Conférence de presse
16 mai 2008

Présentation du 28ème rapport d'activité 2007

La CNIL en 2007 : toujours plus !

L'année 2007 a encore une fois souligné une activité en pleine croissance pour la CNIL qui s'est traduite par une augmentation sensible du nombre de plaintes, de demandes de droit d'accès indirect, de contrôles, de sanctions, de délibérations, etc.
Trente ans après sa création, la CNIL réaffirme sa position, tant au niveau national qu'international, puisqu' Alex Türk vient d'être élu à la présidence du groupe des CNIL européennes (G29). Pour célébrer ses trente ans, la CNIL organisera du 15 au 17 octobre 2008 avec la Commission Allemande, également trentenaire, la 30ème conférence mondiale de la protection des données et de la vie privée à Strasbourg au Conseil de l'Europe. L'année 2008 s'annonce donc riche en événements et en actions.

La CNIL en chiffres

En 2007, la CNIL a :

- **enregistré 56 404 traitements de données nominatives**
- **reçu 4 455 plaintes** (+25% par rapport à 2006)
- **reçu 2 660 demandes de droit d'accès indirect** (+67 % par rapport à 2006)
- **adopté 395 délibérations** (+ 32% par rapport à 2006)
- **effectué 164 contrôles** (+21 % par rapport à 2006)
- **adressé 101 mises en demeure**
- **adressé 5 avertissements**
- **prononcé 9 sanctions financières** pour un montant de 175 000 euros

Les moyens

Grâce aux 15 postes supplémentaires obtenus en 2008, la CNIL comptera 120 postes à la fin de cette année.

Cependant, au regard des missions qui lui sont dévolues et des comparaisons internationales avec ses homologues notamment européens, cet effort devra être soutenu et poursuivi. L'accroissement de l'activité est en effet plus rapide que ce qui avait été envisagé en 2004 et 2005. En termes d'effectifs globaux, l'autorité anglaise comprend 260 agents et l'autorité allemande près de 400 ; l'autorité canadienne dispose quant à elle de 300 agents (pour une population totale de 30 millions d'habitants).

Rattachée au budget de la Justice, la CNIL est souvent assimilée à un service parmi d'autres d'une administration centrale, sans considération pour son indépendance, pourtant spécifique et voulue par le législateur. Son statut d'Autorité Administrative Indépendante n'est qu'une formule si son indépendance n'est pas réellement assurée.

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

Les séances plénières

Au cours de l'année 2007, la CNIL a siégé 40 fois et adopté **395 délibérations**.

Parmi les décisions prises en 2007 par la CNIL, il convient de relever :

- **214 autorisations**
- **26 refus d'autorisation**
- **22 avis sur des traitements sensibles ou à risques**
- **6 avis sur des projets de loi ou de décret**
- **4 autorisations uniques**
- **1 682 autorisations de transferts de flux transfrontières**

Les plaintes

La CNIL a reçu 4 455 plaintes de particuliers ayant rencontré des difficultés à exercer leurs droits « informatique et libertés », **soit 25% de plus qu'en 2006**. La CNIL reçoit aujourd'hui deux fois plus de plaintes qu'il y a 10 ans !
Les secteurs d'activité qui ont suscité le nombre le plus important de plaintes en 2007 sont: la banque-crédit, la prospection commerciale, le travail, les télécommunications.

Le droit d'accès indirect

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

Ces demandes concernent en général plusieurs fichiers et nécessitent en conséquence de nombreuses vérifications.
En 2007 la CNIL a clôturé 2350 demandes (soit 71% de plus qu'en 2006). L'instruction de ces demandes a nécessité 5000 vérifications de dossiers.
Le stock de demandes droit d'accès indirect reste important : aujourd'hui, 2898 saisines sont en cours (arrivées entre 2002 et 2007) dont 1450 datant de 2007 et 568 de 2006.

En 2008, la CNIL a déjà reçu près de 600 demandes de droit d'accès indirect.

