STIC, dans les fichiers de la sécurité publique des commissariats et dans le fichier JUDEX de la gendarmerie nationale.

Bilan des 5712 vérifications effectuées en 2009 permettant de clôturer 2294 demandes

	Nombre de vérifications	% sur le nombre total de vérifications (5712)
Ministère de l'Intérieur	**4279**	**75%**
Police judiciaire – STIC	1385	24%
Fichiers de renseignement	1236	22%
Sécurité Publique-commissariats	1197	21%
Système d'information Schengen	390	7%
Direction de la surveillance du territoire et Direction centrale de la sécurité du CEA	71	1%
Ministère de la Défense	**1433**	**25%**
Police judiciaire de la gendarmerie nationale – JUDEX	1385	24,2%
Direction de la protection de la sécurité de la défense – DPSD	31	0,5%
Direction générale de la sécurité extérieure – DGSE	17	0,3%

Bilan 2009 pour les fichiers de renseignement: 1236 vérifications

		% sur le total des demandes aux fichiers de renseignement «ex-RG» soit 1236
Requérants non signalés dans les fichiers de renseignement	**1037**	84%
Requérants signalés dans les fichiers de renseignement	**199**	16%
Dossier totalement communicable	191	
Dossier non communicable	7	
Dossier partiellement communicable	1	

Comment ça marche ?

En application de l'article 41 de la loi «Informatique et Libertés» toute personne peut demander à la CNIL de vérifier les renseignements qui sont susceptibles de la concerner dans les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique. Les vérifications sont effectuées par les magistrats membres de la Commission et issus du Conseil d'État, de la Cour de cassation ou de la Cour des comptes.
Quels sont les principaux fichiers concernés par cette procédure ?
– les fichiers de police judiciaire (STIC et JUDEX) ;
– les fichiers de renseignement ;
– le système d'information Schengen.

Bilan 2009 pour le fichier de police judiciaire du ministère de l'Intérieur (STIC): 1385 vérifications

Sur les **1385 vérifications effectuées dans le STIC** dans le cadre du droit d'accès indirect, **683 personnes étaient fichées en tant que mises en cause**.

- 17% des fiches des personnes mises en cause ont été supprimées du fichier ;
- 20% des fiches étaient rigoureusement exactes ;
- 63% des fiches ont été modifiées, soit :

– pour traduire les mentions de suites judiciaires favorables (relaxe, acquittement, non-lieu, classement sans suite pour insuffisance de charges ou infraction insuffisamment caractérisée) ;
– pour des requalifications d'incriminations pénales ;
– pour des suppressions partielles d'infractions imputées aux mis en cause.

Cependant, dans la majorité des cas, ces rectifications n'ont pas eu d'incidence sur la durée de conservation des signalements.

Enfin, il convient de relever la carence de nombreux parquets dans la transmission des suites judiciaires nécessaires à la mise à jour du STIC. Ainsi, seulement 32% des 2096 affaires examinées avaient fait l'objet d'une transmission des suites judiciaires.

Ça la fiche mal !

Une absence de mise à jour par les parquets qui conduit au chômage

▶ Monsieur M., 28 ans, avait suivi une formation d'agent de sécurité incendie et avait été recruté par une société de sécurité et de gardiennage. Après un avis défavorable du préfet à la suite d'une enquête administrative, il perd son emploi. Il était en effet enregistré dans le STIC en tant que mis en cause pour des faits de vols de véhicule et d'escroquerie en 1998 et 2004. Les deux affaires avaient été classées sans suite pour infractions insuffisamment caractérisées, mais le fichier n'avait pas été mis à jour. À la suite des démarches de la CNIL, ces informations ont été effacées.

▶ Monsieur B., 30 ans, avait été recruté par une compagnie d'aviation en septembre 2008. L'enquête administrative pour l'obtention d'un titre de circulation pour l'aéroport avait cependant révélé qu'il était enregistré dans le STIC en tant que mis en cause pour une atteinte involontaire à la vie datant de février 2004. Impliqué dans un accident de la route, Monsieur B. avait été reconnu non coupable et relaxé par le TGI de Paris en avril 2005. À la suite des démarches de la CNIL, les informations relatives à Monsieur B. ont été effacées du fichier de police judiciaire mais malheureusement l'emploi avait été pourvu entre-temps.

Un mauvais enregistrement initial des faits qui fait rater une embauche

▶ Monsieur J. devait être recruté par une société privée de sécurité. L'enquête administrative de la préfecture a révélé qu'il avait fait l'objet d'une procédure de violences volontaires. Il était enregistré dans le STIC en tant que victime, notamment pour ces faits de violences volontaires. À la suite d'une erreur, il avait aussi été enregistré en tant que mis en cause. À la demande du TGI, ces informations ont été supprimées du STIC, ce que la CNIL a pu vérifier.

▶ Monsieur R., 49 ans, a été enregistré dans le STIC en 1992 dans une affaire de séquestration, viol et actes de barbarie commis par son frère : en fait il n'était que témoin et a donc été supprimé du fichier.

Un fichage de mineur qui prive de stage

▶ Monsieur P. devait effectuer un stage en tant que steward. L'enquête administrative pour l'habilitation d'accès aux aéroports a révélé qu'il était enregistré dans les fichiers de police judiciaire en tant que mis en cause pour des faits anciens de dégradations de biens publics alors qu'il était mineur et d'implication directe dans une affaire de trafic de stupéfiants. À la suite des démarches de la CNIL, il est apparu que les faits de dégradations n'avaient pas été effacés à l'expiration du délai de cinq ans, et que Monsieur P. n'était pas mis en cause dans l'affaire de stupéfiants. Les mentions relatives aux deux affaires ont été supprimées du fait de l'expiration du délai de conservation pour la première, et d'un enregistrement erroné pour la seconde…

Une requalification des faits ayant une incidence sur la durée de conservation des informations

▶ Monsieur B, qui exerçait dans le domaine de la sécurité incendie depuis près de 20 ans a été convoqué pour un entretien préalable en vue d'un licenciement en raison du refus d'agrément préfectoral qui lui a été opposé. Ce refus était fondé sur son enregistrement dans le STIC pour des faits de « port illégal d'une arme de 6ème catégorie » et de « violences volontaires avec armes ». A la suite des démarches de la CNIL, la qualification de port d'arme a été supprimée et les précisions apportées concernant le nombre de jours d'ITT (incapacité temporaire de travail) pour les violences volontaires ont conduit à la réduction du délai de conservation de 20 à 5 ans et à la suppression immédiate de cette affaire du STIC. Le Préfet en a été informé par les services gestionnaires afin qu'il puisse reconsidérer favorablement la demande d'agrément de Monsieur B.

Le système d'information Schengen (SIS)

Sur les **390 demandes** de droit d'accès indirect au système d'information Schengen traitées par la CNIL et clôturées en 2009, **286 personnes** (soit 73 %) **n'étaient pas signalées** dans ce fichier européen. En revanche, **104 personnes** (soit 27 %) **étaient signalées** et se répartissaient ainsi, suivant l'origine du signalement :
– 67 signalements français ;
– 14 signalements allemands ;
– 12 signalements italiens ;
– 5 signalements espagnols ;
– 6 signalements opérés par le Luxembourg, le Portugal, les Pays-Bas et l'Autriche.

À la suite des vérifications opérées par la CNIL, 16 signalements ont été supprimés du SIS, soit 15 % des 104 personnes fichées (principalement par la France).

De quoi s'agit-il ?

Le SIS

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

INFORMER

La CNIL vous informe au quotidien

Partenariat France Info

La CNIL a renouvelé en 2009 son partenariat avec France Info, initié en octobre 2007. Ce partenariat consiste en un rendez-vous hebdomadaire dans l'émission « Le droit d'info » présentée par Karine Duchochois. Ainsi, chaque vendredi, une chronique répond à une question très pratique, touchant souvent à la vie quotidienne. Cela permet d'aborder de façon pragmatique les droits à la protection des données personnelles et de la vie privée qui sont encore trop méconnus. Cela contribue également à mieux faire connaître les actions de la CNIL dans la défense de ces droits. Au total, ce sont cinquante chroniques qui ont été diffusées en 2009 portant sur des sujets tels que : la prospection par SMS, les passeports biométriques, le vote électronique, l'usurpation d'identité, les PV électroniques, la sécurité des ordinateurs portables, les traces laissées sur internet, etc.

Le premier Prix de thèse « Informatique et Libertés »

Le Prix de thèse « Informatique et Libertés » incite au développement des recherches universitaires concernant la protection de la vie privée et des données personnelles. Ce prix s'adresse à de très nombreuses disciplines telles que les sciences humaines, le droit, les sciences politiques, l'économie mais aussi les disciplines techniques.

Un montant de 7 000 euros est alloué au lauréat afin de faciliter la publication de sa thèse. Huit thèses ont été adressées à la CNIL en 2009.

Le jury, présidé par Jean-Marie Cotteret, membre de la CNIL, a décerné ce premier Prix de thèse « Informatique et Libertés » à Marie-Charlotte Roques-Bonnet pour sa thèse sur « La constitution et l'internet », droit public, université de Toulouse-I.

Cette thèse a été jugée à la fois originale et utile. L'ouvrage est susceptible de susciter l'intérêt de tout juriste, et pas seulement de ceux qui s'intéressent à internet. Les trois parties de l'ouvrage illustrent les unes et les autres l'importance de défis et mutations en cours. En effet, afin d'inscrire la Constitution dans l'environnement numérique et d'appréhender la place de l'internet dans le Pacte social, la thèse réalise une triple observation, en confrontant l'internet aux institutions de la République (partie I), aux droits des citoyens français (partie II) et aux systèmes de normes que protège depuis un demi-siècle notre Constitution (partie III). **L'ouvrage paraîtra en septembre aux éditions Economica.**

Compte tenu de la qualité des travaux proposés, les membres du jury ont également décidé d'attribuer **deux mentions spéciales** décernées à Caroline Lancelot-Miltgen pour « Dévoilement de soi et réponses du consommateur face à une sollicitation de ses données personnelles : une application aux formulaires sur internet », sciences de gestion, université de Paris-Dauphine, ainsi qu'à Julien Le Clainche pour « L'adaptation du droit des données à caractère personnel aux communications électroniques », droit privé, université de Montpellier-I.

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

La CNIL continue son tour de France des régions. Dix-huit régions ont été visitées depuis janvier 2005. Cette initiative de communication de proximité a permis de rencontrer plus de 8 000 personnes : entreprises, administrations, collectivités locales, élus, associations, journalistes, citoyens, avocats, professionnels de la santé et de l'éducation, acteurs sociaux, etc.

En 2009, les agents ou membres de la CNIL ont participé à **127 colloques, séminaires, conférences ou animation de formations** sur la loi « Informatique et Libertés » ou la fonction de correspondant « Informatique et Libertés » auprès d'entreprises, d'administrations, de collectivités locales, d'organisations professionnelles, de grandes écoles, d'universités, en France et à l'étranger. Ce sont en tout près de 200 demandes d'intervention que la CNIL a reçues en 2009.

L'envoi du guide des collectivités locales dans toute la France

En septembre 2009, la CNIL a adressé un exemplaire du guide pratique « collectivités locales » à l'ensemble des communes et collectivités locales, soit plus de 40 000 envois. Cet envoi massif constitue pour la CNIL un investissement important mais il était indispensable pour mieux

sensibiliser les collectivités locales au respect des règles. En effet, les collectivités locales sont amenées à recourir de façon croissante aux moyens informatiques pour gérer les nombreux services dont elle ont la compétence : fichiers de l'état civil, liste électorale, fichiers sociaux, fichiers cadastraux, dispositifs de vidéosurveillance ou de biométrie, fichiers des associations subventionnées, téléservices, administration électronique, usages d'internet, etc.

Lors de nombreuses rencontres avec les représentants des collectivités locales, la CNIL a pu constater que ceux-ci n'étaient pas toujours suffisamment informés de l'importance de ces enjeux, notamment en termes de responsabilité personnelle, civile et pénale.

Enfin, le routage a permis de susciter des désignations de correspondants « Informatique et Libertés » (CIL). Ces désignations montrent aux administrés que la collectivité s'est engagée résolument dans une démarche citoyenne qui va dans le sens d'une meilleure protection de leurs droits. Désigner un CIL permet aussi de mieux préparer la collectivité à un éventuel contrôle et de limiter le risque de sanctions.

Le nouveau site internet www.cnil.fr

En juillet 2009, la CNIL a mis en ligne un nouveau site internet. Nouveau graphisme, nouvelle arborescence, le nouveau cnil.fr souhaite impliquer davantage les citoyens en les informant sur l'exercice de leurs droits au quotidien.

Les messages fondamentaux de la protection des données personnelles sont illustrés à travers des diaporamas qui aident à la compréhension des enjeux par l'image. Le site cnil.fr s'ajuste à la diversité des missions et des activités de la CNIL. La rubrique la CNIL met en avant l'activité de la Commission à travers une actualité riche et un agenda.

La charte graphique et la navigation du site sont repensées autour de grandes rubriques qui placent chacun face à un équilibre entre ses libertés et ses responsabilités. Des informations ciblées sont désormais proposées dans des espaces dédiés à différents publics (citoyens, déclarants, correspondants, élus, presse). Les correspondants « Informatique et Libertés » (CIL) bénéficient d'un extranet qui facilite l'exercice de leurs missions au quotidien (forum, modèles de documents, FAQ…).

En responsabilisant les utilisateurs sur les nouveaux enjeux, et en fournissant des services aux professionnels, le nouveau site cnil.fr offre au plus grand nombre les moyens de s'informer et d'agir.

L'information sur les droits s'est enrichie d'un volet concret « Vos droits en questions ». De nouvelles FAQ répondent aux principales interrogations des citoyens. Le générateur de courriers est complété d'un modèle pour saisir directement la CNIL.

Avec désormais plus de 2 millions de pages vues par mois, cnil.fr construit une relation de proximité et se positionne comme le média de référence en matière de protection des données personnelles et de la vie privée.

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 2009 par l'Ifop sur un échantillon de 1 000 personnes représentatives de la population française.

La notoriété de la CNIL

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

	Juin 2004	Décembre 2009	Évolution 2004/2009
Oui	32	**42**	+ 10
Non	68	58	
	100%	100%	

Le niveau d'information sur les droits

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

	2004	2009	Évolution 2004/2009
Oui, tout à fait	3	7	
Oui, plutôt	18	30	
Sous-total oui	**21**	**37**	**+ 16**
Non, plutôt pas	39	30	
Non, pas du tout	39	25	
Sous-total non	78	55	
Sans opinion	1	8	
	100 %	100 %	

On constate en 2009 une progression sensible du nombre de personnes qui se sentent suffisamment informées à propos de leurs droits ; elles représentent 37 % des Français contre 21 % en 2004 et 33 % en 2008. Cette progression s'explique sans doute par la présence régulière de la CNIL dans les médias à propos de sujets très variés. La problématique de la protection de la vie privée sur internet et la notion de droit à l'oubli ont été assez largement abordées par les médias en 2009. La chronique hebdomadaire sur France Info permet de répondre simplement à des questions qui touchent à la vie quotidienne et d'expliquer de quels droits disposent les personnes. La CNIL s'est orientée depuis quelques années vers une communication plus pratique, que ce soit sur son site, dans ses publications et ses communications (scénarisation de cas concrets, questions/réponses, démonstrations). Plus de 400 demandes d'interview ou de tournages ont généré 500 citations de la CNIL dans la presse audiovisuelle.

La CNIL vous répond au quotidien

C'est le service d'orientation et de renseignement du public (SORP) qui est en première ligne pour répondre aux usagers, qu'ils soient des professionnels ou des particuliers : c'est lui qui reçoit les courriers, les déclarations, les appels téléphoniques et les signalements opérés sur le site internet de la CNIL.

Les courriers

24 880 courriers reçus.

Les déclarations

68 185 déclarations reçues en 2009.

Le succès de la dématérialisation des procédures se confirme : la grande majorité des déclarations se font en ligne sur le site internet de la CNIL :
– pour les déclarations simplifiées : 94 % des déclarations simplifiées ont été faites en ligne en 2009, contre 88 % en 2008. Le délai moyen de délivrance du récépissé est de 48 heures ;
– pour les déclarations normales : 69 % des déclarations normales ont été faites en ligne en 2009, contre 63 % en 2008. Le délai moyen de délivrance du récépissé est de quatre semaines.

Les appels téléphoniques

10 000 appels par mois en moyenne.

C'est votre droit

Droit d'accès, d'opposition et de rectification

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

La boîte à signalements (sur www.cnil.fr)

Ce dispositif, qui est disponible sur le site internet de la CNIL, permet à toute personne de témoigner d'un problème rencontré et d'alerter la CNIL. Ces témoignages ne sont pas des plaintes, mais permettent à la CNIL de se saisir d'un problème ou d'identifier de nouveaux sujets relatifs à la vie quotidienne et qui peuvent poser difficulté au regard de la protection des données.

En 2009, la CNIL a enregistré **2724 signalements**. Le sujet le plus fréquemment abordé est internet (demandes de radiation de réseaux sociaux, phishing, etc.); viennent ensuite les secteurs du marketing (personnes recevant des sollicitations commerciales par messagerie électronique, SMS, ou autre support) et du travail (outils technologiques de surveillance des salariés).

Signalement :

bonjour, je suis abreuvé de sollicitations par .com, un site marchand auquel je ne porte aucun intérêt. j'ai demandé à 3 reprises la radiation de mes coordonnées de leur liste de diffusion et de leur fichier: le 6.3.2010 le 6.4.2010 le 18.4.2010 malgré ces inonctions, j'ai reçu hier une nouvelle publicité. veuillez svp faire respecter mon intimité et cesser le harcèlement de à mon encontre. vous pouvez en mon nom prendre toute mesure disciplinaire que vous jugerez utile. cordialement c. d

Signalement :

bonjour, ma famille et moi-même avons eu le profond désagrément de voir publier sur internet nos informations d'état civil alors même que nous n'avons jamais donné notre accord. nous veillons à préserver notre anonymat sur internet et sommes très en colère surtout que cela concerne aussi nos enfants mineurs. cette pratique de (où l'on peut mettre son arbre en ligne gratuitement et par défaut, celui-ci est accessible à tous) est intrusive et fortement condamnable. je ne comprends pas pourquoi ce n'est pas soumis à l'accord préalable des personnes concernées. cordialement, m b

Signalement :

j'ai demandé un virement de ma banque à la banque de notre nouveau propriétaire pour payer le loyer. ma banque exige d'avoir une copie du bail pour effectuer ce virement. est-ce légal ' après tout, il s'agit de mon argent et non du leur. je suis en droit d'en faire ce que je veux, il me semble

Signalement :

vidéo surveillance en continu du personnel dans se centre de contrôle technique automobile, ainsi que de sa clientelle sans qu'a se jour l'affichage légal ne soit en place.utilisation de cette vidéo par le gérant a fin d'arcélement moral d'un salarié.

CONSEILLER

La CNIL conseille et informe les pouvoirs publics

Tout au long de l'année 2009, notre Commission a poursuivi et renforcé le dialogue qu'elle entretient avec les pouvoirs publics. Le Président de la CNIL a été auditionné à de nombreuses reprises par les principales Commissions des deux Assemblées, par l'Office parlementaire d'évaluation des choix scientifiques et technologiques et dans le cadre de missions et de rapports parlementaires, par des Groupes d'études, sur des projets et des propositions de loi. Les membres de la CNIL ont été auditionnés par le Parlement, sur des thématiques en lien avec leurs secteurs respectifs.

La réforme constitutionnelle votée en 2008 a eu un impact direct sur le nombre des propositions de loi concernant notre Commission, qui se sont multipliées en 2009. Ce foisonnement législatif a conduit la CNIL à être davantage présente au plus près des deux Assemblées. Le nombre des auditions du Président et des commissaires s'est ainsi fortement accru. En 2009, le Président a, pour la première fois, été auditionné par le Groupe UMP de l'Assemblée nationale sur le thème de la protection des données personnelles et par la Commission LIBE du Parlement européen, sur le dossier SWIFT.

Des contacts réguliers ont eu lieu avec les ministères (Justice, Intérieur, Éducation nationale, Santé, Économie numérique, Enseignement supérieur) sur les dossiers communs. En 2009, notre Commission a auditionné en séance plénière Mme Nathalie Kosciusko-Morizet, secrétaire d'État chargée de la prospective et du développement de l'économie numérique et M. Éric Besson, ministre de l'Immigration, de l'Intégration, de l'Identité nationale et du Développement solidaire, afin de connaître les grandes lignes de leurs programmes d'action.

Le Président de la CNIL a rencontré la garde des Sceaux, ministre de la Justice et des Libertés, Mme Michèle Alliot-Marie, pour faire le point sur les fichiers de l'administration pénitentiaire et la mise à jour du STIC par les parquets.

Un rendez-vous avec le ministre de l'Éducation nationale, M. Luc Châtel, a permis au Président de rappeler la nécessité de sensibiliser les publics scolaires à l'internet et d'évoquer la mise en place des correspondants « Informatique et Libertés » au sein de l'éducation nationale. M. Türk s'est entretenu avec le commissaire à la diversité et à l'égalité des chances, M. Yazid Sabeg, sur les statistiques ethniques, sujet sur lequel notre Commission s'est positionnée dès 2007, en présentant une série de soixante recommandations.