Les contrôles

- **164 contrôles effectués**
  - une augmentation de 21% par rapport à 2006
- **40% des contrôles réalisés font suite à des plaintes de particuliers ou des signalements déposés sur le site internet de la CNIL**
- **101 mises en demeure, 9 sanctions financières pour un montant de 175 000 euros et 5 avertissements résultent des contrôles**

En 2007, les missions de vérification sur place ont porté sur des sujets tels que :

- les dispositifs biométriques des établissements scolaires, des entreprises ou des structures médicales ;

- la prise en compte du droit d'opposition des personnes à être démarchées commercialement par téléphone par des organismes appartenant à des secteurs d'activité très hétérogènes, que ce soit des banques ou des installateurs de fenêtres ;
- les conditions de conservation des données « de connexion » (données relatives au trafic des communications électroniques ;
- l'expérimentation du dossier pharmaceutique ;
- les systèmes de vidéosurveillance ;
- les fichiers concernant les salariés ;
- l'information des personnes par les opérateurs de communications électroniques ;
- les fichiers dits « de police », d'importance nationales.

On relèvera que près d'un tiers des contrôles a donné lieu à l'engagement d'une procédure de sanction devant la formation contentieuse.

Les sanctions

Le renforcement en personnel du service des sanctions a permis de faire croître son activité de plus de 30% par rapport à 2006. Le nouveau rôle de contrôle *a posteriori* de la CNIL est mis en exergue par la formation restreinte dite « contentieuse » depuis 2004.
Les principaux secteurs concernés dans les dossiers de la formation restreinte sont les organismes bancaires et de crédit ainsi que les sociétés de démarchage commercial. Plus d'un tiers des dossiers ont trait au non-respect des obligations de la loi en matière d'information des personnes et de droit d'opposition.

- 9 sanctions financières ont été prononcées correspondant à des amendes allant de 5 000 à 50 000 euros (pour un total de 175 000 euros).
- 120 procédures ont été engagées (soit 30 % de plus qu'en 2006).

Les correspondants informatique et libertés

Désigner un correspondant permet certes de bénéficier d'un allègement des formalités déclaratives mais surtout de s'assurer que l'informatique de l'organisation se développera sans danger pour les droits des usagers, des clients et des salariés. C'est aussi, pour les responsables de fichiers, le moyen de se garantir de nombreux risques résultant d'une mauvaise application du droit en vigueur.

Aujourd'hui, **2 438 organismes ont désigné un correspondant** (dont 80% dans le secteur privé). Ils n'étaient que 73 organismes en 2005 et 650 en 2006.

La CNIL propose une cellule entièrement dédiée aux correspondants leur offrant un accueil privilégié et prioritaire. Par ailleurs, elle organise des journées d'information généraliste ou thématiques « sur mesure » pour les correspondants désignés.

Ça la fiche mal ! Histoires vécues.

A l'occasion de la publication de son rapport annuel 2007, la CNIL présente des histoires vécues par des personnes qui ont rencontré des difficultés à défendre leurs droits et que la CNIL a aidés. Elle entend ainsi, au travers d'histoires vraies, mieux faire connaître les droits à la protection des données personnelles.

- ***Kafka à l'ère numérique : quand l'usurpation d'identité vire au cauchemar***

Monsieur R., jeune père de famille, décide de se rendre à San Francisco, via Pittsburgh, pour quelques jours de vacances. Lors de l'escale à Pittsburgh, les services de l'immigration américaine lui signalent qu'il est fiché et accusé d'avoir tiré sur un policier allemand à Francfort. Suivent alors un interrogatoire en règle avec fouille corporelle, prise de photos et d'empreintes. Après des échanges verbaux assez vifs avec les autorités, il est amené en quartier d'isolement à la prison fédérale de Pittsburgh pour être incarcéré avec trois co-détenus. Au bout de quelques heures, les services de l'immigration sont venues le chercher, chaînes aux pieds, à la taille et aux mains pour l'autoriser à passer deux appels. Il a ensuite été raccompagné par cinq personnes pour être extradé par avion vers la France.

Dès son arrivée à Paris, Monsieur R a établi un procès-verbal à la PAF et déposé plainte pour usurpation d'identité. En effet, un ressortissant du Maghreb, figurant dans de nombreux avis de recherche à propos du meurtre de quatre policiers, utilisait son passeport falsifié perdu quelques années auparavant.

Saisie par Monsieur R de son problème d'usurpation d'identité, la CNIL a procédé à des investigations dans les fichiers du Ministère de l'intérieur, de la Défense et d'Interpol.

Malheureusement pour Monsieur R, celui-ci figure toujours dans certains fichiers qui rendent ses déplacements très difficiles. Il n'a pas été possible de supprimer totalement son signalement car ce serait « donner carte blanche » à l'usurpateur, selon les autorités compétentes.