Informer le Parlement

• Poursuite de la Lettre d'information à l'intention des parlementaires

Les députés et les sénateurs ont, en 2009, été régulièrement informés sur l'activité de notre Commission par une Lettre, qui a été spécifiquement créée à leur intention, et dont la parution est liée à l'agenda politique et parlementaire. Ce support de communication permet au Président de la CNIL d'exprimer ses préoccupations sur un sujet d'actualité. Deux sujets ont notamment été traités en 2009 : la communication des listes électorales et la biométrie dans les établissements scolaires.

• Les auditions

Le Président de la CNIL a été auditionné par :
– l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur les nanotechnologies ;
– la commission des Lois de l'Assemblée nationale, sur les sujets d'actualité de la CNIL ;
– le député Charles de La Verpillière sur le projet de loi organique relatif à l'application du cinquième alinéa de l'article 13 de la Constitution ;
– les députés Delphine Batho et Jacques-Alain Bénisti sur la proposition de loi relative aux fichiers de police ;
– le député Éric Ciotti sur le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure ;
– les sénateurs Anne-Marie Escoffier et Yves Detraigne sur le thème « Traçage électronique et protection de la vie privée » ;
– le sénateur Christian Cointat sur la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique des sénateurs Anne-Marie Escoffier et Yves Detraigne ;
– les commissions des Affaires européennes de l'Assemblée nationale et du Sénat et par la commission des Libertés civiles, de la Justice et des Affaires intérieures du Parlement européen sur SWIFT ;
– la commission des Affaires européennes du Sénat sur le groupe d'experts chargé de réfléchir à la révision

de la directive de 1995 sur la protection des données personnelles ;
– le Groupe UMP de l'Assemblée nationale dans le cadre du groupe de travail sur « L'éthique du numérique ».

Les membres de la Commission ou les services ont été auditionnés par :
– les députés Franck Riester, Patrick Bloche et Bernard Gérard sur le projet de loi favorisant la diffusion et la protection de la création sur internet (HADOPI) ;
– le député Georges Pau-Langevin sur la proposition de loi relative à la lutte contre les discriminations liées à l'origine ;
– le député Jacques Grosperrin concernant la mission d'information sur les écoles de la deuxième chance et l'accès à l'emploi ;
– le député Olivier Jardé sur la proposition de loi relative aux recherches sur la personne ;
– les députés Claude Birraux et Pierre Lasbordes sur le dossier médical personnel ;
– le député Jean-François Lamour sur le projet de loi relatif à l'ouverture à la concurrence et la régulation du secteur des jeux d'argent et de hasard en ligne ;
– les députés François Loos et Éric Diard sur le projet de loi relatif à la consommation ;
– le député Arnaud Robinet sur la proposition de loi tendant à permettre le recours au vote à distance par voie électronique lors des élections des membres des conseils des établissements à caractère scientifique ;
– le sénateur Alain Dufaut sur le dopage ;
– le sénateur Yves Detraigne sur la décision-cadre relative à l'utilisation des données des passagers à des fins répressives ;
– le sénateur Philippe Marini sur le projet de loi relatif au crédit à la consommation ;
– les sénateurs Fabienne Labrette-Ménager et Denis Jacquat sur le surendettement ;
– le sénateur François Trucy sur le projet de loi relatif à l'ouverture à la concurrence et la régulation du secteur des jeux d'argent et de hasard en ligne ;
– les sénateurs Annie David, Jean-Claude Peyronnet et Hugues Portelli sur le programme de Stockholm.

Sensibiliser les pouvoirs publics

Revoir la composition du groupe d'experts européens chargés de réviser la directive de 1995 sur la protection des données personnelles

En 2009, notre Commission s'est fortement mobilisée contre la composition du groupe d'experts chargé d'engager la réflexion sur la révision de la directive européenne de 1995, mis en place par la Commission européenne. En effet, ce groupe était composé de cinq personnes qui, pour quatre d'entre elles, étaient issues soit de sociétés américaines, soit de cabinets d'avocats dont les principaux établissements étaient également basés aux États-Unis. Or il s'agissait, pour ce groupe d'experts, d'envisager une modification de la directive qui constitue précisément le cadre juridique protecteur des droits individuels des citoyens européens en matière de données personnelles. Le Président de la CNIL a rapidement appelé l'attention du Vice-président de la Commission européenne, du Premier ministre, des ministres concernés et des parlementaires sur ce point. Le groupe a finalement été dissous et M. Jacques Barrot a lancé une consultation des différentes « parties prenantes » sur ce sujet.

SWIFT

La mise en place d'un système de surveillance, par les autorités américaines, des transferts bancaires internationaux transitant par la société SWIFT a, en juin 2006, suscité de vives réactions des instances européennes, du Groupe des CNIL européennes et de notre Commission. Au printemps 2007, des garanties ont été négociées par la Commission européenne et le Conseil européen avec le Gouvernement américain : la création d'un centre de stockage sur le territoire européen et la nomination d'une personnalité européenne – M. Jean-Louis Bruguière – chargée de veiller au bon fonctionnement du programme de surveillance. Or de nouvelles négociations se sont ouvertes entre la Commission européenne et les États-Unis permettant aux autorités américaines d'avoir finalement accès aux données stockées par SWIFT sur le serveur en

Suisse. De plus, la CNIL n'a pu avoir accès au rapport rendu par M. Bruguière, le rapport ayant été classifié par les autorités américaines. Notre Commission s'est, une fois encore, fortement engagée sur ce dossier : le Président de la CNIL a adressé un courrier au Premier ministre, aux ministres concernés, ainsi qu'à M. Jacques Barrot. Notre Commission a fortement mobilisé les députés européens français en les informant des menaces que ferait peser, sur les libertés et la protection des données personnelles, un tel accord. La Commission LIBE et le Parlement européen ont finalement rejeté cet accord, début 2010.

De quoi s'agit-il ?

SWIFT *(Society for Worldwide Interbank Financial Telecommunication)*

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

Les initiatives parlementaires pour réviser la loi « Informatique et Libertés »

L'année 2009 a été marquée par plusieurs initiatives parlementaires visant à réviser la loi « Informatique et Libertés ».

Fin 2008, la commission des Lois du Sénat a confié aux sénateurs Anne-Marie Escoffier et Yves Détraigne **une réflexion sur le respect de la vie privée à l'heure des mémoires numériques**. Il s'agissait ainsi de conduire une étude sur les « technologies de traçabilité » capables de pister les individus dans l'espace (biométrie, vidéosurveillance, géolocalisation, nanotechnologies, réseaux sociaux …) et dans le temps (cas des moteurs de recherche capables d'agréger des données éparses pour établir le profil de millions de personnes …), technologies susceptibles de brouiller la frontière entre vie publique et vie privée, voire de porter atteinte au droit à la vie privée.

Les recommandations qu'ils ont formulées dans leur rapport d'information, publié au nom de la commission des lois le 27 mai 2009, ont été traduites pour partie dans une proposition de loi déposée au Sénat le 6 novembre 2009. Ce texte devrait être examiné par le Parlement au cours de l'année 2010.

La proposition de loi propose tout d'abord de donner une plus grande effectivité au droit à l'oubli numérique, en renforçant l'obligation d'information sur la durée de conservation des données et en facilitant l'exercice du droit de suppression notamment sur internet.

Par ailleurs, il s'agit de rendre obligatoires les correspondants « Informatique et Libertés » lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel et que plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre.

Mais le texte vise aussi à conforter les pouvoirs de contrôle et de sanction de la CNIL en lui permettant notamment de prononcer des sanctions financières d'un montant plus important. Il renforce ses possibilités d'actions juridictionnelles : à l'égal de la Halde, la Commission pourrait présenter ses observations devant les juridictions.

En outre, la proposition de loi tend à rendre obligatoire, pour les responsables de traitements, l'information de la CNIL en cas de violation de l'intégrité ou de la confidentialité de ces traitements, afin de les inciter à mettre en œuvre les mesures de protection adéquates. La CNIL pourra ensuite, en cas d'atteinte portée aux données d'une ou plusieurs personnes physiques, exiger des responsables de traitement qu'ils avertissent ces personnes. Cet article transpose ainsi une disposition de la directive « Vie privée et communications électroniques » du 25 novembre 2009.

Enfin, le texte a également pour objet de modifier le régime d'encadrement des fichiers de police.

La proposition de loi relative aux fichiers de police, déposée par les députés Delphine Batho et Jacques-Alain Bénisti s'inscrivait, elle, dans la continuité des conclusions du rapport d'information sur les fichiers de police présenté par les mêmes parlementaires en mars 2009. Ce rapport appelait à une refonte du cadre juridique régissant la création et le fonctionnement desdits fichiers. La proposition de loi entendait ainsi confier au seul législateur la faculté de créer des fichiers de police et prévoyait, pour ce faire, de modifier les dispositions de la loi du 6 janvier 1978, modifiée par la loi du 6 août 2004, en particulier son article 26. Elle a été rejetée en novembre 2009.

Cette réforme de l'encadrement des fichiers de police a cependant été reprise, mais selon des modalités différentes, par le député Jean-Luc Warsmann, président de la commission des lois de l'Assemblée nationale, dans le cadre, cette fois-ci de la proposition de loi de simplification et d'amélioration du droit. Ce texte a été adopté en première lecture en décembre 2009.

Questions à ...

Claude Domeizel

Sénateur des Alpes-de-Haute-Provence
Commissaire en charge du secteur
« Développement durable et logement »

En tant que parlementaire mais aussi membre de la CNIL, quel regard portez-vous sur ces initiatives ?

De telles initiatives témoignent bien sûr de l'intérêt accru que porte le Parlement aux questions de protection des données. Elles démontrent surtout qu'à l'heure du monde internet, du phénomène des réseaux sociaux et de l'explosion, bientôt, des nanotechnologies, il est aujourd'hui nécessaire que le législateur apporte de nouvelles réponses aux défis technologiques et sociétaux qui nous sont ainsi lancés.

Il ne s'agit pas, bien entendu, de remettre en cause les « fondamentaux » de la protection des données, qui restent plus que jamais valides, ou l'action de la CNIL, qui a fait la preuve de son efficacité. Il s'agit en revanche de déterminer si le cadre juridique actuel ne mérite pas d'être renforcé et adapté, compte tenu des bouleversements intervenus ces dernières années (et à venir !).

Comme vous le savez, des initiatives sont lancées pour faire évoluer le cadre juridique communautaire – et à terme international – dans ce domaine. Il est donc tout à fait essentiel que notre pays, patrie des Droits de l'homme et qui a été en 1978, un des premiers à se doter d'une loi « Informatique et Libertés » soit à nouveau précurseur. Notre Parlement a plus que jamais un rôle moteur à jouer.

La CNIL a-t-elle contribué à ces initiatives ?

Oui. Tout d'abord, notre Commission, depuis déjà quelques années, a souhaité renforcer et systématisé le dialogue avec le Parlement afin de mieux le sensibiliser aux enjeux de la protection des données. Ceci s'est traduit notamment par le fait que le Président de la CNIL est désormais auditionné chaque année par les commissions des lois des deux assemblées et par l'office parlementaire des choix scientifiques et technologiques. Ces auditions sont autant d'occasions d'évoquer les problématiques auxquelles est confrontée la CNIL qu'il s'agisse du droit à l'oubli sur internet, de la mise à jour des fichiers de police, du manque de sensibilisation des jeunes aux risques liés à internet... En outre, le Président et selon le cas, un membre de la Commission, sont régulièrement auditionnés dès lors qu'une mission d'information, un projet ou une proposition de loi concerne le domaine de la protection des données.

Par ailleurs, notre Commission, estimant que sa contribution pouvait être utile au débat, a décidé de s'autosaisir et de prendre position sur des textes qui la concernent directement. En juin 2009, elle a ainsi fait part aux députés Batho et Bénisti de ses observations. Et notre Commission devrait prochainement en faire de même en ce qui concerne la proposition de loi des sénateurs Detraigne et Escoffier.

Un acteur privilégié : le CIL

Un nouveau métier en plein essor

Fin 2009, près de 6 000 **organismes** avaient désigné un correspondant « Informatique et Libertés » (CIL). Ce chiffre démontre que, quatre ans après l'entrée en vigueur du décret permettant de désigner un CIL, cette nouvelle fonction tend à s'imposer dans notre paysage professionnel. Il s'agit désormais d'un métier connu et reconnu. Le Conseil national des barreaux a d'ailleurs modifié son règlement intérieur pour faciliter l'exercice de cette fonction par les avocats. De même, des formations diplômantes préparant aux missions de CIL ont également vu le jour.

Après examen, le premier constat qui s'impose est que le CIL séduit avant tout les entreprises. Sur les 6 000 organismes ayant désigné un CIL, **plus de 90 % sont des entreprises du secteur privé**. Il s'agit aussi bien de grandes entreprises telles que Michelin, Safran, Thalès ou Vinci que de PME/PMI. Tous les secteurs d'activité sont représentés.

Pourtant, l'intérêt d'avoir un CIL est tout aussi réel pour les administrations. C'est pourquoi la CNIL a renforcé ses actions de sensibilisation et de communication auprès des administrations et des collectivités locales. La Commission a ainsi signé une convention de partenariat avec l'Association des Maires de Meurthe-et-Moselle afin notamment de développer des actions pédagogiques auprès des élus et des agents des collectivités locales. L'objectif est d'étendre cette initiative à d'autres départements et régions.

Un avantage technique, éthique et compétitif

Les motifs pour lesquels un organisme désigne un correspondant ont évolué au fil des ans. Initialement, la première motivation était la possibilité de bénéficier d'un allégement des obligations en matière de formalités préalables des traitements ordinaires et courants. En effet, en présence d'un CIL, seuls les traitements identifiés comme sensibles par la loi demeurent soumis à autorisation et continuent à faire l'objet de formalités.

Désormais, cinq arguments supplémentaires ressortent des raisons pour lesquelles il est utile de disposer d'un CIL :

1. Un vecteur de sécurité juridique

Le CIL permet de garantir la conformité des organismes à la loi « Informatique et Libertés ». Cette maîtrise des risques juridiques est d'autant plus importante que certains manquements à celle-ci sont pénalement sanctionnés.

2. L'assurance d'un accès personnalisé aux services de la CNIL

Les CILs disposent :
– d'ateliers de formation sur huit thèmes différents (sécurité, biométrie, RH…) ;
– d'une ligne téléphonique et d'une adresse électronique dédiées qui leur permettent d'obtenir rapidement des réponses personnalisées à leurs demandes de conseil ;
– d'un extranet proposant des outils exclusifs ;
– d'un suivi de l'état d'instruction de l'ensemble de leurs demandes adressées à la CNIL (courriers, demandes d'avis, plaintes …).

3. Une source de sécurité informatique

Parmi les missions du CIL, celui-ci doit s'assurer que toutes les précautions utiles ont été prises pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des personnes non autorisées y aient accès.

4. La preuve d'un engagement éthique et citoyen

La désignation d'un correspondant témoigne de l'engagement de l'organisme en faveur du respect de la vie privée et des droits des personnes dont les données sont traitées.

5. Un outil de valorisation du patrimoine informationnel

En s'assurant de la fiabilité des données traitées, le CIL garantit la possibilité de céder, transmettre ou louer les fichiers détenus par l'organisme dans le respect de la loi « Informatique et Libertés ».

Un avenir assuré ?

Compte tenu du nombre d'organismes ayant fait le choix de désigner un CIL, le bilan apparaît dès à présent positif. Cette analyse se trouve d'ailleurs confortée par la proposition de loi des sénateurs Détraigne et Escoffier, « visant à mieux garantir le droit à la vie privée à l'heure du numérique », qui a notamment pour objectif de rendre le CIL obligatoire.

Cette obligation reposerait néanmoins sur des critères destinés à ne pas mettre en difficulté les entreprises ou les collectivités de petites tailles. En effet, outre le fait qu'elles ne disposent pas toujours des moyens humains ou financiers nécessaires pour désigner un CIL, elles mettent rarement en œuvre des traitements sensibles au regard de la loi « Informatique et Libertés ».

Seraient ainsi concernés, les organismes qui recourent à un traitement de données à caractère personnel auquel plus de cinquante personnes ont directement accès ou participent à sa mise en œuvre.

Si cette disposition de la proposition de loi venait à se concrétiser, la philosophie de l'actuelle loi « Informatique et Libertés » en serait modifiée. Le contrôle *a priori* effectué par la CNIL dans le cadre de l'instruction des dossiers de déclaration serait encore réduit au profit de l'accompagnement et de la formation des CIL.

Focus sur l'extranet CIL

Au cours de l'été 2009, la CNIL a ouvert un extranet exclusivement dédié aux correspondants « Informatique et Libertés ». Les CIL disposent ainsi d'un identifiant et d'un mot de passe qui leur permettent de se connecter depuis le site www.cnil.fr à ce nouveau service en ligne. Cet extranet leur donne notamment accès à :
– des forums de discussion pour échanger entre CIL et avec la CNIL ;
– des outils pratiques sous forme de modèles de lettres, de fiches techniques, de FAQ … ;
– un annuaire des CIL afin de fédérer la communauté et de créer de nouveaux réseaux.
Cette initiative témoigne de la volonté de la CNIL de toujours mieux accompagner et favoriser le développement des CIL.

Les CIL en chiffres

- **1 466 correspondants représentant 6 000 organismes**
- **23 sessions de formation réalisées en 2009**
- **350 participants**
- **1 700 demandes de conseil**
- **3 600 appels par an**

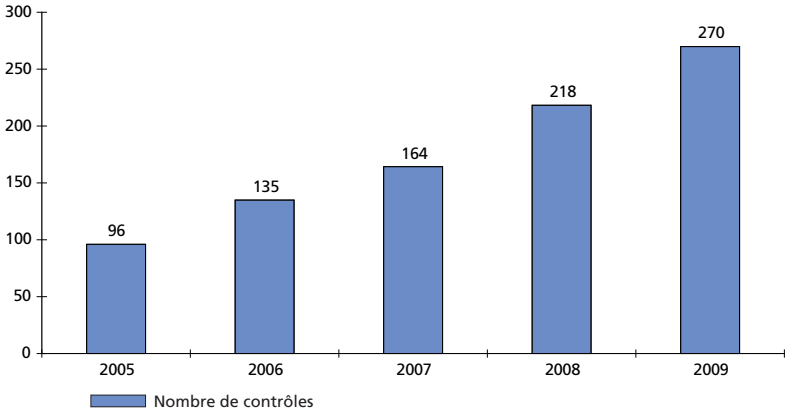
CONTRÔLER/SANCTIONNER

Contrôler

2009 aura confirmé l'importance croissante des contrôles dans les missions de la CNIL, tant au regard du nombre de contrôles effectués, que des secteurs contrôlés de plus en plus variés. La CNIL a mis en place de nouvelles procédures pour faire suite aux évolutions jurisprudentielles concernant son activité.

270 contrôles ont été effectués en 2009, soit **une augmentation de près de 24 %** par rapport à 2008. L'augmentation soutenue du nombre de contrôles réalisés n'est pas un phénomène nouveau et témoigne de la volonté de la CNIL de s'inscrire pleinement dans la philosophie de la loi de 2004 qui privilégie le contrôle sur place des fichiers, au bénéfice des personnes dont les données sont traitées.

Le graphique ci-dessous démontre l'évolution croissante du nombre de contrôles menés par la CNIL :



Comme elle l'avait annoncé, la CNIL a veillé à être présente sur l'ensemble du territoire national afin de pouvoir vérifier la correcte application de la loi par les responsables de fichiers, où qu'ils se trouvent. La carte (page 49) témoigne des efforts de la CNIL en ce sens.

L'origine et la diversité des thématiques des contrôles effectués soulignent, une nouvelle fois, la compétence généraliste d'une autorité de protection des données comme la CNIL.

La première source des contrôles opérés s'inscrit dans **la mise en œuvre du programme annuel** des contrôles (31 % des contrôles effectués) adopté par la formation plénière. Le programme 2009 des contrôles aura été très largement respecté. Ainsi plus de quarante contrôles ont été effectués dans le cadre de la révision de la recommandation sur le recrutement. Ils concernent aussi bien de grands groupes français, que des cabinets de recrutement étrangers ou encore de petites entreprises qui se sont lancées sur ce marché.

Le contrôle du fichier des personnes recherchées (FPR) mis en œuvre par le ministère de l'Intérieur est sur le point de s'achever et aura conduit la Commission à contrôler tous les types d'organismes susceptibles d'interroger ce fichier : commissariats de police, brigades de gendarmerie, mairies, préfectures, etc.

Les dispositifs de télébillettique utilisés sur l'ensemble du territoire sont restés sous surveillance constante de la CNIL, qui a multiplié les contrôles dans ce secteur. Enfin, on peut citer également le contrôle des quelques sociétés utilisant le marketing dit « ethnique », afin de vérifier les conditions de collecte de données parfois sensibles.

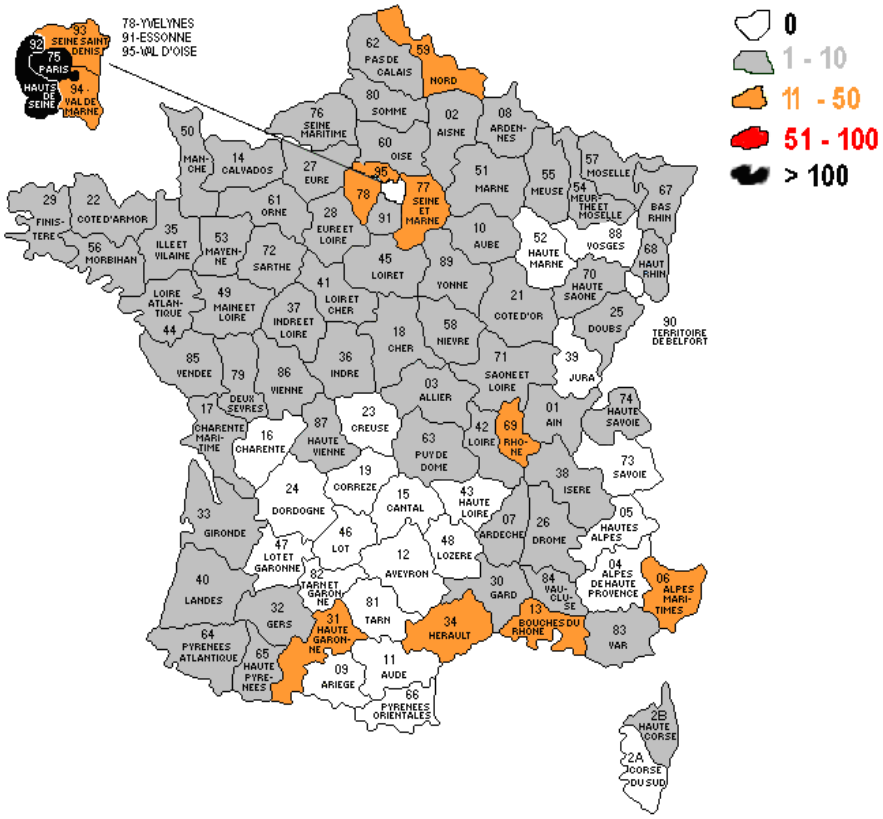
Les quelques thématiques qui n'ont pu être abordées (dispositifs de *pay-as-you-drive* pour les assurances automobiles, le dispositif GAM du ministère de la Justice, etc.) le seront en 2010.

Le deuxième axe fort est la réalisation de contrôles sur le fondement des plaintes reçues par la CNIL. **25 % des contrôles réalisés en 2009 ont ainsi été décidés dans le cadre de l'instruction des plaintes** et ont permis d'apprécier la réalité des faits portés à la connaissance de la CNIL par les plaignants.

De nombreux contrôles (11 %) sont décidés afin de vérifier **le respect des engagements pris à la suite d'une mise en demeure** adoptée par la formation restreinte de la Commission à l'encontre d'un organisme qui ne respectait pas les dispositions de la loi.

Les autres contrôles effectués (33 %) témoignent de la diversité des actions de contrôle : réaction à des sujets portés à la connaissance de la CNIL (par exemple, contrôle d'un fichier d'exclusion des agriculteurs par un hypermarché), vérification des formalités préalables effectuées auprès de la CNIL ou encore contrôle des dispositifs biométriques et de géolocalisation. La CNIL a également été amenée, par ses contrôles, à porter une attention

Répartition géographique des contrôles depuis 2005



toute particulière au respect de la loi par certaines études d'huissiers chargées du recouvrement des amendes pour le compte du Trésor public.

L'année écoulée aura été également marquée pour la CNIL par **deux décisions du Conseil d'État** en date du 6 novembre 2009 qui a estimé que le responsable des lieux où se déroule une mission de contrôle devait être préalablement informé de son droit à s'opposer au contrôle.

Ces décisions ont conduit la CNIL à modifier sa pratique en matière de contrôle sur place : dorénavant, il est systématiquement procédé à l'information des organismes contrôlés. Dès lors que la CNIL se verra opposer un refus, elle saisira le juge aux fins de se voir délivrer une ordonnance lui permettant de procéder au contrôle.

La CNIL a pris attache avec la Chancellerie pour envisager une modification de la loi « Informatique et Libertés » afin de permettre au président de la CNIL d'obtenir du juge une autorisation préalable au contrôle.

En tout état de cause, les possibles conséquences contentieuses de ces décisions expliquent que seuls 22 % des contrôles effectués en 2009 ont été examinés par la formation restreinte.

Vu dans les fichiers !

[illegible]	12h-18h30 4 jours enfant de 3,5 ans 15,104h, 95 Aged s'occuper de mes 2 enfants scolarisés à partir du 28 aout 2006 tous les jours 15h50-19h,mercredi 8h30-19h,a l'ai tres chiante, connait les contrats de travail.. 15 €, Aged, 95 par mail	320553754101
[illegible]	1 enfant de 6 ans,gen pr devoirs,etudiant,pas genant si garçon,fermeté ms sympa,sortie CLIENTE REMBOURSEE !	357969060021

France	mess le 12/05 pr [illegible]	
France	Message 26/05/08, pas d'exp de garde d'enfants sauf famille	
FRANCE	NULL	
france	vieille, chiante dès les premiers instants !!!!!!!!!!	
	NULL	

Sanctionner

Les procédures engagées devant la formation restreinte (commission des sanctions) de la CNIL auraient dû connaître en 2009 une nouvelle progression à deux chiffres, comme c'était le cas depuis plusieurs années maintenant. Les décisions, évoquées plus haut, du Conseil d'État du 6 novembre 2009, remettant en cause le déroulement des contrôles opérés par la Commission, ont conduit à reporter ou annuler plusieurs dizaines de procédures qui n'ont pu être adoptées. En volume donc, le nombre de mises en demeure reste inférieur à 2008 (90 contre 126) ainsi que le nombre de procédures de sanctions (10 contre 13).

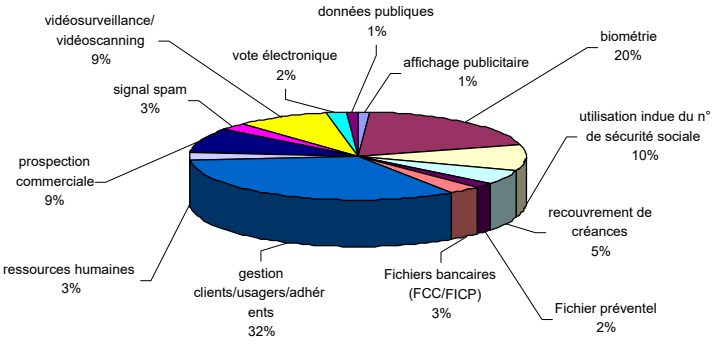
Le rythme d'activité de la formation restreinte reste néanmoins important et le taux de mise en conformité élevé puisque le nombre de procédures clôturées à l'issue des mises en demeure est quasi identique à 2008, soit 85%. L'année 2009 s'illustre également par la mise en œuvre, pour la première fois, des procédures d'urgence prévues par la loi, d'une part, pour mettre en demeure un organisme sous huit jours de corriger des manquements à la loi et, d'autre part, pour engager une procédure d'interruption d'un traitement en raison de la détection d'une faille de sécurité majeure.

Les principaux secteurs d'activité dont les dossiers ont pu être examinés par la formation restreinte de la CNIL restent identiques depuis trois ans maintenant, à savoir le secteur du commerce et des prestataires de services, ainsi que les secteurs de la téléphonie et d'internet. Ce sont toujours les sollicitations commerciales abusives ainsi que la mauvaise gestion des fichiers clients (refus de droits d'accès ou d'opposition) qui génèrent ce classement. À noter, que le secteur public (administrations d'État et collectivités locales) représente plus de 10% des procédures engagées par la formation restreinte en 2009.

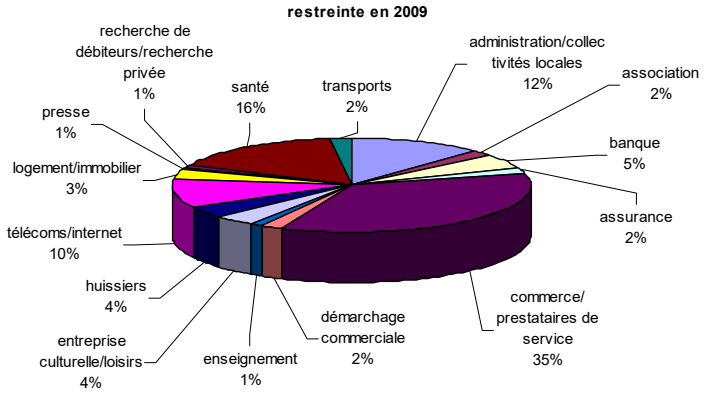
L'opérateur rennais des transports en commun sanctionné pour les conditions restrictives de mise en place du passe anonyme

Après avoir constaté de véritables obstacles à la souscription d'un passe anonyme dans les transports rennais, la Commission a adressé, en janvier 2009, un avertissement public à la société Keolis Rennes, exploitant ce réseau. En effet, il n'était possible de « charger » sur le passe anonyme que des tickets à l'unité (pas d'abonnement). Le passe anonyme revenait ainsi entre 2,5 et 4 fois plus cher que le passe nominatif. En outre, la très faible information diffusée par la société sur son existence ne permettait pas une promotion égale des deux types de cartes. Seuls 53 passes anonymes avaient été distribués au jour du contrôle contre 186650 passes nominatifs. La formation restreinte

Typologie des principaux dossiers présentés en formation restreinte en 2009



Typologie des principaux secteurs d'activité présentés en formation restreinte en 2009



de la CNIL a estimé que le respect de la vie privée et de la liberté d'aller et venir anonymement impliquait que les voyageurs disposent d'un véritable choix entre des déplacements anonymes ou nominatifs, ce qui suppose que ceux-ci soient réalisés dans des conditions commerciales équivalentes. Parallèlement, la Commission a mis en demeure la société de remédier à cette carence. Les mesures prises devraient entrer en vigueur prochainement.

La CNIL met de l'ordre dans les pratiques des « pigistes immobiliers »

Les sociétés de pige immobilière compilent les annonces immobilières de particuliers sur internet, en vue de leur revente à des professionnels, principalement des agences immobilières. Suite à l'amende de 40000 euros à l'encontre de la société DIRECTANNONCES (voir page 34), la CNIL va maintenant veiller à ce que l'ensemble des pigistes immobiliers permettent aux personnes de s'opposer à la revente des annonces qui les concernent.

Pas de vidéosurveillance des salariés

La formation restreinte de la CNIL a prononcé, en avril 2009, une sanction pécuniaire d'un montant de 10000 euros à l'encontre de la société de prêt-à-porter

Jean-Marc-Philippe. Il est apparu que le système de vidéo-surveillance n'était pas conforme à la loi « Informatique et Libertés », en plaçant les salariés sous surveillance constante et permanente sous couvert de lutte contre les vols.

Zéro pointé pour un site de notation

Le site de notation palmares.com affichait, quant à lui, la volonté de permettre aux internautes de noter les avocats, les médecins ou les chefs d'entreprises, ainsi que des personnalités publiques telles que des joueurs de football ou des membres du gouvernement. Ce site soulevait des difficultés similaires au regard de la loi « Informatique et Libertés », à savoir un défaut d'information des professionnels concernés sur leurs droits et une collecte déloyale des données. Mis en demeure de se conformer à la loi, la société Servtel, éditrice du site palmares.com, a informé la Commission qu'elle cessait cette activité. Par ailleurs, le site Note2bib, qui souhaitait noter les médecins, a également cessé son activité quelques jours après son lancement, ses concepteurs ayant pris conscience très tôt de l'illégalité de leur site au regard de la législation relative à la protection des données personnelles.

Néanmoins, de nouveaux sites apparaissent régulièrement, obligeant la formation restreinte de la CNIL à rester très vigilante.

Des huissiers peu rigoureux

Un contrôle de la CNIL a permis de mettre en évidence une faille de sécurité majeure au sein d'un fichier d'un groupement parisien d'huissiers, effectuant du recouvrement d'amendes. Il était, en effet, possible d'accéder par internet à ce fichier et de connaître le nom des clients ainsi que le montant de l'amende à recouvrer. Averti, l'organisme n'a pas réagi, ce qui a conduit la Commission à engager en avril 2009, pour la première fois, une procédure d'interruption de ce traitement dans l'attente de la mise en œuvre de mesures garantissant sa sécurité. Dans le délai des quinze jours, requis par la loi afin de recueillir ses observations, le groupement a corrigé la faille.

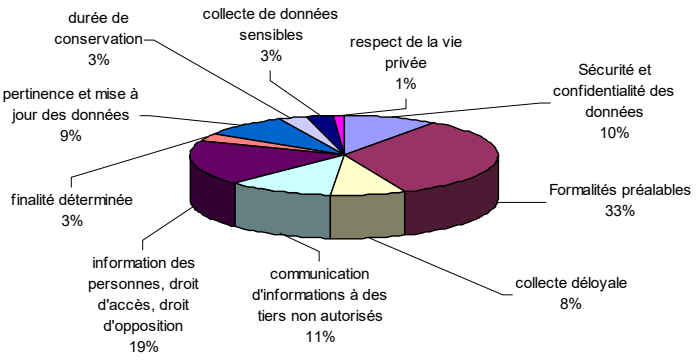
À Montpellier, ce sont deux études d'huissiers à l'encontre desquelles a été prononcée, en juillet dernier, une sanction de 10 000 euros, notamment pour n'avoir pas cessé d'enregistrer des commentaires litigieux sur leurs débiteurs. De nombreuses mentions relatives à la santé des personnes ou à des infractions avaient été relevées dans les fichiers des deux études.

Les manquements les plus importants à la loi Informatique et Libertés ont évolué par rapport à 2008. L'absence de formalités préalables ou le non-respect de celles effectuées a concerné en 2009 un tiers des procédures engagées, marquant ainsi une forte progression.

Ça la fiche mal !

- « vieil hystérique violent »
- « idiot fini »
- « deb en maladie cancer avec métastase »
- « fréquent séjour prison pr pb drogue »
- « deb serait alcoolique »
- « vit dans taudis »

Typologie des principaux manquements de fond constatés par la formation restreinte en 2009



Si les problèmes liés à l'information des personnes et à l'exercice des droits d'accès, de rectification ou d'opposition restent à un niveau élevé, tout comme les manquements à la sécurité et à la confidentialité des données, la communication d'informations à des tiers non autorisés a aussi augmenté.

La vigilance des responsables de fichiers sur la transmission de telles informations doit donc redoubler. Les autres manquements à la loi relevés restent sensiblement dans des proportions identiques à celles des années précédentes.

Trois recours à l'encontre de décisions de la formation restreinte de la Commission ont été engagés, en 2009, par des organismes sanctionnés. Les deux décisions du Conseil d'État évoquées précédemment ont conduit à remettre en cause toutes les procédures de la formation restreinte engagées sur la base des contrôles « viciés », soit une centaine de procédures.

Les chiffres

de la formation restreinte

- **91 mises en demeure**
- **5 sanctions financières pour un montant de 75 000 euros**
- **4 avertissements**

ANTICIPER

La CNIL accompagne le développement technologique pour qu'il respecte la vie privée

La CNIL accompagne les entreprises et les pouvoirs publics dès la conception de leurs systèmes. À travers son rôle de conseil et lors de l'examen des dossiers de formalités, la Commission peut être amenée à inciter les entreprises ou les pouvoirs publics à modifier leur système, à utiliser des solutions techniques alternatives ou à prévoir des garanties pour la protection des données des personnes. Citons quelques exemples.

Dans le domaine de la santé, la CNIL participe au comité de pilotage chargé de mettre en place le nouvel identifiant de santé, qui sera la pierre angulaire du futur Dossier médical personnel de chacun. Elle fait également partie du comité du RGI (Référentiel général d'interopérabilité), publié le 12 juin 2009, qui est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration.

Suite aux études menées l'année dernière sur les dispositifs biométriques de reconnaissance du réseau veineux du doigt, une biométrie considérée sans trace, la CNIL a adopté en mai 2009 une autorisation unique relative à ces dispositifs.

Les contrôles

Afin de concilier développement technologique et respect de la vie privée, la CNIL a contrôlé plusieurs traitements mettant en œuvre des nouvelles technologies à des fins notamment marketing. Ainsi, elle a contrôlé les panneaux publicitaires numériques mis en place par la Régie publicitaire des transports parisiens métrobus. Ces panneaux peuvent diffuser des publicités et mesurer l'audience des spots publicitaires. La CNIL a considéré qu'un traitement de données à caractère personnel, soumis à la loi

Questions à ...

Dominique Richard

Consultant
Commissaire en charge du secteur «Affaires culturelles et sportives»

En quoi la CNIL est-elle concernée par la lutte contre le dopage ?
La lutte contre le dopage nécessite la constitution de différents fichiers, pouvant recenser de multiples informations sur les athlètes (localisation des sportifs de haut niveau, résultats d'analyses sanguines ou urinaires, sanctions prises contre les fraudeurs, etc.). L'alimentation de ces fichiers implique le traitement de données à caractère personnel et donc l'application de la loi «Informatique et Libertés».

Pourquoi les sportifs sont-ils suivis «à la trace» ?
Pour rendre plus efficace la lutte contre le dopage, il est apparu nécessaire de pouvoir réaliser des contrôles inopinés, ce qui n'est possible que si les contrôleurs sont en mesure de localiser le sportif à tout moment de la journée, et ce, même hors du cadre des compétitions. Pour ce faire, l'Agence française de lutte contre le dopage (AFLD) demande aux athlètes de l'informer, trois mois à l'avance, de leurs emplois du temps.

Seuls les sportifs de haut niveau peuvent être soumis à cette contrainte de localisation et tout refus de se soumettre à ces contrôles peut entraîner des sanctions. Par exemple, un sportif ayant refusé de fournir des informations sur sa localisation pourra être exclu des prochaines compétitions.

Quel est le rôle concret de la CNIL dans ce dispositif ?
La CNIL est attentive aux conditions dans lesquelles sont mis en œuvre ces fichiers. Elle s'assure tout particulièrement du respect des droits des personnes prévus par la loi «Informatique et Libertés» et de l'efficacité des mesures de sécurité et de confidentialité des données.
Saisie de plaintes par des syndicats de sportifs professionnels, la CNIL a créé un groupe de travail, procédé à de nombreuses auditions et abouti à des recommandations à destination des acteurs concernés afin de les informer de leurs obligations et de leurs droits.
Par ailleurs, comme il existe une base de données mondiale regroupant au Canada les données sur les sportifs de haut niveau, la CNIL est également intervenue au niveau du groupe des CNIL européennes dans une perspective d'harmonisation des règles relatives à ces fichiers de lutte contre le dopage.
Le G29 a d'ailleurs émis un avis réservé sur les conditions de transmission de ces données hors de l'Union européenne.

« Informatique et Libertés », était mis en œuvre. En effet, même si le système ne conserve que des données statistiques, il n'en demeure pas moins que ces statistiques sont effectuées à partir d'images qui comportent des visages et donc des données à caractère personnel.

Aujourd'hui, ces systèmes ne font que compter le nombre de personnes ayant regardé l'écran. Mais en cas d'évolution vers une « vidéoanalyse » des caractéristiques des personnes (sexe, âge, taille, etc.), la Commission serait amenée à étudier la légitimité de la finalité de ces nouveaux traitements. Elle examinerait alors également la pertinence des données collectées et les possibilités pour les personnes d'exercer leur droit d'opposition.

Par ailleurs, la CNIL a contrôlé des dispositifs utilisant la technologie Bluetooth pour envoyer des offres publicitaires ou des informations publiques sur des téléphones mobiles. Le but de ces contrôles était de s'assurer des mesures de sécurité mises en œuvre et que seules les personnes réellement intéressées par ce type d'offres étaient sollicitées. C'est le cas, par exemple, lorsqu'elles doivent approcher leur téléphone à quelques centimètres d'une borne car le consentement s'exprime alors par un geste physique.

Normalisation et standards

En 2008, la CNIL avait rejoint le GC SSI (Groupe de la coordination de la sécurité des systèmes d'information) en charge de la normalisation de la sécurité à l'AFNOR (Agence française de normalisation), dans le but de se positionner comme un acteur incontournable de la normalisation dans des domaines clés de la protection des données. Ce groupe élabore les positions françaises sur les projets de normes ISO (International Standardisation Organisation).

Il est essentiel pour la CNIL de participer à ces travaux dans la mesure où les normes internationales permettent notamment d'attester du respect par un organisme de certaines bonnes pratiques. S'agissant de la protection des données, la CNIL doit donc s'assurer que les modèles français et européen de protection de la vie privée sont bien pris en compte au moment de l'élaboration de ces instruments.

L'ISO développe actuellement des projets de normes dans le cadre de la protection de la vie privée et de la protection des données personnelles. Elle travaille depuis 2005 sur un projet de norme appelé ISO 29100 « Privacy Framework » (cadre de protection de la vie privée) qui détermine des exigences et une terminologie communes en matière de protection de la vie privée à l'échelle internationale. Il s'agit d'un document fondateur qui pourrait à terme servir de référence à d'autres normes.