- ***Manifs lycéennes : classement sans suite…à suivre de près***

Les parents d'un mineur ont saisi la CNIL pour savoir s'il existait des informations concernant leur fils dans les fichiers de police judiciaire et dans l'affirmative d'en vérifier la conformité.

L'adolescent avait posé des chaises devant un lycée pour contester la suppression des épreuves du bac blanc. Ces faits avaient donné lieu à un classement sans suite pour insuffisance de charges mais l'ADN et les empreintes du jeune homme avaient été relevés durant l'enquête.

Les investigations de la CNIL ont mis en évidence que le jeune homme était fiché en tant que mis en cause dans le STIC, le FAED et le FNAEG. Le procureur de la république ayant été saisi, ces signalements vont finalement être supprimés. L'intervention de la CNIL a donc permis au jeune homme d'éviter toutes les conséquences défavorables que ces fichages erronés auraient pu engendrer pour son avenir.

- ***Quand un témoin devient mis en cause…c'est mal fiché !***

Mademoiselle C., souhaitant présenter un concours d'entrée à une école de police, était enregistrée dans le STIC en tant que mis en cause, alors qu'elle avait été uniquement entendue en tant que témoin dans une affaire de trafic de produits anabolisants par la sûreté départementale compétente.

A l'issue du contrôle de la CNIL, les informations la concernant ont été supprimées du STIC, et cette personne a pu, de nouveau, présenter le concours qu'elle souhaitait.

- ***Rester dans le STIC peut nuire à la création d'entreprise***

Monsieur D. souhaitait créer une société de surveillance et de gardiennage privés. Or, il a fait l'objet d'un refus d'agrément de la part du préfet territorialement compétent au motif qu'il était fiché dans le STIC en tant que mis en cause.

A l'issue du contrôle de la CNIL, les informations enregistrées dans le STIC concernant Monsieur D. ont été supprimées, la durée de conservation des données étant dans le cas d'espèce expirée, ce qui lui a enfin permis de créer son entreprise.

En effet, les données n'avaient pas été supprimées par la logiciel d'épurement en raison de l'absence de précision du nombre de jours d'interruption temporaire de travail, qui a une conséquence directe sur la durée de conservation des informations dans le STIC.

- ***Comment perdre son travail parce que l' on est fiché à tort dans le STIC***

Monsieur B. occupait un emploi dans une société de sécurité. A l'occasion de l'instruction de sa demande de renouvellement d'habilitation pour accéder aux zones réservées aéroportuaires, au cours de laquelle les fichiers de police judiciaire peuvent être consultés, il s'est avéré qu'il était fiché dans le STIC en tant que mis en cause, ce qui était susceptible de conduire le préfet territorialement compétent à refuser cette habilitation et, de fait, à lui faire perdre son emploi.

Au terme des investigations menées par la CNIL, il est apparu que Monsieur B. était enregistré dans le STIC à tort, puisque les faits de violence volontaire retenus à son encontre n'ayant pas entraîné d'interruption temporaire de travail, il n'étaient passibles que d'une contravention de 4ème classe.
En conséquence, Monsieur B. a conservé son emploi.

LE DROIT D'ACCES INDIRECT

Toute personne peut demander à la CNIL de vérifier les informations la concernant éventuellement enregistrées dans des fichiers intéressant la sûreté de l'Etat, la défense ou la sécurité publique : police judiciaire, gendarmerie nationale, renseignements généraux, DST (Direction de la Surveillance du Territoire), DGSE (Direction Générale de la Sécurité Extérieure), etc. Cette demande s'effectue par écrit à l'attention du Président de la CNIL

- ***Privée de téléphone mobile à cause d'un homonyme***

Mademoiselle B demande l'ouverture d'une ligne de téléphonie mobile dans un point de vente d'un opérateur télécoms. Un refus lui est opposé au motif qu'elle est inscrite dans le fichier Préventel qui recense les impayés de la téléphonie mobile et interdit tout nouvel abonnement à défaut de remboursement des sommes dues.

Mlle B, qui n'a jamais été cliente d'un opérateur de téléphonie mobile, interroge l'organisme responsable de ce fichier. Elle apprend ainsi que figure dans Préventel *« un homonyme exact au lieu de naissance près »* (nom, prénom, date de naissance).

Mlle B produit auprès de l'opérateur des justificatifs prouvant sa bonne foi, mais le point de vente persiste à considérer qu'elle pourrait être la débitrice défaillante inscrite dans Préventel. Face à ce nouveau refus injustifié, elle saisit la CNIL.