Comme la structure et les principes de ce projet de norme apparaissaient en retrait et souvent en contradiction avec les standards européens, le Président de la CNIL a mobilisé en urgence le G29 et la Commission européenne sur cette question au mois de juin 2009. Le G29 s'est pleinement mobilisé sur cette question et la CNIL a coordonné l'élaboration de commentaires avec ses homologues européens, ainsi qu'avec ses interlocuteurs industriels ou institutionnels à l'AFNOR. De plus, le Vice-président de la Commission européenne, Monsieur Jacques Barrot, a soutenu l'initiative du G29 et le report souhaité par les autorités de protection afin d'assurer une pleine conformité avec la réglementation européenne.

Pour la première fois, en novembre 2009, un représentant de la CNIL a participé à l'une des réunions internationales biannuelles du groupe chargé de l'élaboration de cette norme à l'ISO. Les contributions de la CNIL et de ses homologues du G29 ont ainsi pu être prises en compte pour la préparation d'un nouveau projet qui sera examiné fin avril 2010 et sur lequel la Commission continuera de se mobiliser *via* l'AFNOR et le G29. L'ISO a d'ailleurs souligné son intérêt pour les contributions des autorités de protection des données en exprimant le souhait de formaliser une « liaison » avec le G29.

Toutefois, face au nombre de normes et de domaines comportant une dimension relative à la protection de la vie privée, il est devenu nécessaire d'envisager les moyens d'améliorer la veille, le suivi et la coordination de l'élaboration des normes.

Au niveau national, la CNIL a collaboré sur ces questions avec l'AFNOR et le secrétariat d'État à la prospective et au développement de l'économie numérique.

Au niveau international, l'ISO à décidé de mettre en place un comité d'orientation sur la vie privée (Privacy Steering Committee, PSC) afin de mieux coordonner ses activités dans le domaine de la vie privée. Consciente de l'importance stratégique et transversale de ce comité, la CNIL a obtenu qu'un de ses représentants fasse partie de la liste des experts intégrant le PSC, dont la première réunion aura lieu en février 2010.

De quoi s'agit-il ?

L'ISO

L'organisation internationale de normalisation (ISO ou *International Standardisation Organisation*) est le premier organisme en matière de production et de publication de normes internationales. ISO est un réseau d'agences nationales de normalisation de plus de 150 pays avec un secrétariat central basé à Genève, qui coordonne le système. L'impact des normes et des certifications ISO jouit d'une très forte influence au sein du secteur privé.

Les nouvelles applications biométriques

De quoi s'agit-il ?

La reconnaissance faciale

La reconnaissance faciale permet de reconnaître un individu en analysant les caractéristiques de son visage et en les comparant à des données préenregistrées. Ces dispositifs peuvent notamment être utilisés dans certaines applications de contrôle d'accès ou pour reconnaître une personne sur une photo ou une vidéo. Dans certaines conditions, il est même techniquement possible d'identifier un individu dans une foule à partir d'images de vidéosurveillance. Si cette technologie n'en est qu'à ses balbutiements, il importe de comprendre que son caractère intrusif est croissant puisque la liberté d'aller et venir anonymement pourrait à terme être remise en cause.

La reconnaissance du réseau veineux

Le dessin que forme le réseau veineux à l'intérieur d'un doigt ou à l'intérieur de la paume de la main est propre à chaque individu. Cette caractéristique est maintenant exploitée dans des dispositifs biométriques de contrôle d'accès physique ou logique.
Par rapport à l'empreinte digitale, la CNIL considère que cette technologie présente un avantage particulier car il s'agit d'une technologie « sans trace ». En effet, nous laissons tous des « traces » de nos empreintes digitales sur les objets que nous touchons. En revanche, nous ne laissons aucune « trace » de notre réseau veineux. Son utilisation présente donc des risques réduits de détournement ou de falsification.
Suite aux travaux d'expertise qui ont été réalisés en 2008 sur ce sujet, la CNIL a adopté en juillet 2009 une autorisation unique concernant les dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main dont la finalité est le contrôle de l'accès aux locaux sur les lieux de travail.

Questions à …

Jean-François Carrez

Président de chambre honoraire
à la Cour des comptes
Commissaire en charge du secteur
« Éducation et enseignement supérieur »

Pour quelles raisons l'organisme GMAC a-t-il souhaité recourir à un système biométrique pour lutter contre la fraude à l'examen ?
Parce que le danger de fraude le menace particulièrement : GMAC est un organisme américain qui administre un examen mondial appelé « GMAT », qui permet aux candidats les mieux classés d'intégrer des grandes écoles de commerce et de gestion comme HEC ou l'ESSEC en France, ou Harvard aux États-Unis. Les enjeux pour les candidats sont donc considérables. Cet examen est organisé dans le monde entier, et les candidats de toutes les nationalités peuvent se présenter dans les centres d'examen de leur choix, dans n'importe quel pays. Cet examen est donc susceptible de faire l'objet de tentatives de fraude, en particulier par la substitution de candidats munis de faux documents d'identité. Ainsi, en 2004, ont été détectées six personnes, qui avaient passé l'examen dans plusieurs pays à la place d'au moins 186 candidats, malgré les contrôles d'identité classiques opérés à l'entrée des centres d'examen. Il s'agit de faux candidats « professionnels » qui avaient proposé de passer l'examen à la place du véritable candidat en échange d'une rémunération de 3 000 dollars. Selon le GMAC, ce phénomène de fraude se serait considérablement développé au cours des dernières années.

La CNIL avait-elle déjà autorisé le recours à un système biométrique pour lutter contre la fraude à un examen ?
Non, c'est la première fois que la CNIL autorise un tel dispositif. Je tiens à insister sur le fait que l'autorisation accordée à GMAC en juin 2009 ne signifie pas que la CNIL est, de façon générale, favorable à l'utilisation de bases biométriques centralisées pour empêcher la fraude aux concours et examens.

Pourquoi alors la CNIL a-t-elle autorisé le GMAC à utiliser ce dispositif ?
La CNIL a autorisé ce dispositif à la faveur de deux arguments principaux.
En raison d'abord de la nature très particulière de cet examen, qui s'apparente à un « concours mondial », pour lequel les risques de fraude à l'identité sont élevés, et donc pour lequel des contrôles très rigoureux sont absolument indispensables.
La seconde raison tient à la technologie biométrique utilisée. Le dispositif proposé analyse l'image du réseau veineux à l'intérieur de la paume de la main. Il s'agit de ce que la CNIL appelle une biométrie « sans trace ». En effet, contrairement à une photographie du visage ou une empreinte digitale, il est difficile de capter l'image du réseau veineux d'un individu sans sa participation. En l'état actuel de la technique, cette biométrie présente des risques réduits de capture des données à l'insu des personnes et donc d'usurpation d'identité. Les responsables de GMAC se sont d'ailleurs engagés à généraliser le dispositif autorisé en France reposant sur le réseau veineux. Il remplacera le dispositif actuel, reposant sur la collecte des empreintes digitales, qui a été mis en œuvre depuis 2006 dans de nombreux autres pays organisant cet examen.

C'est nouveau, ça vient de sortir !

– Pour quelques dollars de plus, une application téléchargée sur votre smartphone vous permet de savoir si votre rendez-vous galant est recommandable. Cette application récupère les informations à partir d'une base de données dont les informations proviennent des palais de justice, et bureaux gouvernementaux américains ainsi que des profils publics de Facebook, Twitter et MySpace. Tapez son nom et vous saurez tout de votre futur partenaire !

– Wamiz, le Facebook des animaux qui propose aux amis des animaux un réseau social avec des profils d'animaux et de maîtres.

– Seppukoo, le réseau antisocial qui propose un suicide virtuel par désabonnement aux déçus de Facebook. Le slogan dit : « Impressionnez vos amis, déconnectez-vous ! »

– « Il est où le doudou du bébé ? » Grâce à un nouveau gadget composé de deux boîtiers en plastique, dont l'un se fixe sur le doudou, il suffit d'appuyer sur l'autre boîtier pour localiser le doudou. Chaque doudou possède un numéro d'identifiant qui peu être enregistré par les parents sur le site du fabricant, ce qui permet de retrouver un doudou perdu.

– Quand Google se mêle de la consommation électrique. Aux États-Unis, Google propose de relier son compteur électrique numérique à son ordinateur *via* le moteur de recherche.

– Y a-t-il une vie après la mort sur internet ? La question de l'accès aux comptes de réseaux sociaux d'une personne décédée pose question. Les sites proposent des réponses aux familles qui souhaitent accéder aux contenus mis en ligne par les défunts, ou commander un CD des mails de la personne disparue.

– Un quartier animé de Berlin, par un soir printanier. Thomas, s'installe dans son bar habituel et sort son téléphone mobile, un smartphone connecté à internet. Il sait en un instant tous les détails de la vie de sa voisine de droite, elle aussi connectée sur le réseau Aka Aki.

– Vous êtes célibataire et utilisateur de Vélib ? Le site Vélibataire vous permet de faire des rencontres en géolocalisant les habitués de votre station !

– Le site « Please Rob Me », vous propose de savoir quelles maisons sont vides dans votre entourage afin de pouvoir mieux les cambrioler. Derrière une vraie blague, ce site nous rappelle les risques éventuels de la localisation.

C'EST ARRIVÉ PRÈS DE CHEZ NOUS !

La surveillance des salariés

▶ En Allemagne, on a retrouvé dans la poubelle d'une station-service des mini-dossiers médicaux concernant plus de 600 salariés du groupe de magasin discount Lidl. Ces dossiers comportaient des commentaires du type « veut un enfant, échec de la fécondation artificielle », « opération d'une tumeur sans gravité ». À la suite de cette affaire, qui faisait déjà suite à des pratiques d'espionnage systématique des employés par des détectives privés, le groupe a licencié son directeur.
Le président de la Deutsche Bahn a, lui, démissionné après la révélation de mise sous surveillance d'un millier de responsables de la compagnie. Les comptes bancaires des 173 000 salariés étaient également croisés avec ceux des 80 000 sociétés partenaires dans le cadre de la lutte anticorruption.

Les citoyens britanniques sous surveillance

▶ La société britannique Internet Eyes a annoncé en octobre qu'elle proposerait à des volontaires de regarder les images prises par les caméras de vidéosurveillance depuis leur ordinateur et de signaler d'éventuels délits. Le signalement d'un délit permet d'accumuler des points qui se transforment à la fin en argent.

▶ Le gouvernement britannique a annoncé vouloir réduire la délinquance juvénile grâce à la surveillance permanente des 2 000 familles posant le plus de problèmes. Un système de vidéosurveillance les surveillera 7 jours sur 7 et 24 heures sur 24 pour contrôler si les enfants vont à l'école, s'ils se couchent à l'heure et font bien leurs devoirs.

▶ C'est enfin la création d'un fichier des 11,3 millions de Britanniques qui s'occupent d'enfants, soit un adulte sur quatre qui a été annoncée pour octobre. Sont concernés les enseignants, les infirmières, les médecins, les assistantes maternelles, les proviseurs mais aussi les dentistes.

La perte ou la revente de données personnelles

▶ L'Information Commissioner's Office (ICO), l'équivalent britannique de la CNIL, a annoncé en novembre 2009 qu'il avait ouvert une enquête sur la transmission de données de clients T-Mobile au Royaume-Uni. Des employés de l'opérateur auraient revendu à des concurrents des informations portant sur des milliers de leurs abonnés, principalement la date de fin de contrat. Ces clients étaient contactés peu avant la fin de leur contrat pour leur proposer de changer d'opérateur.

L'arroseur arrosé

▶ La perte de contrôle des données publiées sur internet concerne tout le monde, y compris ceux qui prétendent pourtant que les internautes contrôlent tout et qu'il n'y a aucun risque.

▶ En novembre 2009, le responsable mondial de la protection des données d'un mastodonte de l'internet s'agaçait sur son blog que les informations qu'il y publiait aient été réutilisées contre lui dans le cadre des poursuites dont il fait l'objet en Italie.

▶ Puis en décembre, c'est le PDG d'un grand réseau social américain qui a été victime des changements de sa propre politique de confidentialité : pendant quelque temps, ses photos personnelles sont devenues accessibles à tous. Comme lui, de nombreux internautes se sont d'ailleurs laissés surprendre par ces nouvelles règles.

▶ On comprend mieux pourquoi George Clooney déclarait en septembre dernier : « Je préférerais me faire examiner la prostate en direct à la télé [...] qu'avoir une page sur Facebook. »

LES DÉFIS

LE FUTUR DE LA VIE PRIVÉE

Quel futur pour la vie privée ?

En mai 2009, M. Barrot, Vice-président de la Commission européenne, a organisé une **conférence** intitulée « Données personnelles : plus d'usage, plus de protection » réunissant les grands acteurs de la protection des données. À l'issue de cet événement, M. Barrot a lancé une **consultation publique** afin d'obtenir des contributions relatives aux nouveaux défis en matière de protection des données personnelles et à l'amélioration du cadre juridique au sein de l'Union européenne.

Le groupe de l'Article 29 et le groupe Police-Justice ont ainsi mis à profit leur expérience et leur expertise pour livrer un avis qui prend en compte **l'impact de l'entrée en vigueur du traité de Lisbonne au 1er décembre** et réaffirment leur soutien aux principes fondateurs de la directive, toujours valides.

Cet avis présente des propositions pour améliorer les outils et les pratiques existants. Citons, entre autres, la volonté de développer des mesures pratiques à l'attention de l'individu notamment par une **meilleure lisibilité de ses droits** et la mise en place de moyens d'action concrets à sa disposition pour les exercer.

Il s'agit aussi d'élever la protection des données dans l'entreprise au rang des valeurs éthiques communes et partagées et de renforcer l'efficacité concrète des actions entreprises par les responsables de traitement pour démontrer leur conformité aux textes juridiques applicables (par exemple : audits, études d'impact sur la vie privée, désignation de correspondants à la protection des données …).

Un premier pas vers des standards internationaux

Lors de la Conférence mondiale des commissaires à la protection des données qui s'est tenue à Madrid du 4 au 6 novembre 2009, les représentants de près de quatre-vingts autorités de protection des données, parmi lesquelles la CNIL, **ont à l'unanimité voté une résolution** qui établit des standards internationaux sur la protection des données personnelles et de la vie privée.

Questions à …

Georges de la Loyère

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

Peut-on qualifier ce premier pas vers les standards d'historique ?

Oui, car les autorités sont parvenues à élaborer un corpus de principes communs adaptés aux dernières évolutions technologiques. La résolution, adoptée à Madrid, définit les grands principes de protection des données, énonce les droits dont bénéficient les individus, ainsi que les obligations incombant aux personnes et organisations traitant des données personnelles. Elle précise également les procédures internes à mettre en place au sein des entreprises et administrations à l'échelle mondiale.

Quelle est la prochaine étape pour ces standards internationaux ?

Le groupe de travail, auquel la CNIL participe, va continuer ses efforts et étudier la deuxième étape de la procédure. Cette étape pose la question de la valeur juridique des standards internationaux, ainsi que les problématiques de droit applicable et de contrôle par les autorités de protection des données.

Comment le gouvernement français a réagi à l'adoption de ces standards et à la réflexion sur la révision de la directive européenne ?

Le Premier ministre, François Fillon, a indiqué à Alex Türk qu'il partageait sa préoccupation de voir réaffirmer au niveau international les principes importants qui régissent la protection des données. Il considère que les évolutions technologiques actuelles, leur interopérabilité et leur mondialisation rendent nécessaires ces réflexions. Avec le soutien du Premier ministre, il va désormais falloir s'organiser ensemble afin d'avancer sur l'encadrement concret et l'utilisation de ces standards.

Il s'agit d'un premier pas essentiel attendu depuis plusieurs années tant par les organisations de défense des libertés et des droits individuels que par les entreprises.

Une longue marche s'engage désormais pour parvenir à une définition commune de la **valeur juridique contraignante de ces principes**. À ce stade, les pouvoirs publics de l'ensemble des pays concernés auront à prendre des initiatives de façon à mettre en place un instrument juridique international ayant valeur de droit positif.

C'est pourquoi le Président de la CNIL a adressé début novembre cette résolution au Premier ministre en soulignant que la prise en compte de ces principes fondamentaux de données personnelles constituera, dans la société numérique dans laquelle nous entrons, la seule garantie future de l'exercice de nos libertés fondamentales.

Pour une approche francophone de la protection des données personnelles

La CNIL au service de la promotion d'une « culture Informatique et Libertés » au sein de la Francophonie

L'Association francophone des autorités de protection des données personnelles (AFAPDP), dont la CNIL assure le secrétariat général, se veut un outil au service d'une volonté politique axée sur la modernité et les droits de l'homme, dans le droit fil des engagements pris par les chefs d'État et de gouvernement de la Francophonie.

Le chemin qui mène à la reconnaissance et à l'effectivité de ce droit passe par la mise en œuvre d'un cycle vertueux : sensibiliser les parties prenantes par le partage des expériences, au cours, par exemple, de conférences notamment régionales et lors de la conférence annuellement dédiée à cette problématique en Francophonie ; contribuer au déclenchement de la décision de mettre en chantier l'élaboration d'une législation au moyen de visites auprès des autorités nationales ; mettre à disposition les textes internationaux de référence, des experts et des structures de dialogue dans la phase législative ; accueillir et coopérer avec les autorités nouvellement installées ; organiser des stages et des formations sur les bonnes pratiques aux fins de professionnalisation.

Une tribune pour l'espace francophone

Le Président de la CNIL s'est pleinement engagé en 2009, notamment au travers de l'AFAPDP, pour initier et consolider les actions favorisant cette dynamique positive. L'AFAPDP a organisé, grâce au soutien de l'Organisation internationale de la francophonie, la troisième Conférence francophone annuelle des commissaires à la protection des données personnelles, qui s'est tenue à Madrid en novembre 2009. Cette Conférence a offert une tribune unique aux 30 délégations représentant des pays francophones et des organismes internationaux. Elle a permis de sensibiliser et partager des expériences avec les États francophones dépourvus, pour le moment, de législation sur la protection des données personnelles mais également d'initier la mise en place d'un partenariat avec le réseau ibéro-américain de protection des données.

L'émergence d'un espace francophone de protection des données

L'espace francophone a su prendre la pleine mesure de l'urgence, face à l'émergence d'un monde des nouvelles technologies sans frontières, de faire évoluer, partout dans le monde, un corpus de règles protectrices de la vie privée et des données personnelles. Aussi tous les pays francophones du Nord sont désormais dotés d'une loi sur la protection des données. Mais, depuis 2004, le mouvement s'intensifie également dans les pays du Sud. Le Burkina Faso, en 2008, a ouvert la voie avec la mise en place de son autorité. Le Bénin, le Maroc, l'île Maurice, le Sénégal et la Tunisie ont adopté une loi sur la protection des données personnelles et les autorités de protection des données se mettent actuellement ou sont d'ores et déjà en place. Dans de nombreux autres pays francophones, des projets sont en gestation, notamment en Égypte, au Gabon ou encore à Madagascar.

Ce mouvement vers une reconnaissance mondiale du droit fondamental à la vie privée s'étend désormais vers d'autres régions francophones. Aussi la CNIL, notamment en la personne de sa vice-présidente, Isabelle Falque-Pierrotin, et l'AFAPDP ont largement participé à la Conférence régionale sur le droit des technologies de l'information et de la communication qui s'est tenue en novembre à Hanoi au Vietnam. Cette conférence a été l'opportunité unique de sensibiliser les pays francophones de la région, à savoir le Cambodge, le Laos, la Thaïlande et le Vietnam, sur la nécessité de mettre en place un cadre pour la protection de la vie privée. Certains de ces pays ont d'ores et déjà des projets en cours pour développer une loi en matière « Informatique et Libertés ».

Vers un renforcement des compétences

La CNIL et l'AFAPDP entendent également constituer une plateforme pour favoriser le renforcement des compétences au sein de la Francophonie et divers projets sont actuellement mis en œuvre. Aussi l'AFAPDP a engagé, avec le soutien et en étroite collaboration avec l'Organisation internationale de la francophonie, un ambitieux partenariat sur la protection de la vie privée des enfants et a mis en place un groupe de réflexion sur l'élaboration d'un instrument international sur la protection des données.

L'AFAPDP poursuit de plus sa collaboration avec le Conseil de l'Europe, notamment pour l'élaboration d'une recommandation sur le profilage.

Enfin, l'année 2010 sera également celle de la mise en place d'un programme de stages collectifs, qui permettra de réunir des experts francophones du monde entier pour favoriser l'échange d'expériences et de bonnes pratiques sur des thématiques précises.

De quoi s'agit-il ?

AFAPDP

L'Association francophone des autorités de protection des données personnelles a été créée en 2007 (présidence québécoise, vice-présidences burkinabé et suisse, secrétariat général assuré par la CNIL).

Les membres votant sont les autorités de protection des données, les membres observateurs sont l'OIF, de droit, et les représentants des États non dotés de l'autorité de protection des données qui le souhaitent.

Son objectif : promouvoir le droit universel à la protection des données personnelles en renforçant les capacités de ses membres, en réfléchissant aux nouveaux enjeux, en fournissant une expertise à l'appui des travaux législatifs et des normes internationales.

Conférence régionale sur le droit des technologies de l'information et de la communication, Hanoi, novembre 2009.

L'ÉCHANGE D'INFORMATION À L'HEURE DE LA MONDIALISATION

De quoi s'agit-il ?

Les BCR

BCRs signifie « Binding Corporates Rules ». Il s'agit de règles internes applicables à l'ensemble des entités de l'entreprise qui contiennent les principes-clés en matière de traitement de données personnelles permettant de régir les transferts de données à la fois au sein et hors du groupe, à l'intérieur et à l'extérieur de l'Union européenne.
Pour les transferts hors de l'Union européenne, ces BCRs sont une alternative au Safe Harbor (qui ne vise que les transferts vers les États-Unis) ou aux clauses contractuelles types adoptées par la Commission européenne. Elles doivent garantir qu'une protection équivalente à celle octroyée par la directive européenne de 1995 s'applique aux données personnelles transférées hors de l'Union européenne.

Les BCR, une alternative aux clauses contractuelles types

Face au nombre croissant de transferts de données, les entreprises multinationales reconnaissent peu à peu les BCR comme une véritable alternative aux clauses contractuelles types permettant d'assurer **un niveau de protection adéquat** aux données transférées hors de l'Union européenne. En effet, les BCR sont des **codes de conduite** qui définissent la politique interne d'un groupe en matière de transferts de données personnelles hors de l'Union européenne.

La CNIL, en tant que rapporteur du sous-groupe de travail BCR au G29, participe largement au succès des BCR. Plusieurs documents ont ainsi été adoptés par le G29 afin de constituer une boîte à outils reprenant les critères déterminants et obligatoires pour obtenir la validation des BCR par les autorités de protection des données.

Par ailleurs, afin de rendre l'adoption de ces BCR plus efficace et plus rapide, une procédure dite de **reconnaissance mutuelle** a été mise en place, aux termes de laquelle, l'instruction des BCR menée par l'une des autorités européennes de protection des données de ces pays vaut instruction pour les autres. À la fin de l'année 2009, **dix-neuf autorités** avaient adhéré à cette procédure : l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, l'Espagne, la France, la Grande-Bretagne, l'Islande, l'Irlande, l'Italie, la Lettonie, le Liechtenstein, le Luxembourg, Malte, la Norvège, les Pays-Bas, la République tchèque, la Slovénie.

En 2009, **la CNIL, en tant qu'autorité de coordination, a instruit les BCR des sociétés Sanofi Aventis, Michelin et Safran** qui ont été reconnus par l'ensemble des autorités européennes de protection comme offrant des garanties suffisantes pour encadrer les transferts hors de l'Union européenne. Par ailleurs, la CNIL coordonne actuellement la rédaction des BCR de **sept autres entreprises.** Il est intéressant de noter que de nombreux secteurs de l'industrie sont ainsi représentés : secteur pharmaceutique, secteur aéronautique, secteur pétrolier, transport maritime, industrie du luxe, nouvelles technologies, banque assurance.

En 2010, la **CNIL devrait également recevoir plus de dix nouveaux BCR** coordonnés par d'autres autorités européennes de protection des données.

De quoi s'agit-il ?

Discovery

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

Quel cadre juridique pour les procédures de Discovery

La procédure de Discovery correspond à la phase d'investigation et d'instruction préalable au procès civil et commercial essentielle pour toute action en justice aux États-Unis. Dans ce cadre, les demandes de communi-

cation auprès des entreprises peuvent être très larges (et notamment porter sur les courriers électroniques des salariés français) et le refus d'obtempérer peut aboutir à un jugement défavorable aux États-Unis. La CNIL a constaté la multiplication des cas de communication de données de la France vers les autorités judiciaires américaines dans le cadre de ces procédures de « Discovery ».

Face à cette situation, **le G29**, groupe des CNIL européennes, a adopté un document de travail en février 2009 auquel la CNIL a contribué de façon significative. Cet avis européen a été prolongé par une délibération de la CNIL du 23 juillet 2009 portant recommandation afin de répondre aux demandes pressantes des entreprises engagées dans des procès aux États-Unis. Reconnue pour son caractère concret, cette délibération rappelle le cadre juridique dans lequel ces demandes américaines doivent s'inscrire : **respect de la loi** « Informatique et Libertés »**, de la convention de La Haye et de la loi du 26 juillet 1968 dite « loi de blocage »**. Il s'agit de la loi relative à la communication de documents ou renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères réglementant la communication d'informations à des autorités étrangères. Elle prévoit que, « sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci ». Le non-respect de cette disposition est sanctionné par une peine d'emprisonnement de six mois et/ou par une amende de 18 000 €.

La loi « Informatique et Libertés » s'applique aux procédures de Discovery dès lors qu'elles impliquent des traitements et des transferts de données personnelles. Cependant, il n'est pas nécessaire de procéder à des déclarations spécifiques Discovery, les données concernées par ces traitements ayant précédemment dû faire l'objet de déclarations pour leurs finalités principales (gestion RH…). Les flux internationaux de données doivent pour leur part faire l'objet de déclarations ou le cas échéant d'autorisations à la CNIL.

Par ailleurs, les principes de protection des données personnelles s'appliquent aux procédures de Discovery : légitimité du traitement et respect du secret professionnel, proportionnalité des données (filtrage des données au niveau local), durée de conservation des données, mesures de sécurité à mettre en place, respect des droits et information des personnes, règles relatives aux conditions de transferts internationaux de données.

S'agissant de ces transferts, la recommandation de la CNIL apporte des solutions à la fois lorsque les données sont localisées en France puis transférées aux États-Unis, mais également dans l'hypothèse où les données ont déjà été transférées aux États-Unis pour une autre finalité légitime et préalablement autorisée.

Le développement de l'externalisation

L'externalisation par les entreprises de certaines de leurs activités par le recours à la sous-traitance est aujourd'hui de plus en plus fréquente. Elle est « offshore » quand elle concerne la création ou l'utilisation d'une entité juridique dans un autre pays ; elle a alors souvent pour but la recherche d'une réduction des coûts, notamment fiscaux, financiers ou salariaux. L'externalisation offshore est synonyme de délocalisation, lorsqu'elle s'accompagne du transfert d'une activité préexistante en France. Mais qui est responsable dans un tel schéma économique ? Quelle est la responsabilité du destinataire des données ? Comment encadrer ces transferts vers l'étranger ?

Devant le constat d'un tel développement de l'externalisation offshore, la CNIL a constitué un groupe de travail chargé d'étudier cette problématique sous l'angle de la protection des données personnelles. Après avoir auditionné les grands acteurs du secteur (clients, prestataires, cabinets d'avocats), un rapport complet a été présenté aux membres de la CNIL afin de faire le point sur les questions posées par l'externalisation hors de l'Union européenne des traitements informatiques et de proposer des solutions.

En ce qui concerne le désengorgement du système d'autorisation, le traitement des demandes d'autorisations de transferts va être accéléré grâce à la nouvelle procédure mise en place suite à l'adoption de la loi du 12 mai 2009 de simplification et de clarification du droit et d'allégement des procédures. En effet, la Commission composée des dix-sept commissaires peut désormais déléguer ce pouvoir d'autorisation à son président et son vice-président délégué. En revanche, les dossiers de transferts sensibles continueront à faire l'objet d'un passage en séance plénière devant l'ensemble des commissaires.

De quoi s'agit-il ?

Le Cloud Computing

Le Cloud Computing (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (Cloud) composé de nombreux serveurs distants interconnectés. D'un point de vue « Informatique et Libertés », ce concept soulève des problématiques de sécurité, de qualification des parties, de droit applicable, d'exercice effectif des droits et d'encadrement des transferts internationaux de données personnelles.

Questions à …

Didier Gasse

Conseiller maître à la Cour des comptes
Commissaires en charge du secteur
« Télécommunications et internet »

La CNIL a-t-elle pris une position au sujet du « Cloud Computing » ?

La CNIL étudie cette notion et ses applications sous l'angle de la protection des données. En effet, ce concept soulève des problématiques liées à la qualification des parties (notamment la qualification du prestataire de Cloud Computing : responsable de traitement ou sous-traitant), le droit applicable, l'exercice effectif des droits par les personnes concernées (accès, modification, suppression), l'encadrement des transferts de données personnelles, et à la sécurité des données.
Elle devrait émettre des recommandations pratiques à destination des clients des prestataires de Cloud Computing courant 2010.

Quelles sont les conclusions du groupe de travail relatif à l'externalisation mis en place par la CNIL ?

Ces travaux ont permis au groupe de travail de mettre en avant deux nécessités : celle d'aider les entreprises à qualifier leurs rôles et leurs responsabilités, et également celle de désengorger le système d'autorisation de la CNIL. Des outils à cet effet sont donc en cours de développement et seront prochainement mis à la disposition des entreprises.
S'agissant de la qualification des parties – responsables de traitement ou sous-traitants –, un faisceau d'indices a notamment été développé pour aider les sociétés qui s'interrogent sur leurs rôles et leurs responsabilités. Ce faisceau d'indices a vocation à être un outil pratique pour aider à qualifier les parties et ainsi les accompagner dans l'application effective des principes de protection des données personnelles.

Le G29 a-t-il adopté un document relatif à l'externalisation ?

En 2009, le G29 s'est saisi de la question des définitions des responsables de traitement et des sous-traitants, qui constituent des concepts-clés dans la problématique de l'externalisation.
À l'instar de ce qui avait été fait en 2007 avec l'avis sur la définition de donnée personnelle, un sous-groupe du G29 a rédigé un projet d'avis très complet sur ces deux notions fondamentales en y incluant une série d'exemples très concrets et inspirés de situations réelles.
La CNIL a très largement contribué à la rédaction de ce document dans lequel ont été introduits les critères du faisceau d'indices. Cet avis a été adopté en février 2010 par le G29.

Surveillance des voyageurs à l'intérieur de l'Europe

Le dispositif e-Borders

Par une loi de mars 2006, le parlement britannique a adopté un dispositif dénommé e-Borders dans le but de renforcer les contrôles frontaliers. Ce dispositif, qui devait être mis en place au premier semestre 2009, vise à rendre obligatoire dans un premier temps, sous peine de sanctions financières, la transmission par les compagnies aériennes à l'agence frontalière britannique United Kingdom Borders Agency (UKBA) de toutes les données personnelles des passagers et membres d'équipage voyageant à destination du Royaume-Uni.

À terme, e-Borders devrait s'appliquer indifféremment à tous les voyageurs, y compris aux ressortissants des États membres de l'Union européenne, quel que soit le moyen de transport utilisé (bateau, avion, train, voiture). Il est aussi prévu de collecter à la frontière les données biométriques de tous les voyageurs entrant sur le territoire britannique. Les données seraient conservées pendant dix ans dans une base centrale et pourraient être, au cas par cas, partagées avec d'autres autorités.

Ce projet soulève de sérieuses questions quant à sa conformité au droit et principes fondamentaux européens, et notamment au principe de la libre circulation des citoyens européens prévu par les traités fondateurs. En effet, les autres pays de l'Union pourraient exiger la réciprocité et étendre entre eux des mesures similaires, ce qui serait susceptible de remettre en cause l'existence même de la convention de Schengen. En outre, des distorsions de concurrence pourraient découler des éventuelles sanctions financières infligées aux transporteurs qui refuseraient de se conformer à l'obligation de transmettre aux autorités britanniques les données qu'ils détiennent.

La question de la conformité du dispositif à la directive européenne de 1995 relative à la protection des données et à la loi « Informatique et Libertés » se pose également, dans la mesure où la liste des données collectées (soixante-neuf catégories au total, contre les dix-neuf prévues dans l'accord entre l'Union européenne et les États-Unis pour le transfert de données relatives aux passagers dit « *PNR USA* »), ainsi que leur durée de conservation (dix ans) seraient bien plus étendues que celles jusqu'à présent demandées par des pays tiers à l'Union européenne, sans que cela soit justifié.

Il convient de relever qu'un rapport du Parlement britannique (House of commons) du 15 décembre 2009 sur le programme e-Borders a demandé à l'agence frontalière britannique de suspendre le déploiement du dispositif et d'engager de façon prioritaire des discussions sur l'ensemble des difficultés liées à la protection des données personnelles.

La Commission européenne a estimé qu'à la lumière des clarifications, engagements et assurances données par l'agence frontalière britannique, le dispositif e-Borders ne constituait ni une violation de la directive de 1995 relative à la protection des données personnelles, ni de la directive de 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres.

Elle a cependant relevé que des difficultés importantes, s'agissant des fondements juridiques nationaux ainsi que de la durée de conservation excessive, devraient encore être levées.

Compte tenu des enjeux du dossier, la CNIL a saisi en décembre 2009 le Premier ministre, ainsi que les parlements français et européen, afin de leur faire part de sa vive préoccupation et d'appeler leur attention sur les difficultés juridiques soulevées. La CNIL a ainsi souligné la nécessité qu'un accord politique entre les Gouvernements concernés soit conclu afin d'autoriser et d'organiser de tels transferts d'informations.

Elle a par ailleurs demandé à la société Air France de surseoir à la transmission des données.

Le projet de décision-cadre pour l'utilisation des données des passagers à des fins répressives (PNR européen)

La Commission européenne a présenté le 6 novembre 2007 une proposition de décision-cadre relative à l'utilisation des données des dossiers passagers (*Passenger Name Record – PNR*) à des fins répressives. Ces données sont utilisées dans un cadre de prévention et de lutte contre les infractions terroristes et autres formes graves de criminalité. Elles servent aussi à l'élaboration d'indicateurs de risque (technique de « profilage »).

Le projet vise principalement à créer une obligation pour les compagnies aériennes de collecter les données des passagers en provenance ou à destination d'un État membre, et de les transmettre aux autorités compétentes. Les données collectées seraient transmises à des « Unités de renseignement passager » nationales, entités spécialement créées afin de procéder aux opérations de collecte, d'analyse, de transfert vers les États membre et les pays tiers, de conservation, d'effacement des données, et d'analyse des risques.

Ces données seraient quasi identiques à celles de l'accord PNR entre les États-Unis et l'Europe de juillet

2007. Elles seraient conservées pendant une durée maximale de dix ans au total (trois ans en base « active » et entre trois à sept ans dans une base de données dite « passive »). Elles seraient en principe transmises selon une méthode dite « push » (envoi par les compagnies aériennes) et non de « pull » (accès direct aux bases de données des compagnies par les autorités répressives).

Les autorités de protection des données ont tout d'abord émis des avis très critiques sur cette proposition, qui a ensuite fait l'objet de nombreuses discussions au sein du Conseil. Ce texte a également fait l'objet d'un avis de l'Agence des droits fondamentaux le 28 octobre 2008, ainsi que d'une résolution législative du Parlement européen très critique, le 20 novembre 2008.

Une version modifiée du texte de proposition de décision-cadre intégrant des garanties en matière de protection des données a été présentée au groupe de travail multidisciplinaire « criminalité organisée » du Conseil le 23 janvier 2009.

Toutefois, cette version de la décision-cadre ne fait toujours pas l'objet d'un consensus entre les délégations nationales, notamment sur : la question de l'inclusion ou non des vols intracommunautaires, la possibilité ou non de collecter et d'utiliser des données « sensibles », la durée de conservation exacte des données traitées, ainsi que les modalités précises de transfert de ces données traitées vers des États tiers.

Le législateur français a entamé des réflexions approfondies sur le projet de PNR européen. À cette occasion, la CNIL a été auditionnée à plusieurs reprises par les commissions compétentes de l'Assemblée nationale et du Sénat.

Le Sénat a ainsi adopté une résolution sur ce sujet le 30 mai 2009, et l'Assemblée nationale a fait de même le 18 octobre 2009. Ces deux résolutions appellent notamment :
– à délimiter plus strictement les finalités des traitements mis en œuvre à la prévention, détection et répression des infractions pénales graves ;
– à prévoir des garanties supplémentaires afin d'assurer le respect des droits fondamentaux des personnes, et notamment du droit à la vie privée et du droit à la protection des données personnelles ;
– à encadrer strictement, voire exclure totalement, la possibilité pour les autorités compétentes de traiter des données sensibles ;
– à réduire la durée de conservation des données PNR ;
– à mieux encadrer la possibilité de transfert ultérieur vers des pays tiers.

La CNIL sera très attentive à l'évolution de ce dossier.

LES DONNÉES DE SANTÉ : UNE PROTECTION NÉCESSAIRE

Hébergement des données de santé : les premiers hébergeurs sont agréés

La procédure d'agrément ministériel des hébergeurs de données de santé a repris le 2 février 2009 après une suspension de deux ans. La Commission s'est prononcée sur les dossiers de candidature qui lui ont été adressés par la ministre de la Santé après s'être assurée du déploiement par les candidats hébergeurs de solutions de sécurité effectives et de haut niveau et de l'exercice effectif des droits des patients.

À l'heure où le partage des données de santé entre un nombre croissant d'acteurs du système de soins est reconnu par tous comme contribuant à l'amélioration de la qualité des soins et à la maîtrise des dépenses, le développement de l'e-santé est inéluctable. Dans ce contexte, la sécurité des données personnelles de santé est une priorité renforcée.

La procédure d'agrément des hébergeurs de données de santé à caractère personnel, instaurée par la loi du 4 mai 2002 relative aux droits des malades, vise à garantir la sécurité des données personnelles de santé lorsqu'elles sont hébergées par un organisme distinct du professionnel ou de l'établissement de santé qui soigne le malade.

Les conditions de l'agrément ont été fixées par le décret du 4 janvier 2006 qui organise la procédure d'agrément et fixe le contenu du dossier qui doit être fourni à l'appui de la demande.

Cet agrément est délivré pour une durée de trois ans par le ministre chargé de la Santé, qui se prononce après avis de la CNIL et du Comité d'agrément créé auprès de lui.

Cette procédure particulière et préalable s'applique sans préjudice des formalités propres à la loi « Informatique et Libertés », auxquelles restent soumis les professionnels et établissements de santé, qui, en leur qualité de responsables de traitements automatisés de données à caractère personnel, font héberger leurs bases de données chez des organismes agréés.

En raison notamment de la lourdeur de la procédure et du grand nombre d'applications susceptibles d'être concernées, la loi du 30 janvier 2007 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, le temps, pour le comité, d'élaborer les référentiels nécessaires à l'instruction des dossiers.

Ce référentiel, destiné à permettre une autoévaluation par les candidats et un traitement efficace des demandes d'agrément, a été élaboré par l'Agence des systèmes d'information partagés de santé (ASIP Santé, anciennement dénommée GIP-DMP), en concertation avec les industriels. La CNIL a été associée à la définition de ce référentiel. Elle est également associée aux réunions du Comité d'agrément des hébergeurs.

Les premières décisions de la ministre sont intervenues et devraient être publiées en mars 2010. En dehors des agréments délivrés en 2006 dans le cadre de l'expérimentation du DMP pour le temps de l'expérimentation, les premiers hébergeurs de données de santé seront donc agréés.

Quel calendrier pour le DMP ?

Le projet initial a donné lieu à de nombreux rapports sur la conduite du projet qui ont guidé les orientations d'un programme de relance du projet. L'idée maîtresse de ce programme est d'inscrire le projet DMP dans une stratégie de développement des systèmes d'information de santé.

Une nouvelle Agence des systèmes d'information de santé partagés (ASIP) a été mise en place et regroupe le GIP-DMP, le GIP-CPS (carte de professionnel de santé) et le département « interopérabilité » du GMSIH (Groupement pour la modernisation du système d'information hospitalier). Cette agence est chargée de relancer le projet DMP et d'*« élaborer des normes d'interopérabilité et de sécurité des systèmes d'information »* de santé en général.

Le projet, orienté sur la notion de services rendus aux usagers du système de santé et aux professionnels de santé, devrait être développé en deux étapes :

• La première étape : 2009 à 2012

Il s'agit d'une phase d'expérimentation au cours de laquelle un dossier patient « socle » sera déployé au niveau national et alimenté notamment par les comptes rendus de consultation et d'hospitalisation. Parallèlement, les conditions du développement des systèmes d'informations partagées seront précisées (concertation avec les acteurs concernés, développement de l'usage de la carte de professionnel de santé (CPS) dans les établissements, mise en convergence des projets territoriaux, production de référentiels d'interopérabilité et de sécurité).

• La deuxième étape : à partir de 2012

Un portail unique sera mis en place permettant le déploiement complet du DMP.

La loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital, relative aux patients, à la santé et aux territoires (dite « HPST ») a consacré le caractère facultatif du DMP et supprimé la sanction de moindre remboursement en cas de refus d'accès du patient.

Questions à …

Jean Massot

Président de section honoraire
au Conseil d'État
Commissaire en charge du secteur
« Santé et assurance maladie »

Quel est le rôle de la CNIL dans ce dispositif ?

En sa qualité d'autorité de protection des données personnelles, la CNIL a accompagné toutes les phases de définition et de réalisation du dossier médical personnel.

Elle devra encore se prononcer sur un certain nombre de textes qui commandent la généralisation du dispositif (décret DMP, décret identifiant) et autoriser les différentes phases de développement du projet.

À diverses reprises, la Commission a eu l'occasion de rappeler les conditions qui, de son point de vue, sont nécessaires pour mener à bien ce projet.