La CNIL demande au responsable du fichier Préventel de lui préciser le département de naissance et l'adresse postale de l'homonyme de Mlle B. Ces données sont effectivement totalement différentes de celles de Mlle B.

La CNIL communique ces informations au correspondant informatique et libertés (CIL) de l'opérateur responsable du point de vente, lui demandant de réexaminer la demande d'abonnement de Mlle B.

Un mois plus tard, l'opérateur reconnaît la bonne foi de Mlle B et précise qu'une offre d'abonnement assortie d'un geste commercial en guise de dédommagement lui a été proposée.

- ***Mal fichée et mal logée***

Madame M, en attente d'un logement social, souhaite compléter son dossier de demande de logement par l'information relative à la naissance de son fils.

Elle découvre que son dossier informatique fait état de deux précédents refus de sa part de propositions de logement social. Or, le premier refus était lié à une localisation inadaptée du logement proposé, et le second était imputable au bailleur social qui avait retiré sa proposition.

Ces mentions sont d'autant plus préjudiciables à Madame M qu'existe, dans son département, un fichier commun de la demande locative accessible aux différents bailleurs sociaux. Depuis ses deux « refus », plus aucun logement ne lui est proposé.

La CNIL interroge les bailleurs à l'origine des différentes inscriptions. Elle leur demande de mentionner dans le dossier, d'une part, l'arrivée d'un enfant au foyer de Madame M et, d'autre part, de clarifier les motifs de « refus » des deux précédentes propositions de logement, non imputables à Madame M.

Les organismes concernés y donnent rapidement une suite favorable.

Grâce à l'intervention de la CNIL, Madame M peut à nouveau se voir proposer des logements adaptés à sa situation.

- ***Interdit à tort de carte bancaire pendant deux ans***

Monsieur D se voit retirer sa carte bancaire par sa banque et est inscrit au Fichier Central des Chèques (FCC), géré par la Banque de France. Il ne peut plus avoir de carte bancaire ni ouvrir de compte dans une autre banque.

Contestant le bien-fondé de cette inscription, et n'obtenant pas de réponse de sa banque, il saisit la CNIL d'une plainte plus d'un an et demi après avoir été inscrit au FCC.

La banque confirme rapidement que cette inscription est infondée et qu'elle procède à sa radiation auprès de la Banque de France.

Mais, plusieurs mois après, Monsieur D informe la CNIL qu'il est toujours inscrit dans le FCC. Quelques jours plus tard, son inscription est automatiquement supprimée par la Banque de France, à l'expiration du délai maximum d'inscription de deux ans.

Mise en demeure de s'expliquer sur cette situation par la formation contentieuse de la CNIL, la banque indique que le défaut de suppression de l'inscription résulte d'une erreur dans la demande adressée à la Banque de France. La demande de suppression n'a ainsi pas pu être prise en compte par la Banque de France.

La banque précise les mesures qu'elle prend en interne afin que les demandes adressées à la Banque de France soient désormais réalisées correctement.

Grâce à l'action de la CNIL, d'autres clients de cette banque ne devraient pas connaître à leur tour les difficultés rencontrées par Monsieur D dans sa vie quotidienne.

- ***Dossier égaré par la banque, cliente défichée***

Madame P. de Neuilly-sur-Seine (92) se voit réclamer d'importantes sommes d'argent par sa banque pour des dettes souscrites par son ex-mari, aujourd'hui décédé. Contestant son inscription au FICP, Mme P prend attache avec un avocat. Sans réponse de sa banque, elle saisit également la CNIL. Contactée par la CNIL pour connaître les motifs et conditions d'inscription au FICP, la banque répond que le dossier de Mme P a été « égaré ». Il ne lui est donc pas possible de justifier de la régularité de cette inscription. En conséquence, la banque a déficher Mme P.

LE DROIT DE RECTIFICATION ET DE RADIATION

Toute personne peut demander directement à l'organisme qui détient un fichier que les informations détenues sur elle soient rectifiées (si elles sont inexactes), complétées (si elles sont incomplètes), mises à jour (si elles sont périmées) ou effacées (si ces informations ne pouvaient pas être collectées de manière régulière.

- ***Un numéro pas si privé que ça***

Mme R., a déménagé dans une autre région en juillet 2007 afin de fuir les violences de son ex-époux. Elle a pris un nouvel abonnement téléphonique auprès d'un opérateur et demandé expressément son inscription en liste rouge.