Outre la définition d'un cadre juridique stable déjà évoquée, le déploiement de solutions de sécurité effectives et de haut niveau est nécessaire. Seul un contexte de sécurité garantie sera de nature à permettre un exercice effectif des droits des patients prévus par la loi. La modernisation des systèmes d'information des professionnels de santé est donc un préalable à la poursuite du projet.

La CNIL porte une attention particulière à l'effectivité des droits des patients, notamment en matière de recueil du consentement explicite et exprès. Conformément aux dispositions de la loi du 6 janvier 1978, l'information délivrée au patient sur ses droits doit être claire, complète et préalable sur les finalités et fonctionnalités du DMP.

En outre, la CNIL souhaite une harmonisation des régimes juridiques, et en particulier des modalités de consentement du patient à l'ouverture ou à l'accès des différents dossiers de santé sur internet (dossier pharmaceutique, dossier de cancérologie, dossier de réseaux de soins).

La CNIL est associée au groupe de travail qui a été constitué en 2009 et dont l'objectif est de produire un guide de bonnes pratiques sur les modalités de recueil du consentement des patients et l'utilisation par les professionnels de santé des données de santé à caractère personnel.

Un équilibre est à trouver entre les besoins des professionnels de santé et ceux des patients dont l'implication est indispensable. La CNIL ne peut trouver que des avantages à voir renforcés les voies et les moyens d'une coopération régulière entre les différents acteurs sur le sujet des dossiers médicaux électroniques et de la protection des données personnelles de santé.

L'anonymisation : une condition d'accès des complémentaires aux données de santé

La Commission nationale de l'informatique et des libertés a autorisé le 10 décembre 2009, la Mutualité française, les sociétés Axa-France et GROUPAMA, à prolonger les expérimentations ayant pour finalité de recourir et d'exploiter, sous forme anonymisée, les données de santé figurant sur les feuilles de soins électroniques.

En décembre 2009, elle a autorisé, pour une durée de trente-six mois, la poursuite de ces expérimentations après avoir analysé les bilans des complémentaires santé qui en avaient fait la demande. Les expérimentations ont toutes pour objet de permettre la transmission aux organismes d'assurance-maladie complémentaire (AMC) des codes des médicaments et en matière d'optique des codes produits et prestations délivrées à l'assuré. L'accès à ces données qui figurent sur les feuilles de soins électroniques permet aux complémentaires de mieux identifier les soins remboursés et ainsi de simuler ou de proposer à leurs assurés des garanties contractuelles modulées, d'affiner leur tarification sur la prise en charge de spécialités non remboursées par le régime obligatoire et d'inciter les assurés à adhérer à des actions de prévention. Alors que la politique du gouvernement vise à diminuer ou à dérembourser certains produits ou prestations à service médical rendu estimé insuffisant, l'accès apparaît pour les AMC d'autant plus nécessaire qu'elles souhaitent jouer un rôle accru en matière de maîtrise des dépenses de santé.

Afin de s'assurer que les données qui pourraient conduire à identifier les assurés ne viennent à la connaissance des AMC tout en permettant à ceux-ci d'affiner les garanties qu'ils proposent, la Commission a demandé que l'anonymisation repose sur l'utilisation d'une boîte noire, c'est-à-dire un dispositif matériel inviolable même par les complémentaires santé, audité par un organisme extérieur à l'AMC.

La CNIL a également donné son aval sur un dispositif technique proposé par le ministère de la Santé en concertation avec les différents acteurs du secteur qui permettra, dans le cadre de SESAM Vitale, de transmettre des données détaillées des feuilles de soins électroniques (FSE) vers les serveurs des organismes complémentaires. Cette solution définit des règles de sécurité pour les échanges de données de santé (FSE) entre le professionnel de santé et les complémentaires santé. Les AMC disposent de trois ans pour se mettre en conformité avec ce dispositif.

La CNIL a donc autorisé les trois organismes d'AMC, qui en ont fait la demande, à poursuivre les expérimentations en cours, en les invitant à adopter, dans l'intervalle, l'architecture commune proposée par le ministère.

L'audit du système par un organisme extérieur et la mise en conformité avec la solution générique d'acheminement des données de santé sont des points indispensables avant toute généralisation. Les trois organismes d'AMC devront, au terme de la période de trois ans, présenter une nouvelle demande d'autorisation et soumettre, à l'appui de la demande la nouvelle architecture d'acheminement des données adoptée dans leurs systèmes d'information.

Toutefois, la Commission continue d'appeler de ses vœux une loi qui définisse les données de santé pouvant être transmises aux AMC, les garanties appropriées et les conditions de transmission de ces données.

La CNIL explique

L'anonymisation

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

La CNIL contrôle les conditions de traitement des données de santé par les assureurs

Dans le cadre des demandes de prêts, en particulier immobiliers, les emprunteurs ont l'obligation de souscrire une assurance qui garantit à la banque le remboursement du crédit en cas de décès ou de maladie. Ces contrats se concluent auprès de compagnies d'assurance qui sont amenées, à cette occasion, à collecter de nombreuses données de santé concernant les demandeurs de crédit.

L'enjeu des traitements mis en œuvre, tant au regard du nombre de personnes concernées que de la nature des données traitées, nécessite que la loi « Informatique et Libertés » soit rigoureusement respectée. La Commission a donc effectué plus d'une quinzaine de contrôles auprès de compagnies d'assurance, de cabinets de courtage en assurance et du bureau commun d'assurances collectives (BCAC).

La CNIL a constaté que les sociétés d'assurance ne procédaient pas à une mutualisation ou à un échange d'informations concernant la santé des personnes. Toutefois, elle a relevé d'importants manquements à la loi « Informatique et Libertés », portant notamment sur la confidentialité, la sécurité et la durée de conservation des données de santé. En effet, ces informations sensibles sont souvent accessibles à un très grand nombre de salariés au sein des compagnies d'assurance (service informatique, service clientèle, etc.). De surcroît, les dossiers contenant des données de santé sont parfois examinés par des services qui ne sont pas placés sous la responsabilité des médecins conseils. Les contrôles ont mis également en évidence l'insuffisance globale des mesures de sécurité apportées aux données de santé, en particulier leur absence de chiffrement. Par ailleurs, de nombreuses compagnies d'assurance conservent de manière excessive des informations de santé, en particulier sur des personnes qu'elles n'assurent pas ou plus. Enfin, lorsqu'une personne exerce son droit d'accès, les informations la concernant détenues par l'assureur ne lui sont pas toujours communiquées en intégralité.

LES SALARIÉS SOUS SURVEILLANCE

Alertes professionnelles : la Cour de cassation se prononce en faveur d'un champ d'application réduit de l'autorisation unique

Dans un arrêt du 8 décembre 2009, la chambre sociale de la Cour de cassation rappelle que les alertes professionnelles autorisées par la CNIL dans le cadre de l'autorisation unique n° 4 doivent avoir un champ d'application limité.

Afin de se conformer aux exigences de la loi américaine dite « Sarbanes Oxley », la société Dassault Systèmes a mis en place un Code de conduite des affaires énumérant les règles que les salariés s'engagent à respecter dans l'exercice de leur activité professionnelle. Ce code instaure notamment un dispositif d'alerte professionnelle permettant aux salariés de signaler tout manquement *via* une adresse électronique dédiée. Préalablement à la mise en place du dispositif, la société Dassault Systèmes a effectué une déclaration de conformité à l'autorisation unique n° 4.

À l'occasion du contentieux né de ce système d'alerte, la Cour de cassation rappelle que le champ d'application de l'autorisation unique doit être limité. Elle indique clairement que la mise en œuvre d'un dispositif d'alerte professionnelle, faisant l'objet d'un engagement de conformité à l'autorisation unique, doit se limiter aux seuls domaines comptables, financiers, et de lutte contre la corruption.

En effet, la CNIL avait prévu, à l'article 3 de son autorisation unique n° 4, la prise en compte de faits ne relevant pas de ce champ d'application mais mettant en jeu « l'intérêt vital de l'organisme ou l'intégrité physique ou morale de ses employés ». La Cour de cassation précise que cet article ne doit pas être interprété comme permettant un élargissement de la finalité des dispositifs d'alertes tels que prévus par l'autorisation unique. Les systèmes d'alertes qui ne répondent pas strictement aux conditions de l'autorisation unique n° 4 doivent faire l'objet d'une autorisation spécifique accordée au cas par cas par la CNIL.

Par ailleurs, la Cour de cassation souligne la nécessité pour les entreprises d'informer les personnes concernées conformément aux dispositions de la loi « Informatique et Libertés ». Sur ce point, l'arrêt rappelle que « les mesures d'information prévues par la loi du 6 janvier 1978 reprises par la décision d'autorisation unique [...] doivent être énoncées dans l'acte instituant la procédure d'alerte ». En effet, dans l'affaire Dassault, cette information était incomplète s'agissant des droits d'accès, de rectification et d'opposition.

La CNIL mènera en 2010 des auditions en vue de modifier prochainement son autorisation unique à la lumière de l'arrêt rendu par la Haute Juridiction et des constats opérés lors des contrôles récemment menés auprès d'entreprises.

De quoi s'agit-il ?

Une « alerte professionnelle » (ou « whistleblowing »)

C'est un outil mis à la disposition des salariés. Il peut s'agir par exemple d'un numéro de téléphone « ligne éthique » ou d'une adresse électronique particulière. Ce dispositif leur permet de signaler des problèmes pouvant sérieusement affecter l'activité d'une entreprise ou engager gravement sa responsabilité.

Les alertes recueillies sont ensuite vérifiées, dans un cadre confidentiel, et permettent à l'employeur de décider, en connaissance de cause, des mesures correctives à prendre.

Ce dispositif est-il obligatoire ?

Compte tenu de la multiplicité des voies d'alertes déjà disponibles dans les entreprises (voie hiérarchique, commissaires aux comptes, fonctions de l'audit ou de la conformité interne, représentants du personnel, inspection du travail, etc.), le dispositif d'alerte professionnelle ne peut être que facultatif. Un salarié ne peut pas être sanctionné s'il ne souhaite pas l'utiliser.

La CNIL contrôle les « contrôleurs »

La CNIL a effectué plusieurs contrôles relatifs à la surveillance des salariés.

Les contrôles réalisés apprécient les conditions de mise en œuvre des dispositifs de vidéosurveillance. Ils permettent de vérifier l'information délivrée aux salariés et le caractère non intrusif de la surveillance.

Les contrôles de la CNIL ont également porté sur la mise en œuvre de dispositifs de géolocalisation. Ceux-ci connaissent un développement certain et comportent des risques de dérives : « flicage » permanent des salariés disposant d'un véhicule, collecte de données interdites par la loi (infractions routières) ou encore surveillance du salarié lorsque celui-ci est autorisé à utiliser le véhicule à des fins privées. Les contrôles effectués par la CNIL permettent ainsi de vérifier la correcte application de sa recommandation en date du 16 mars 2006 sur la géolocalisation des véhicules des salariés.

Enfin, la Commission a réalisé de nombreux contrôles dans le cadre de l'instruction de plaintes de salariés qui estimaient que leurs droits issus de la loi « Informatique et Libertés » n'étaient pas respectés. D'une manière générale, les contrôles ont démontré un manquement à l'obligation d'information des personnes et la mise en œuvre de dispositifs ne comprenant aucune durée de conservation des données déterminée.

AU PROGRAMME 2010

PROTÉGER SON IMAGE SUR INTERNET, ÇA S'APPREND !

Les actions de sensibilisation

La CNIL prévoit en 2010, notamment à l'occasion de la journée européenne de protection des données et de la vie privée du 28 janvier, de mener des actions de sensibilisation à destination des jeunes (12-16 ans) pour les inciter à adopter de bonnes pratiques sur internet. Bien que destinées aux enfants, ces actions s'adressent aussi aux parents et aux enseignants ou éducateurs. Certains supports de communication seront accompagnés d'outils pédagogiques ou de fiches pratiques permettant d'aborder en classe les questions de vie privée sur internet sous la forme d'ateliers, d'exposés ou de débats.

L'objectif premier de ces actions est de responsabiliser les jeunes aux contenus qu'ils publient de façon à limiter les propos pouvant nuire à leur image ou à celles de leurs « amis ». La vigilance s'impose très jeune surtout lorsqu'il s'agit de diffuser des informations à caractère politique, sexuel, médical ou religieux. **C'est bien avant de publier qu'il faut réfléchir** car une fois en ligne, il est difficile de supprimer les informations qui peuvent constituer une identité numérique très persistante. La CNIL propose des conseils pratiques qui permettent de profiter des avantages d'internet sans que sa vie privée en fasse les frais.

La CNIL qui participe déjà au comité scientifique d'Internet sans crainte depuis plusieurs années renforcera en 2010 son partenariat pour mutualiser des ressources et des compétences complémentaires.

La CNIL sur les réseaux sociaux

En 2010, la CNIL prévoit l'ouverture de comptes sur Twitter, Faceboook et Dailymotion afin de dispenser des conseils pratiques pour utiliser ces réseaux tout en préservant sa vie privée.

Le site jeunes.cnil.fr

La CNIL mettra en ligne une nouvelle version de son site à destination des jeunes intégrant tous les outils et supports développés à l'occasion de la journée européenne de la protection des données ou du Safer Internet Day, Journée pour un internet plus sûr, le 9 février.

LA LABELLISATION

Depuis plusieurs années, la tendance générale est d'aborder les problématiques relatives à la protection des données sous l'angle de la régulation. Cette nouvelle approche suppose, d'une part, des normes auxquelles se référer et, d'autre part, des instruments comme la labellisation permettant de vérifier leur application.

La loi du 6 août 2004 a confié à la CNIL une mission spécifique d'évaluation des technologies et d'accompagnement du développement économique des entreprises, en lui permettant de délivrer des labels à des produits ou des procédures qui respectent la vie privée.

La loi du 12 mai 2009 de simplification et de clarification du droit et d'allégement des procédures offre la possibilité à la CNIL de faire appel à des experts extérieurs indépendants pour procéder à des évaluations des procédures ou des produits candidats à un tel label, quand la complexité de l'évaluation le justifie. La procédure de labellisation peut, quant à elle, être définie dans le règlement intérieur de la Commission.

Ce pouvoir de labellisation, bien qu'il ne soit pas encore mis en œuvre, représente une réelle opportunité pour la CNIL. Il lui permettra de se positionner comme une référence dans le paysage institutionnel et économique. Il transformera la CNIL en un véritable régulateur économique pouvant orienter le marché vers les solutions les plus protectrices en matière de vie privée et lui permettant d'inciter les sociétés à respecter les principes de la loi « Informatique et Libertés ».

En effet, la confiance et la sécurité constituent les clés de voûte du développement des nouvelles technologies. Leur acceptation et leur développement harmonieux ne peuvent être assurés qu'à condition que soient mises en place des garanties portant sur tous les droits fondamentaux des individus et notamment en matière de protection des données. Pour les utilisateurs ou les clients d'une société, un label représente donc un critère permettant d'éclairer ses choix puisqu'il implique à la fois une garantie de qualité et une information claire. L'argument de qualité lié au respect des principes « Informatique et Libertés » constitue ainsi un véritable outil de compétitivité pour les entreprises qui peuvent, grâce à lui, se démarquer de leurs concurrents.

L'année 2010 devrait être une année clé dans la mise en œuvre de ce nouveau pouvoir durant laquelle la CNIL devrait assembler toutes les briques nécessaires pour délivrer ses premiers labels dès 2011.

Parmi les éléments à prendre en compte, il sera notamment nécessaire de définir des référentiels d'évaluation, de construire un modèle économique viable pour ce processus et d'adapter le règlement intérieur.

LA GÉOLOCALISATION DES VÉHICULES DE PARTICULIERS

La géolocalisation embarquée dans les véhicules

Depuis 2005, la CNIL suit avec une attention particulière les dispositifs de géolocalisation expérimentaux pour le calcul des primes d'assurance, ainsi que les autres traitements faisant appel à la géolocalisation des véhicules mis en place par les assureurs et les constructeurs automobiles. Elle entend élaborer, en 2010, une recommandation sur le sujet afin d'apporter aux professionnels des solutions pratiques à leurs questions.

Les systèmes permettant de moduler le calcul des primes d'assurance, souvent dénommés sous le terme anglais générique de *Pay As You Drive* (ou PAYD), n'ont pas la géolocalisation pour but, mais ils utilisent cette technique pour vérifier le kilométrage, la durée de temps de conduite, les périodes de conduite et la vitesse des véhicules.

La recommandation devrait préciser que ces dispositifs ne doivent pas aboutir à la mise en place de traitements d'infractions, et que seule la vitesse moyenne, dans l'hypothèse où des assureurs trouveraient pertinent d'utiliser cette donnée, pourrait être collectée.

La Commission est par ailleurs très vigilante sur l'information donnée aux personnes, dans la mesure où ces dispositifs de calcul de prime ne prévoient pas de fonction de désactivation. La licéité des dispositifs de PAYD repose donc sur le consentement éclairé des intéressés et sur une information préalable des automobilistes, ce qui pose le problème de la bonne information non seulement de l'assuré, conducteur habituel, mais également des autres conducteurs éventuels.

Au-delà des mesures de sécurité susceptibles d'être mises en œuvre, la CNIL devrait préconiser l'effacement des données de géolocalisation dès l'instant que les données nécessaires au calcul de la prime ont été relevées ou calculées. C'est à cette condition que les dispositifs de PAYD pourront être considérés comme acceptables au regard de la protection de la vie privée.

De 2006 à 2008 des dispositifs de géolocalisation ont été mis en œuvre à titre expérimental par des compagnies d'assurance pour définir le montant des cotisations d'assurance de leurs clients ou leur offrir des services d'appel d'urgence et/ou de lutte contre le vol. À ce jour, la généralisation de ces dispositifs impose que la CNIL effectue au cours de l'année 2010 des missions de contrôle auprès de ces prestataires pour s'assurer que le principe d'aller et venir anonymement est respecté, notamment en vérifiant quels types de données sont traitées par les assureurs et leur durée de conservation.

Le système d'urgence e-call

D'autres services existent en complément ou indépendamment du PAYD : des services tels que la mise sous surveillance du véhicule ou le « tracking » en cas de vol et l'e-call (l'appel d'urgence) sont fréquemment proposés par les assureurs. On retrouve une démarche similaire chez les constructeurs automobiles qui profitent de l'informatisation des véhicules pour fournir en « option » ou « en série » certains de ces dispositifs. À la différence du PAYD, ces services n'utilisent pas la géolocalisation à titre accessoire, puisque celle-ci est précisément la finalité du traitement.

Les systèmes de lutte contre le vol, s'ils sont mis en place, ne devraient pas, notamment, permettre aux propriétaires des véhicules volés d'avoir connaissance des informations issues des boîtiers afin d'éviter qu'ils ne se fassent justice eux-mêmes. La Commission considère, de plus, que ces dispositifs nécessitent qu'une procédure de levée de doute soit systématiquement intégrée.

S'agissant des dispositifs d'e-call, la finalité d'urgence devrait être clairement définie afin qu'il n'y ait pas de détournement de finalité : les données de localisation ne doivent pas être réutilisées à d'autres fins que celle de faire venir les secours sur les lieux de l'accident le plus rapidement possible. À cet effet, la durée de conservation de ces données devra être limitée. Par ailleurs, une information claire et préalable des personnes ainsi qu'un accès restreint aux informations devront être prévus.

Raisonnant dans le cadre du futur e-call européen fondé sur le 112, le G29 a recommandé en 2006, en l'absence d'obligation légale de ce système, l'installation d'un dispositif de désactivation instantanée, en s'appuyant notamment sur deux raisons : le consentement doit pouvoir être retiré à tout moment, et, un grand nombre de personnes pourrait désirer ne pas en vouloir compte tenu

des risques en termes de vie privée ; par ailleurs, si un système sans désactivation peut se justifier en raison de l'intérêt vital des personnes, l'e-call est néanmoins susceptible de fonctionner quand l'intérêt vital n'est pas en jeu, c'est-à-dire quand l'intervention des services d'urgence n'est pas nécessaire.

Aujourd'hui, après plusieurs années de mise en œuvre, la CNIL constate que les risques en termes de vie privée sont restreints, puisque les données ne sont collectées et transmises qu'en cas d'accident (ou d'incident) et de connexion volontaire. C'est pourquoi, elle considère que l'implantation d'une désactivation instantanée dans les véhicules équipés d'un système d'appel d'urgence ne peut être imposée dès l'instant que ce système est acquis librement et en toute connaissance de cause par le propriétaire du véhicule. Ce dernier doit aussi s'engager à informer les utilisateurs potentiels du véhicule ainsi équipé. Enfin, en termes de sécurité juridique, des problèmes de preuve ne manqueront pas de se poser en cas de dommages subis suite à un accident non suivi d'un appel.

L'ensemble de ces points devraient être prochainement réunis dans une recommandation.

LA COMMUNICATION POLITIQUE À L'HEURE DES NOUVELLES TECHNOLOGIES

Pour se faire connaître et promouvoir leurs idées, les partis politiques, les élus et les candidats à des élections se sont pendant longtemps contentés de réaliser des opérations de mailing postal, de distribuer des tracts et de participer à des manifestations de toutes sortes.