Par hasard, elle découvre que ses coordonnées figurent dans les annuaires publiés sur internet.

Depuis, elle vit dans la terreur que son ex-conjoint ne les retrouve, elle et sa fille âgée de 9 mois. Elle écrit et téléphone à l'opérateur qui ne prend pas en compte ses demandes de suppression de la base annuaires.

Après intervention de la CNIL l'opérateur fait finalement le nécessaire auprès des éditeurs d'annuaires sur internet pour obtenir rapidement la suppression des coordonnées de Mme R.

- ***Publicité non désirée : l'arroseur arrosé***

Madame C reçoit chez elle, sur son télécopieur, une publicité pour une société spécialisée dans la vente de vêtements qui mentionne être « en conformité avec la loi CNIL ».

Ne désirant plus recevoir cette publicité, elle manifeste son opposition en adressant un fax au numéro indiqué.

Malgré ses démarches, elle continue à recevoir en nombre cette même publicité. Elle décide alors d'alerter la CNIL.

Sur la base de plusieurs dizaines d'autres plaintes contre cette société de vente, la formation contentieuse de la CNIL la met en demeure de respecter le droit d'opposition de Mme C et des autres plaignants, et de se conformer à l'ensemble de ses obligations « informatique et libertés ».

Si les envois de fax publicitaires cessent, la CNIL constate que la société ne se conforme pas, dans le délai fixé, à toutes ses demandes. En conséquence, elle lui inflige une sanction pécuniaire de 5.000 euros. Du fait des manquements constatés, cette sanction s'accompagne d'une mesure de… publicité sur le site internet de la CNIL

LE DROIT D'OPPOSITION

Toute personne peut s'opposer, pour des motifs légitimes, à ce que les informations la concernant soient utilisées dans un fichier. Elle peut s'opposer sans frais et sans justification à ce que ses informations personnelles soient utilisées à des commerciales.

- ***C'est mon droit, c'est mon eau !***

Depuis mars 2005, Monsieur J. alerte le syndic de copropriété de son immeuble sur une erreur dans ses relevés de consommation d'eau chaude. De manière à prouver sa bonne foi, il fournit ses relevés individuels de compteur d'eau.

Or, le syndic ne justifie les charges de consommation d'eau que par une indication annuelle de consommation et non par des relevés individuels. Un tel procédé fait obstacle à toute possibilité de vérification.

Monsieur J. demande alors à avoir accès à ses relevé individuels détenus par le syndic depuis 1999, ce qui lui est refusé par le gestionnaire de l'immeuble. La CNIL adresse un courrier au syndic mis en cause pour demander que le droit de Monsieur J. soit respecté. Peu de temps après, le gestionnaire de l'immeuble adresse les documents demandés à Monsieur J.

Satisfait, ce dernier peut alors apporter la preuve de sa consommation réelle d'eau.

LE DROIT D'ACCES

Toute personne peut demander directement à l'organisme qui détient un fichier d'avoir accès, sur place ou par écrit, aux informations la concernant sous une forme accessible dans un délai de deux mois maximum.

Spécial vidéosurveillance

- ***Mangez…vous êtes filmés !***

Madame S. est gérante d'un restaurant dans le sud de la France. Depuis peu, les propriétaires des murs ont décidé d'installer des caméras de vidéosurveillance devant l'entrée de son établissement, sans concertation aucune. Inutile de dire que depuis, les clients du restaurant sont assez mécontents et que le chiffre d'affaires s'en ressent. L'équilibre économique de l'établissement est en péril. Madame S a donc saisi la CNIL récemment d'une plainte qui est actuellement en cours d'instruction du dossier.

- ***Une caméra qui fait des remous…***

Alertée par une plainte, la CNIL s'est rendue dans une piscine de la région parisienne pour vérifier sur place l'implantation de caméras de surveillance. Elle a alors constaté qu'une caméra était orientée sur un jacuzzi. L'établissement indique que cette installation particulière s'explique pour des raisons de sécurité. Mais, vérification faite par les contrôleurs de la CNIL, personne ne regarde ces images. Ensuite, les contrôleurs se rendent dans les vestiaires et constatent qu'il y a bien des caméras orientées pour filmer les espaces communs des vestiaires et les casiers. Les cabines sont bien hors du champ des caméras. Mais, tout le monde ne s'isole pas dans une cabine pour se changer et dans ce cas, comme ont pu le constater les contrôleurs sur les bandes vidéo…On peut donc s'interroger sur le caractère proportionné de ces caméras dans cette piscine.