Face aux multiples évolutions technologiques survenues ces dernières années, ils ont su s'adapter, renouvelant ainsi l'art de la communication politique. En effet, les dernières campagnes électorales menées en France (élections présidentielles de mai 2007 et européennes de juin 2009) et surtout aux États-Unis (élection présidentielle de novembre 2008) ont fait apparaître des pratiques technologiques inédites jusqu'alors dans le domaine politique.

Alors que certains politiques ont investi la toile en recourant à la vidéo en ligne, aux réseaux sociaux, aux forums de discussion et autres blogs, d'autres ont préféré développer de nouveaux canaux de communication « *one-to-one* », tels que les SMS et les courriers électroniques envoyés par Bluetooth. Bien des partis politiques et candidats n'hésitent d'ailleurs plus à utiliser simultanément plusieurs modes de communication, espérant ainsi améliorer d'autant leurs chances de toucher des électeurs potentiels.

Ces nouvelles pratiques génèrent parfois de l'incompréhension de la part des personnes faisant l'objet de telles opérations de communication et posent de nouvelles interrogations sur le plan « Informatique et Libertés ». La spécificité des opérations de communication politique et l'utilisation de technologies particulièrement intrusives poussent la CNIL à porter une attention toute particulière aux garanties qu'il convient d'apporter aux droits et libertés des personnes dont les données sont collectées et utilisées.

Dès le 5 octobre 2006, la CNIL a adopté une recommandation sur le traitement de données personnelles par les partis politiques, élus ou candidats. Cette recommandation fait en particulier le point sur les conditions dans lesquelles il est possible d'organiser des opérations de communication politique.

La CNIL intervient régulièrement auprès des politiques pour rappeler ces bonnes pratiques, et notamment la nécessité d'informer les personnes de la finalité politique du traitement, de leur droit de s'opposer à ce que leurs données soient utilisées à des fins de communication politique, ou encore que seules les personnes y ayant expressément consenti peuvent être démarchées par voie électronique.

La CNIL envisage de mener de nouvelles auditions pour actualiser la recommandation de 2006.

LA MESURE DE LA DIVERSITÉ

Participation de la CNIL au COMEDD

Le Comité pour la mesure et l'évaluation de la diversité et des discriminations (COMEDD) a été mis en place en mars 2009 par Yazid Sabeg, commissaire à la diversité et à l'égalité des chances. Ce comité, était présidé par François Héran, ancien directeur de l'Institut national d'études démographiques (Ined) et réunissait près d'une trentaine d'experts (statisticiens, chercheurs, sociologues, syndicats, associations). Abordant un sujet complexe et controversé, ce comité avait pour mission de procéder à l'identification des méthodes de mesures existantes en matière de discriminations liées aux origines, d'identifier celles qui pourraient aider les administrations et les entreprises à mieux lutter contre ce type de discriminations et à clarifier le cadre juridique existant. Ce comité rendra son rapport début 2010.

Questions à ...

Marie-Hélène Mitjavile

Conseiller d'État
Commissaire en charge du secteur « Recherche et statistique »

Vous avez représenté la CNIL au sein du COMEDD. Pour quelle raison la CNIL a-t-elle été associée aux travaux de ce comité ?

Le plus souvent, les études et les enquêtes sur la mesure de la diversité et des discriminations peuvent nécessiter le recueil et le traitement de données à caractère personnel. Dès lors, les fichiers ainsi constitués sont soumis au contrôle de la CNIL. Notre Commission avait d'ailleurs dès 2005, compte tenu du caractère sensible de ce type de d'études, publié une première série de recommandations en matière de mesure de la diversité et de lutte contre les discriminations dans le domaine de l'emploi. En mai 2007, la CNIL a poursuivi sa réflexion en rendant publiques dix recommandations pour améliorer le développement des outils statistiques sur la mesure de la diversité selon des modalités garantissant la protection des données et en particulier leur confidentialité et le respect des droits des personnes.

Quels ont été les messages de la CNIL ?

Comme le rappelle souvent la CNIL, j'ai tenu à souligner que le traitement de données sensibles sur les origines reste possible à droit constant dès lors qu'il est réalisé selon des modalités garantissant la protection des données et en particulier leur confidentialité et le respect des droits des personnes.
J'ai également fait part des recommandations formulées par la CNIL en 2007 et notamment celle visant à introduire l'information sur la nationalité et le pays de naissance des parents dans le recensement annuel de la population et dans les grandes enquêtes de la statistique publique ou encore celle destinée à faciliter l'accès des données de l'INSEE aux chercheurs. Enfin, j'ai rappelé les fortes réserves de la CNIL sur la création d'un référentiel ethnoracial et réaffirmé le principe selon lequel les résultats des études statistiques ne doivent en aucun cas être intégrés dans les fichiers de gestion.
Les réflexions et recommandations qui devraient être formulées par le COMEDD me paraissent très utiles dans un contexte où tout le monde s'accorde sur la nécessité de lutter contre les discriminations mais sans qu'il y ait forcément de véritable consensus sur les outils à employer ou la manière de procéder.

BON À SAVOIR

Les données sensibles : que dit la loi ?

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

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

L'adresse, la nationalité et le lieu de naissance ne sont pas considérés par la CNIL comme des données « sensibles » au sens de l'article 8.

En effet, l'information sur le lieu de naissance de la personne fait partie de l'état civil et est considérée comme une donnée « objective ».

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

LE RECRUTEMENT EN LIGNE

Internet est devenu un canal de recrutement incontournable. Il offre de formidables capacités de contact avec les candidats et fournit des outils pratiques et moins coûteux pour optimiser le traitement des candidatures.

Les sites dédiés au recrutement en ligne sont légion : plateformes mettant en relation l'offre et la demande d'emploi institutionnelles (Pôle emploi, APEC) ou privées (Monster, Cadre online) ; réseaux sociaux « personnels » (Facebook, Copain d'avant) ou plus « professionnels » (Linkedin, Viadeo) ; sans oublier les moteurs de recherche.

Au-delà d'internet, il existe également de nombreux logiciels de gestion des candidatures permettant de trier des CV et de les analyser en vue de sélectionner les profils les plus pertinents.

Trois notions clés : information, sécurité et proportionnalité

La CNIL veille à ce que les candidats-internautes soient correctement informés sur l'utilisation qui est faite de leurs données. Elle s'attache notamment à vérifier qu'ils sont informés de l'identité du responsable du site, des destinataires de données et de la finalité poursuivie ainsi que de leur droit d'accès, de rectification et de suppression. Des mentions compréhensibles et facilement accessibles doivent ainsi figurer sur les formulaires de collecte et la procédure de suppression d'un CV doit être clairement détaillée.

La protection des données à caractère personnel dépend aussi des mesures de sécurité qui ont été prises par le responsable du site. À cet égard, la CNIL est particulièrement vigilante car en cas d'accès ou de diffusion à des tiers le risque de détournement de finalité est important (par exemple utilisation des données à des fins de prospection commerciale).

Les données collectées par les recruteurs ne doivent pas porter atteinte à la vie privée des candidats. Elles doivent être pertinentes, c'est-à-dire permettre d'apprécier si un candidat dispose des aptitudes nécessaires pour occuper un poste. Ainsi, la collecte d'informations sur l'entourage familial, les opinions philosophiques, politiques ou religieuses, l'orientation sexuelle, est excessive et contraire à la loi « Informatique et Libertés ». Même lorsque le recueil d'information est possible (par exemple collecte de l'âge du candidat, ou de sa nationalité, lorsque ces informations sont justifiées) l'utilisation des données collectées doit être conforme à la réglementation applicable en matière de lutte contre les discriminations qui s'est considérablement renforcée depuis 2006.

Un défi majeur : l'utilisation des réseaux sociaux par les recruteurs

Les recruteurs utilisent de plus en plus souvent les réseaux sociaux pour rechercher un candidat ayant un profil particulier, diffuser des offres d'emploi ou encore vérifier des informations fournies par un candidat ou figurant sur son CV.

Une utilisation mal encadrée de ces réseaux peut conduire des recruteurs à s'orienter volontairement ou non vers des informations de nature personnelle sans lien avec les aptitudes professionnelles du candidat.

Ainsi, selon une étude réalisée par un site américain (CareerBuilder), plus de 45% des recruteurs consultent ce type de site. C'est le site grand public Facebook qui arrive en tête avec 29% des consultations ce qui le place devant d'autres sites comme le réseau social professionnel LinkedIn (26%) et MySpace (21%) ou encore Twitter (11%).

Selon l'étude, **plus d'un tiers des recruteurs (35%) a déjà refusé une candidature suite à la consultation de son profil.** Les motifs de rejets les plus fréquents sont la publication d'informations ou de photographies « inappropriées ou provocantes » (53%), l'apologie de l'alcool ou la boisson (44%), la critique d'un ancien employeur (35%) ou encore une mauvaise maîtrise des outils de communication (29%).

En France, selon une étude menée par Novamétrie en septembre 2009 l'utilisation de réseaux sociaux par les DRH à des fins de recrutement serait minoritaire. Toutefois, 71% des collaborateurs des cabinets interrogés estiment qu'ils sont un outil efficace pour recruter certains profils.

Compte tenu des enjeux en termes de vie privée, la CNIL entend poursuivre ses efforts tout au long de l'année 2010 pour mieux encadrer l'utilisation des réseaux sociaux et sensibiliser l'ensemble des acteurs (futurs candidats et recruteurs) à ces problématiques.

Questions à ...

Hubert Bouchet

Membre du Conseil Économique et Social
Commissaire en charge du secteur
« Ressources humaines »

La CNIL a-t-elle réalisé des contrôles en matière de recrutement ?
Oui, le contrôle des conditions de réalisation des opérations de recrutement était inscrit au programme annuel 2009.
Cela a conduit la CNIL à réaliser plus d'une quarantaine de contrôles, tant auprès de cabinets de recrutement que d'entreprises recrutant pour elles-mêmes.

La CNIL a-t-elle constaté des manquements de la part des recruteurs ?
Ces contrôles ont permis de mettre en lumière des manquements récurrents (collecte de données excessives, absence d'information des personnes et absence d'une durée de conservation) mais ont également permis de comprendre la réalité des opérations de recrutement telles qu'elles sont pratiquées aujourd'hui. Ainsi, les constats effectués permettront à la formation plénière de la Commission de nourrir sa réflexion sur l'évolution de sa recommandation en matière de recrutement.

Les recruteurs n'ont-ils pas intérêt à désigner un CIL (correspondant « Informatique et Libertés ») pour s'assurer de la conformité de leurs opérations de recrutement ?
Si, désigner un CIL est effectivement une bonne façon de se préparer à un contrôle de la CNIL. C'est d'ailleurs le constat qui a été fait à l'occasion du contrôle de l'un des principaux cabinets de recrutement français. À l'initiative du CIL, des procédures ont été mises en œuvre pour s'assurer que la base de données des candidats est en parfaite conformité à la loi « Informatique et Libertés ». Le CIL a mis en place des procédures permettant d'encadrer au mieux la gestion de sa base de données des candidats. Par exemple, les conseillers de recrutement ont pour instruction de travailler uniquement sur la base de données du cabinet. Ils ont interdiction de constituer eux-mêmes des bases de travail. Cette restriction permet une gestion centralisée des informations personnelles relatives aux candidats. Elle garantit ainsi une totale effectivité des droits d'accès, de rectification et d'opposition dont les candidats sont, en outre, parfaitement informés. Cette centralisation des données permet également une gestion efficace des durées de conservation, en évitant la multiplication des opérations de purge. Autre exemple : le CIL, en collaboration avec le service informatique du cabinet, a mis en place des opérations régulières de vérification des mentions présentes dans les zones commentaires que les conseillers de recrutement peuvent remplir librement. Partant du constat qu'une simple information des personnes en charge de remplir ces zones ne suffit pas, la mise en œuvre d'un processus automatique de vérification de ces zones sur la base de mots-clés « interdits » garantit que la base est exempte de toute information non pertinente. Enfin, les contrôleurs de la CNIL ont pu constater un niveau de sécurité tout à fait satisfaisant de la base de données : impossibilité pour les chargés de recrutement de la copier, traçabilité de l'ensemble des actions, renouvellement régulier des mots de passe, verrouillage automatique des postes en cas d'inactivité, etc.

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

Décret d'application de la loi nº 2009-972 du 3 août 2009 relative à la mobilité et aux parcours professionnels dans la fonction publique

Conditions de gestion du dossier du fonctionnaire.

Décret d'application de la loi no 2009-594 du 27 mai 2009 pour le développement économique des outre-mer

Conditions de collecte et de mise en œuvre d'un fichier de données à caractère personnel.

Décret d'application de la loi no 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allégement des procédures

Modalités de constitution des bases de données et des informations susceptibles d'être diffusées.

Décret d'application de la loi no 2009-323 du 25 mars 2009 de mobilisation pour le logement et la lutte contre l'exclusion

Gestion de la liste des données consultables.

Conditions d'accès aux données du livre foncier et du registre des dépôts.

Décret d'application de la loi no 2008-1350 du 19 décembre 2008 relative à la législation funéraire

Modalités d'application de l'article 9, y compris la durée de conservation des informations enregistrées.

Décret d'application de la loi no 2007-131 du 31 janvier 2007 relative à l'accès au crédit des personnes présentant un risque aggravé de santé

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

Décrets d'application de la loi no 2007-127 du 30 janvier 2007 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions

Modalités d'élection par voie électronique.

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

Décret d'application de l'ordonnance no 2007-329 du 12 mars 2007 relative au Code du travail

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

Décret d'application de la loi no 2006-872 du 13 juillet 2006 portant engagement national pour le logement

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

Décret d'application de l'ordonnance no 2006-596 du 23 mai 2006 relative au Code du sport

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

Décret d'application de la loi no 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information

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

CONCLUSION

LA PROPOSITION AUX POUVOIRS PUBLICS

Vers un instrument international contraignant dans le domaine de la protection des données personnelles

Sur le plan international, l'évènement marquant de l'année 2009 est très certainement l'adoption à Madrid, le 5 novembre 2009, par les représentants de près de quatre-vingts autorités de protection des données représentant plus de quarante pays, d'une résolution visant à établir des standards internationaux sur la protection des données personnelles et de la vie privée.

Dans un contexte de mondialisation et de croissance fulgurante des flux transfrontières de données personnelles, il est en effet devenu impératif d'assurer, à tout individu en tout point du globe, une protection efficace de sa vie privée et de ses données personnelles. Nos autorités de protection des données n'ont aujourd'hui d'autre choix que d'encourager des actions de sensibilisation et de contrôle, concertées et conjointes, sur la base de règles juridiques communes assurant un haut niveau de protection aux individus.

Or ces règles juridiques communes en matière de protection des données n'existent pas à l'heure actuelle. La résolution de Madrid constitue à cet égard assurément une avancée historique pour un mouvement vers une régulation internationale efficace du droit à la protection des données personnelles. Cette résolution constitue en effet un corpus de principes communs applicable dans le monde entier et pleinement adapté aux dernières évolutions technologiques.

Le développement de normes de standardisation sur la protection de la vie privée par l'Organisation internationale de la normalisation (ISO) et la réflexion engagée, au sein de l'Union européenne, du Conseil de l'Europe ou de l'OCDE, pour une éventuelle modification des textes existants démontrent également pleinement cette nécessité de régulation mondiale.

Toutefois ces initiatives ne sont pas suffisantes à elles seules. Les autorités gouvernementales et parlementaires doivent prendre le relais et œuvrer ensemble pour leur conférer une valeur juridique contraignante. Elles doivent réfléchir ensemble à l'adoption d'un instrument mondial dans le cadre européen mais également mondial. La tenue d'une Conférence intergouvernementale, sur ce sujet, serait un nouvel acte majeur, qui permettrait de traduire en réalité juridique et pratique l'avancée historique de Madrid.

ANNEXES

LES MEMBRES DE LA CNIL

Le bureau

Président

Alex TÜRK, sénateur du Nord
Membre de la CNIL depuis 1992, président de l'autorité de contrôle Schengen de 1995 à 1997, de l'autorité de contrôle commune d'Europol (2000-2002), de l'autorité de contrôle d'Eurodac (2003) et vice-président de la CNIL de 2002 à 2004, Alex Türk est président de la CNIL depuis le 3 février 2004. Il préside la formation contentieuse chargée de prononcer des sanctions. Il a été Président du G29 de février 2008 à février 2010.

Vice-président délégué

Emmanuel de GIVRY, conseiller honoraire à la Cour de cassation
Secteur: Transports et assurances des biens
Emmanuel de Givry est membre de la CNIL depuis février 2004, puis vice-président délégué depuis février 2009.
Membre de droit de la formation contentieuse.

Vice-président

Isabelle FALQUE-PIERROTIN, conseiller d'État, présidente du Conseil d'orientation et déléguée générale du Forum des droits sur l'internet
Secteur: Vie citoyenne et collectivités locales
Isabelle Falque-Pierrotin est membre de la CNIL depuis janvier 2004 et vice-président depuis février 2009.
Membre de droit de la formation contentieuse.

Les membres (commissaires)

Jean-Paul AMOUDRY, sénateur de la Haute-Savoie
Secteur: Banques et crédit

Jean-Paul Amoudry est membre de la CNIL depuis janvier 2009.

Hubert BOUCHET, membre du Conseil économique et social
Secteur: Ressources humaines
Hubert Bouchet est membre de la CNIL depuis novembre 1990, il a été vice-président délégué de février 1999 à août 2004.

Jean-François CARREZ, président de chambre honoraire à la Cour des comptes
Secteur: Éducation et enseignement supérieur
Jean-François Carrez est membre de la CNIL depuis janvier 2009.

Jean-Marie COTTERET, professeur émérite des universités
Secteurs: Police nationale et sûreté de l'État
Jean-Marie Cotteret est membre de la CNIL depuis janvier 2004. Il est membre élu de la formation contentieuse.

Claire DAVAL, avocate
Secteur: Justice
Claire Daval est membre de la CNIL depuis février 2009. Elle est membre élu de la formation contentieuse.

Claude DOMEIZEL, sénateur des Alpes-de-Haute-Provence
Secteur: Développement durable et logement
Claude Domeizel est membre de la CNIL depuis décembre 2008.

Didier GASSE, conseiller maître à la Cour des comptes
Secteur: Télécommunications et internet
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 GOSSELIN, député de la Manche
Secteur: Questions fiscales et sociales
Philippe Gosselin est membre de la CNIL depuis juin 2008.

Sébastien HUYGHE, député du Nord
Secteur: Identité, défense et affaires étrangères
Sébastien Huyghe est membre de la CNIL depuis juillet 2007. Il est membre élu de la formation contentieuse.

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

Jean MASSOT, président de section honoraire au Conseil d'État
Secteur: Santé et assurance-maladie
Jean Massot est membre de la CNIL depuis avril 2005.

Marie-Hélène MITJAVILE, conseiller d'État
Secteur: Recherche et statistiques
Marie-Hélène Mitjavile est membre de la CNIL depuis janvier 2009.

Bernard PEYRAT, conseiller honoraire à la Cour de cassation
Secteur: Commerce et marketing
Bernard Peyrat est membre de la CNIL depuis février 2004. Il est membre élu de la formation restreinte.

Dominique RICHARD, consultant
Secteur: Affaires culturelles et sportives
Dominique Richard est membre de la CNIL depuis janvier 2009.

Commissaires du gouvernement

Élisabeth ROLIN

Catherine POZZO DI BORGO, adjointe

LES SERVICES AU 1er DÉCEMBRE 2009

Secrétaire général

Yann PADOVA

DIRECTION DES AFFAIRES JURIDIQUES, INTERNATIONALES ET DE L'EXPERTISE

DIRECTION DES RELATIONS AVEC LES USAGERS ET DU CONTRÔLE

DIRECTION DES RESSOURCES HUMAINES, FINANCIÈRES ET INFORMATIQUES

LA CNIL EN CHIFFRES

719 délibérations

En 2009, la CNIL a siégé 48 fois au cours de 35 séances plénières, 13 formations contentieuses. Ces réunions ont conduit à l'adoption de 719 délibérations.

Les délibérations de la CNIL sont disponibles sur le site Légifrance : www.legifrance.gouv.fr

La liste des délibérations adoptées en 2009 est disponible sur le site de la CNIL : www.cnil.fr/deliberations/2009/

4265 plaintes

2217 demandes d'accès aux fichiers de police et de gendarmerie

68 185 déclarations de fichiers

En 2009, la CNIL a enregistré 68 185 nouveaux traitements de données personnelles.

Depuis 1978, ce sont au total 1 356 579 fichiers qui ont été déclarés à la CNIL.

1 500 correspondants « Informatique et Libertés » représentant 6 000 organismes

Au titre du conseil et de l'expertise

7 avis sur projet de loi ou de décret

1 recommandation

Au titre des contrôles et des sanctions

270 contrôles

91 mises en demeure

5 sanctions financières

4 avertissements

Au titre de la simplification

7 autorisations uniques

2 dispenses de déclaration

1 avis sur un acte réglementaire unique

Au titre des formalités déclaratives

544 autorisations

5 refus d'autorisation

35 avis sur des traitements sensibles ou à risques

900 autorisations relatives à des systèmes biométriques (700 en 2008)

3 054 déclarations relatives à des systèmes de vidéosurveillance (2 588 en 2008)

LES MOYENS DE LA CNIL

Le personnel

La CNIL dispose en 2009 de 132 postes budgétaires, soit 65% de plus qu'en 2004 (80 postes). La création de 12 postes supplémentaires par rapport à 2008 représente une augmentation annuelle de 10% des effectifs.