Vu dans les fichiers !

À l'occasion de contrôles sur place, la CNIL constate régulièrement dans des fichiers des commentaires plus que « douteux ». Il peut s'agir d'études d'huissiers, de société de recouvrement de créances, d'établissements de sports et de loisirs, d'hôtels, de banques, de cabinets de recrutement, etc.
Des sanctions ont été infligées aux sociétés concernées (jusqu'à 40 000 euros récemment pour un fichier de gestion des salariés). La CNIL rappelle régulièrement aux responsables de fichiers que les « zones commentaires » offertes par certains fichiers ou logiciels sont à utiliser avec la plus grande prudence et avec objectivité. En les remplissant, il faut avoir à l'esprit que les personnes concernées peuvent y avoir accès à tout moment grâce à la loi « informatique et libertés ».

Petit florilège de commentaires constatés par la CNIL lors de contrôles … sans commentaire !

Études d'huissiers

« Carence totale, alcoolique profond, au RMI »
« séropositif depuis 23 ans »
« l'épouse du débiteur a un cancer du pancréas »
« est en instance de divorce car son mari est en prison pour avoir violé sa fille »

Société de recouvrement de créances

« famille alcoolo »

Banque /crédit

« danger ! Mme est malade nerveusement et a tendance à perdre les pédales »

Prestataire d'animations en grande surface

« bien mais râleuse »
« cerveau de dinausore »
« grosse menteuse »
« très très très chiante »
« 2tension »
« Mr je sais tout »
« bien mais un peu âgée »
« c'est dame qui pue »
« personne sans dent et qui boit »
« ne pas appeler avant 16h car mari très con »

Télémarketing

« Mme est odieuse la taquiner un peu »
« salcon »
« il est comptable et se la pète »

Hôtellerie

« branleur ne veut pas sortir de la chambre à 12h00 ne plus reprendre »
« pisse au lit et dans poubelle »

Établissements de sports et loisirs

« se travesti, ne plus prendre »
« monsieur est très con »
« femme proposant massages payants »
« ébats sexuels à 3 tente ouverte »
« injection viagra 4X4 BMW »

Cabinet de recrutement

« petite enrobée »
« a passé ses examens : elle a fait une fausse couche sans le savoir »
« le genre de personne à mettre tout le monde en copie »

C'est nouveau, ça vient de sortir !

L'invasion des puces

Les puces sans contact connaissent actuellement des utilisations de plus en plus diversifiées, au point de constituer un enjeu économique majeur. Lorsqu'un produit en comporte une, on dit qu'il est « tagué ».

Ce type de puce permettra par exemple dans un futur proche de connaître instantanément le contenu d'un caddie au supermarché. Certains médicaments ou produits de luxe sont déjà tagués pour éviter les contrefaçons. Dans les musées les visiteurs pourront bientôt, grâce à la puce contenue dans leur ticket, télécharger des contenus interactifs, en fonction de leur profil (langue, âge…).

- Au Royaume-Uni, le lycée britannique Hungerhill School de Doncaster teste un système de surveillance basé sur l'utilisation de puces RFID placées dans les uniformes des élèves. Le dispositif en question permet d'identifier un élève dès son entrée dans une classe et de l'associer à des informations personnelles telles que son âge ou son cursus scolaire.

- Dans certaines boîtes de nuit espagnoles, ce sont des puces sous-cutanées qui sont utilisées comme moyen de paiement et banalisent finalement des atteintes à l'intégrité physique.

- Quant à la sécurité des puces RFID, jusqu'ici réputées inviolables, elle est aujourd'hui remise en cause. Des chercheurs d'une université d'Amsterdam ont annoncé avoir créé un virus permettant par simple lecture d'une puce de ce type, de la contaminer et de fausser les informations qu'elles contient.

La CNIL participe à des travaux internationaux menés par la Commission européenne au sein d'un groupe d'experts qui publiera en 2008 une recommandation sur les RFID et un avis sur l'internet des objets.

En liberté surveillée

Les nouvelles technologies permettent aujourd'hui d'observer, de gérer et de surveiller avec précision des comportements de groupe ou d'individus.