L'année 2009 voit donc se confirmer une tendance à l'augmentation régulière des personnels de la CNIL qui s'est amorcée en 2004 avec la réforme de la loi « Informatique et Libertés ».

L'augmentation constante des effectifs depuis 2004 est la réponse à cet accroissement très sensible des missions confiées par le législateur : contrôles, sanctions, animation du réseau des correspondants, conseil, pédagogie auprès du grand public, autorisation des fichiers les plus sensibles, labellisation, veille et expertise informatique, etc. Les postes supplémentaires créés ont ainsi permis à la Commission de répondre en partie, d'une part, au fort accroissement de son activité et, d'autre part, à la nécessaire modernisation de son organisation, induite notamment par ses nouvelles missions.

Par ailleurs, le renforcement des moyens en personnels permet, peu à peu, d'amener les effectifs de la CNIL au niveau de ceux de ses homologues européens et des principales autorités administratives indépendantes nationales.

Les crédits

Le budget global de la Commission a augmenté de 100% entre 2004 et 2009, répondant ainsi à l'augmentation importante des missions de la CNIL. L'accroissement du budget global est de 14% par rapport à 2008.

L'évolution de la dotation budgétaire est cependant différente selon les types de crédits qui composent le budget de la Commission.

Les crédits de personnel représentent près de 64% du budget global. Ils ont augmenté de 15% par rapport à 2008, compte tenu notamment de l'obtention de 12 postes budgétaires supplémentaires.

Les crédits de fonctionnement ne représentent que 36% du total. Ils ont augmenté de moins de 12% par rapport à 2008.

Depuis 2004, l'augmentation des crédits de fonctionnement ne suit pas systématiquement celle des crédits de personnels. Ainsi, après la forte hausse de 2006, liée à la concrétisation du projet de déménagement de la CNIL sur un site unique, le budget de fonctionnement a augmenté à un rythme moins rapide que les crédits de personnels. Ceci signifie que la Commission a mené des efforts de rationalisation et a cherché à faire des économies, bien qu'elle se situe dans le contexte d'un accroissement constant de son activité. Ainsi, le ratio des dépenses de fonctionnement par agent, hors dépenses d'immobilier, est constant entre 2004 et 2009.

Il convient également de souligner que l'augmentation du budget de fonctionnement obtenue en loi de finances initiale 2009, d'environ 512 000 €, a été amputée en gestion de près de 201 000 €, dans le cadre des mesures de précaution prévues par la loi organique relative aux lois de finances (LOLF).

En 2010, le budget de fonctionnement connaîtra une nouvelle augmentation, due principalement à l'extension des locaux de la Commission. Cet accroissement de la surface immobilière est en effet rendu nécessaire par l'augmentation constante des effectifs depuis le dernier déménagement (+ 39% entre 2006 et 2009).

Évolution des moyens de la CNIL (loi de finances initiale)

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

	2004	2005	2006	2007	2008	2009	Évolution 2009-2004	
							en nombre	en %
Postes	**80**	**85**	**95**	**105**	**120**	**132**	**52**	**65%**
Crédits (en M€)	**6,5**	**7,2**	**9,0**	**9,9**	**11,4**	**13,0**	**6,5**	**100%**
- dont personnels	*4,2*	*4,7*	*5,3*	*6,1*	*7,2*	*3,3*	*4,1*	*98%*
- dont fonctionnement	*2,3*	*2,5*	*3,7*	*3,8*	*4,2*	*4,7*	*2,4*	*104%*

Les moyens alloués à la CNIL ont augmenté de manière significative pour répondre aux nouvelles missions qui lui ont été confiées en 2004 démontrant ainsi l'attachement du gouvernement à l'action de notre autorité. Un effort est encore nécessaire pour rejoindre les pays de taille comparable en Europe. Afin de bénéficier de ressources financières propres, la CNIL avait envisagé la mise en place d'une contribution annuelle versée par chaque structure gérant des traitements de données à caractère personnel. Le Gouvernement n'a pas retenu ce projet pour l'instant.

LISTE DES ORGANISMES CONTRÔLÉS EN 2009

ASSOCIATION

ASSOCIATION COLO-VIDÉO

EZRAT MENA'HEM

MUSLIM HANDS

OHR HANNA

ASSURANCE

AIG

BUREAU COMMUN D'ASSURANCES COLLECTIVES

GAN ASSURANCES

PREMAVALS

BANQUE

BANQUE POPULAIRE DU NORD

CAISSE D'ÉPARGNE

CRÉDIT AGRICOLE NORD DE FRANCE

CRÉDIT MUTUEL OCÉAN

SOCIÉTÉ FIDUCIAIRE INTERNATIONALE D'AUDIT

COLLECTIVITÉS LOCALES

CCAS D'AUCH

COMMUNE D'ANSIÈRES-SUR-SEINE

COMMUNE D'AUCH

COMMUNE DE BUSSY-SAINT-GEORGES

COMMUNE DE CHARTRES

COMMUNE DE COLMAR

COMMUNE DE LANCON

COMMUNE DE PANTIN

COMMUNE DE MOUANS-SARTOUX

COMMUNE DE NANTES

COMMUNE DE RENNES

COMMUNAUTÉ D'AGGLOMÉRATION DE BAYONNE ANGLET BIARRITZ COMMUNAUTÉ D'AGGLOMÉRATION DE CLERMONT-FERRAND

COMMUNAUTÉ DE COMMUNES DE GATINES ET CHOISILLES

COMMUNAUTÉ URBAINE DE LYON

CONSEIL GÉNÉRAL DE L'ESSONNE

COMMERCE

ABCD COPIEUR

ADAGE

ADECCO MÉDICAL

ALGOE

ALTIZEM

AK-A

APTITUM

ANDREW MAC ALLISTER

ARMATIS

ARMATIS CENTRE

ARK-DATA

ATEL ÉNERGIE SAS

BENOIST GIRARD SAS

BIS MÉDIA

CABINET COUTOT-ROEHRIG

CARREFOUR

CDISCOUNT

CLUB MÉDITERRANÉE

COMPUTER FUTURES SOLUTIONS

COGNIS FRANCE

CORA

CRAVE AURÉLIE

DÉCISION MD

DIRECT MAILING

DOM'VILLE'SERVICES
EFFERVESCENCE
ENCORE ET TOUJOURS
ENTREPARTICULIERS. COM
ESPACE CHIC
EUROPÉENNE DE PRODUITS DE BEAUTÉ
F2M
FNAC
FOTOVISTA
GESTHOTEL PARIS GARE DU NORD/CHÂTEAU LANDON
GROUPE EXPO NEWS
GO VOYAGES
HABITALIS
HAYS FINANCE
HAYS OUEST
H CONSULTANTS
HELIODESS SERVICES
HERMIEU IMPRESSIONS ET SERVICES
HOLDIMAT RESTAURATION
HONORA CONTACT
HÔTEL DE CASTIGLIONE
HÔTEL L'AMIRAL
HÔTEL VERLAIN
IBIS BERCY VILLAGE
INDIVISION POMMERET
INFOR CRÉANCES
INSTITUT DE SONDAGE LAVIALLE
INTERNATIONAL FLAVORS & FRAGRANCES
J. MILLIET BERCY BISTROT CASH
LA MARQUE ROSE
LIBERAD MEDIA
LOCATIONDEVOITURES.COM
LOUVRE HÔTELS
MARKETING CONSEIL FINANCE
MCAFEE
MDR & ASSOCIES
MEDIACOMM
MICHAEL PAGE INTERNATIONAL
NETMAKERS
NEXENCE
NIM
NOVATRANS
OPTICAL CENTER
QUIVIDI
PERITESCO
PITCH PROMOTION
RAFFAULT SHF
RÉGIE PUBLICITAIRE DES TRANSPORTS PARISIENS (METROBUS)
RHEVOLUTIONS
SAS GRANVIDIS
SELECTA
SELECT TRAITEMENT
SODILANDES
STENTORIUS
STHREE
TECHNI MURS 18
TÉLÉPERFORMANCE CENTRE-EST
TÉLÉPERFORMANCE CENTRE-OUEST
TÉLÉPERFORMANCE GRAND-SUD
TÉLÉPERFORMANCE NORD-CHAMPAGNE
TJM
THE WALT DISNEY COMPANY FRANCE
TLG
TREND CORNER COM
VIRGIN STORES
VOGAGES DIFFERENCES
UCM
WOK TO US

CULTURE

BENCHMARK GROUP
FRANCE TÉLÉVISIONS SERVICES
GOOGLE FRANCE
M2N TECHNOLOGIES
MEETIC
SOCIÉTÉ D'EXPLOITATION SPORTS ET ÉVÉNEMENTS

TROMBI ACQUISITION

VIADEO

ÉDUCATION

ACADOMIA GROUPE

AGESCAL INSTITUTION STE URSULE

AIS 2

CAMAS FORMATION

COMPLÉTUDE

LYCÉE NOTRE-DAME

MINISTÈRE DE LA SANTÉ ET DES SPORTS

SNGS

FINANCES PUBLIQUES

GIE DES HUISSIERS AUDIENCIERS DE PARIS

GIE GROUPEMENT PÉRIPHÉRIQUE

GROUPEMENT DES POURSUITES EXTÉRIEURES

INDUSTRIE

ADB FRANCE

COMPAGNIE D'ENTREPRISE MÉCANIQUE ET ÉLECTRIQUE

COCA COLA SERVICES FRANCE

DANONE

DURAN

EDF

FOSTER WHEELER FRANCE

GROUPE BACARDI FRANCE

ICO POLYMERS FRANCE

JOHNSONDIVERSEY FRANCE

LYONNAISE DES EAUX FRANCE

MICHELIN

OTIS

PAINDOR ROUSSEAU

RABAUD SAS

RENAULT TRUCKS

SPANDEX FRANCE SAS

SEE VILLARD

VÉOLIA PROPRETÉ

LOGEMENT

IMMOBILIÈRE EUROPE SÈVRES

MINISTÈRE

MINISTÈRE DES AFFAIRES ÉTRANGÈRES ET EUROPÉENNES

POLICE – JUSTICE

CENTRE PÉNITENTIAIRE DE LIANCOURT

MINISTÈRE DE L'INTÉRIEUR – COMMISSARIAT DU XV^{e}

PRÉFECTURE DES ALPES-MARITIMES

PRÉFECTURE DES PYRÉNÉES-ORIENTALES

PRÉFECTURE DU PAS-DE-CALAIS

SCP AYNE JEAN-LUC-DURROUX BRUNO-LANCON LUC

SCP ELDIN DANY-BAUDIA PIERRE-GUILLEMAIN BRIGITTE

SCP LE DOUCEN ALAIN-CANDON PATRICK

SCP NEKADI JEAN-MARIE-PEYRACHE THIERRY-DUMAS JEAN-MARC

SANTÉ

AMBULANCES MATELLI

AMBULANCES PAYAN

CENTRE MUNICIPAL DE SANTÉ EUGÈNE ET MARIE-LOUISE CORNET

CENTRE MUNICIPAL DE SANTÉ SAINTE MARGUERITE

CENTRE MUNICIPAL DE SANTÉ TENINE

CENTRE HOSPITALIER DU MANS

CLINIQUE AMBROISE PARE

CLINIQUE ARAGO

HÔPITAL PRIVÉ DE MARNE LA VALLÉE

INSTITUT ARNAULT TZANCK

INSTITUTION NATIONALE DES INVALIDES

JANSSEN CILAG

LABORATOIRES DARPHIN

SANOFI AVENTIS

SECUREX MEDICAL SERVICES

SPACELABS HEALTHCARE

SÉCURITÉ PRIVÉE

AGENCE LEPRIVE

AGIRE

ALBERT LACAVE

BRUN SERGE FRANÇOIS

CABINET ARC

EUROPE ENQUÊTES

HOIST

INTRUM JUSTITIA

LA PARISIENNE DE PHONING

MANUS FACILITIES MANAGEMENT

PARISIENNE DE POURSUITES

POUEY INTERNATIONAL

POUEY INTERNATIONAL SA

POUEY RENSEIGNEMENT COMMERCIAL GARANTI

TDA CONSEIL

VALTIS RHONE-ALPES

VERIFDIPLOMA

VMP INVESTIGATIONS

WORLDMISSING

SPORT

CLUB SPORTIF SEDAN ARDENNES

FC LORIENT BRETAGNE SUD

FIRST LADY ISSY

LADY FITNESS PARIS 17

MANTES FITNESS

OLYMPIQUE LYONNAIS

OLYMPIQUE LYONNAIS GROUPE

PARIS SAINT GERMAIN FOOTBALL (PSG)

PSG MERCHANDISING

SOCIÉTÉ BORDELAISE DE SPORTS ET LOISIRS

SOCIÉTÉ ESPACE FORME

SOFRE

VOUTE SPORT

123 PARIS FITNESS

TRANSPORT

ACHEMINEMENT COOPÉRATIF DEUX-SÉVRIEN

AIGLE AZUR TRANSPORTS AÉRIENS

ALIS

CENT POUR CENT EXPRESS

CORSICA FERRIES

KÉOLIS ARTOIS

KÉOLIS LA ROCHE-SUR-YON

RÉGIE AUTONOME DES TRANSPORTS PARISIENS (RATP)

SERVICES LIVRAISONS DOMICILE

SNCF

SYNDICAT MIXTE DES TRANSPORTS EN COMMUN DE L'AGGLOMÉRATION TOULOUSAINE

TRANSPOLE

TRANSPORTS GEORGES-BERNARD

TRANSPORTS MANUTENTION COUTURIER

UCT

LISTE DES SANCTIONS PRONONCÉES EN 2009

Date	Nom ou type d'organisme	Décision adoptée	Thème
Janvier 2009	KÉOLIS RENNES	**Avertissement**	– Billettique – Restriction à la souscription du passe anonyme
Février 2009	DIRECTANNONCES	**Sanction pécuniaire de 40 000 €**	– Collecte déloyale d'annonces immobilières de particuliers
Mars 2009	Organisme public *	**Avertissement**	– Vote électronique (défaut de confidentialité et de sécurité des données)
Mars 2009	Organisme public *	**Avertissement**	– Vote électronique (défaut de confidentialité et de sécurité des données)
Avril 2009	Société JEAN-MARC-PHILIPPE	**Sanction pécuniaire de 10 000 €**	– Vidéosurveillance constante des salariés
Avril 2009	Groupement d'huissiers *	**Non lieu à statuer (mise en conformité de l'organisme)**	– Faille de sécurité
Mai 2009	OPTICAL CENTER	**Sanction pécuniaire de 5 000 €**	– Absence de prise en compte du droit d'opposition à recevoir de la prospection commerciale
Juillet 2009	Groupement d'huissiers *	**Avertissement**	– Faille de sécurité
Juillet 2009	SCP Huissiers	**Sanction pécuniaire de 10 000 €**	– Enregistrement de commentaires excessifs sur les débiteurs (santé, infractions…)
09/07/09	SCP Huissiers	**Sanction pécuniaire de 10 000 €**	– Enregistrement de commentaires excessifs sur les débiteurs (santé, infractions…)

* Sanctions non rendues publiques.

LEXIQUE « INFORMATIQUE ET LIBERTÉS »

Aletres professionnelles («whistleblowing»)

C'est un outil mis à la disposition des salariés. Il peut s'agir par exemple d'un numéro de téléphone « ligne éthique » ou d'une adresse électronique particulière. Ce dispositif leur permet de signaler des problèmes pouvant sérieusement affecter l'activité d'une entreprise ou engager gravement sa responsabilité.
Les alertes recueillies sont ensuite vérifiées, dans un cadre confidentiel, et permettent à l'employeur de décider, en connaissance de cause, des mesures correctives à prendre.
Ce dispositif est-il obligatoire ?
Compte tenu de la multiplicité des voies d'alertes déjà disponibles dans les entreprises (voie hiérarchique, commissaires aux comptes, fonctions de l'audit ou de la conformité interne, représentants du personnel, inspection du travail, etc.), le dispositif d'alerte professionnelle ne peut être que facultatif. Un salarié ne peut pas être sanctionné s'il ne souhaite pas l'utiliser.

BCR

BCRs signifie « Binding Corporates Rules » ou règles d'entreprise contraignantes. Ces règles internes applicables à l'ensemble des entités du groupe contiennent les principes-clés permettant d'encadrer les transferts de données personnelles, de salariés ou de clients et prospects, hors de l'Union européenne.
Ces BCRs sont une alternative au Safe Harbor (qui ne vise que les transferts vers les États-Unis) ou aux Clauses contractuelles types adoptées par la Commission européenne. Elles garantissent qu'une protection équivalente à celle octroyée par la directive européenne de 1995 s'applique aux données personnelles transférées hors de l'Union européenne.

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…).

Biométrie sans trace ou avec trace ?

Parmi toutes les données biométriques utilisées aujourd'hui, certaines présentent la particularité de pouvoir être capturées et utilisées à l'insu des personnes concernées. C'est le cas, par exemple des empreintes génétiques puisque chacun laisse involontairement derrière soi des traces, même infimes, de son corps, dont on peut extraire l'ADN. C'est également le cas des empreintes digitales, dont on laisse aussi des traces, plus ou moins facilement exploitables, dans beaucoup d'actes de la vie courante.
D'autres données biométriques ne présentent pas, du moins dans l'état actuel de la technique, cette particularité : c'est le cas, par exemple, du réseau veineux du doigt ou du contour de la main, car ces données biométriques laissent peu de trace au quotidien, voire aucune.
La biométrie avec trace impose donc une vigilance toute particulière de la part des personnes concernées.

Cloud computing

Le Cloud Computing (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau.
Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (Cloud) composé de nombreux serveurs distants interconnectés.
D'un point de vue « Informatique et Libertés », ce concept soulève des problématiques de sécurité, de qualification des parties, de droit applicable, d'exercice effectif des droits et d'encadrement des transferts internationaux de données personnelles.

CNIL

Autorité administrative indépendante, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers : 4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 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 5 ans.

Conférence mondiale des commissaires à la protection des données et à la vie privée

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

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 ; en contrepartie de sa désignation, les traitements de données personnelles les plus courants sont exonérés de déclarations auprès de la CNIL.

Déclarant

Personne physique ou morale responsable d'un traitement ou d'un fichier contenant des données personnelles qu'il doit déclarer à la CNIL sous peine de sanctions.

Destinataire

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

Discovery

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

DMP (Dossier médical personnel)

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

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 (ex. 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.

DP (Dossier pharmaceutique)

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

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 lorsqu'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.

Fichier central de crédit ou fichier positif

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

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.

FNAEG

Fichier national des empreintes génétiques
Le FNAEG sert à faciliter l'identification et la recherche :
– des auteurs d'infractions à l'aide de leur profil génétique ;
– des personnes disparues à l'aide du profil génétique de leurs descendants ou de leurs ascendants.
Le FNAEG est placé sous la responsabilité de la direction centrale de la Police judiciaire au ministère de l'Intérieur, sous le contrôle d'un magistrat.

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 €.

G29

L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationale. Cette organisation réunissant l'ensemble des CNIL européennes a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays tiers et de conseiller la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles. Le G29 se réunit à Bruxelles en séance plénière tous les deux mois environ.

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 (Numéro d'inscription au) répertoire

Le NIR 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.

PNR (Passenger Name Record)

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

Reconnaissance faciale

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

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.

RFID (Radio Frequency Identification)

Les puces RFID permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micropuce (également dénommée étiquette ou tag) et d'une antenne qui dialoguent par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. Pour les applications dans la grande distribution, leur coût est d'environ 5 centimes d'euros.
D'autres puces communicantes, plus intelligentes ou plus petites font leur apparition avec l'avènement de l'internet des objets. Certains prototypes sont quasi invisibles (0,15 millimètre de côté et 7,5 micromètres d'épaisseur) alors que d'autres, d'une taille de 2 mm^2, possèdent une capacité de stockage de 512 Ko (kilo-octets) et échangent des données à 10Mbps (méga bits par seconde).

Séance plénière

C'est la formation qui réunit les 17 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.

SWIFT (Society for Worldwide Interbank Financial Telecommunication)

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

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.

VIS (Visa Information System)

Le VIS est destiné à améliorer la mise en œuvre de la politique commune en matière de visas, en permettant la mise en commun et l'échange entre États membres de l'Union européenne de données relatives aux demandes de visas Schengen qui leur sont adressées. Le système repose sur une base centrale européenne reliée aux systèmes nationaux. Il 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 Schengen, soit à terme, environ cent millions d'individus.

« Web médecin »

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

Crédits photo :
Rémy Malingrëy – Iconovox : p. 16, 17, 21, 30, 77
Mric – Iconovox : p. 23
Fotolia : p. 25, 36, 65, 69, 70, 73, 81, 82
CNIL : p. 63
Martin Vidberg : p. 78