- Dans le cadre du projet ELSA (Engin léger pour surveillance aérienne), le ministère de l'intérieur français a présenté un drône baptisé « ELYTRE » destiné à surveiller à distance les villes et les quartiers (en cas d'émeutes notamment)

- En Californie une expérience d'observation en temps réel du trafic autoroutier a été menée via les téléphones GPS des automobilistes.

- En Grande-Bretagne, des caméras installées sur une autoroute très fréquentée peuvent compter le nombre de voyageurs dans chaque voiture qui passe. Dans le même pays, à Middlesborough, des caméras de vidéosurveillance permettent à des employés municipaux d'admoneste en direct des contrevenants (par exemple quelqu'un qui jette un papier par terre).

- Certaines compagnies d'assurance proposent des dispositifs embarqués pour proposer une prime d'assurance adaptée à l'usage réel des véhicules.

- Deux avants-projets en matière de surveillance dans le transport aérien ont été présentés aux autorités européennes en charge de la protection des données :

- Le premier vise à installer des système de vidéos surveillance dans les avions, afin d'étudier les réactions des passagers pendant les vols et de déterminer selon des signes de nervosité des profils de personnes dites « à risque » (si tous les passagers ayant peur de l'avion sont pris pour des terroristes…).
- Le second projet consiste à observer dans les aéroports des « flâneurs », ce type de population qui déambule dans les cafés et les boutiques et fait soit-disant perdre de l'argent aux compagnies aériennes. Ici le système envisagé mêle deux technologies : la vidéosurveillance et les puces RFID (intégrées aux cartes d'embarquement).

- La diffusion des systèmes de vidéosurveillance augmente les risques d'utilisation détournée. On peut ainsi donner l'exemple du vidéoscanning consistant à filmer les caissières dans les grandes surfaces (à hauteur des articles qu'elles scannent) de manière à servir de preuve en cas de contestation d'un client. Ici le risque est évidemment qu'il y ait surveillance implicite des caissières (qui peuvent être identifiées grâce à leurs horaires de travail ou à leurs badges).

- En Grande-Bretagne, l'artiste Manu Luksch a réalisé un film de fiction produit exclusivement à base d'images capturées par les caméras de vidéosurveillance de Londres. Le film aborde le thème de l'identité dans l'espace public et met en garde contre la société de surveillance. Il interpelle également par l'ensemble des démarches légales qui ont été nécessaires à sa réalisation. L'artiste a en effet exploité la loi britannique qui autorise tout personne filmée à réclamer une copie des enregistrements où elle apparaît.

La généralisation des dispositifs biométriques

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques ou biologiques (ADN, empreintes digitales…).

- En Grande-Bretagne, la police anglaise souhaite avoir accès aux profils ADN des enfants qui ont une attitude susceptible d'indiquer qu'ils vont un jour devenir des criminels.

- Toujours en Grande-Bretagne, lors de conversations téléphoniques, des échantillons de voix de demandeurs d'aide sociale vont être mémorisés et soumis à des détecteurs de mensonge afin de démasquer les demandes d'allocations frauduleuses.

- En Allemagne la police a consacré 210 000 euros pour tester en grandeur dans une gare auprès de 200 personnes un dispositif biométrique de reconnaissance faciale par vidéosurveillance. Les conclusions en ont été que les techniques biométriques n'étaient pas encore assez efficaces pour identifier à coup sûr un suspect au milieu d'une foule.

La CNIL a autorisé trois programmes de recherche en matière de biométrie (Université Evry-Val de'Essonne, Groupement des écoles de télécommunications GET et Sagem Défense Sécurité). Ces programmes revêtent une grande importance car ils permettent à la CNIL de disposer d'évaluations fiables sur l'état des techniques. Des bilans relatisf aux résultats de ces recherche seront communiqués à la CNIL.

La surveillance des personnes vulnérables

- La maternité de Montfermeil a été la première en France à mettre en place un système de bracelets électroniques pour nouveaux nés et destiné à prévenir les risques de rapt ou d'échange de bébés.

- Au Japon des scientifiques de l'institut Riken ont présenté Ri-man, un robot qui à terme devrait permettre de venir en aide aux personnes âgées.

- On peut aussi évoquer l'exemple de la géolocalisation des patients atteints d'Alzheimer ou celle des enfants (avec par exemple des doudous équipés de puces électroniques).

La CNIL vient d'engager une réflexion sur le thème de la surveillance des personnes vulnérables avec la mise en place d' un groupe de travail présidé par Mme Anne Debet. Un rapport sera publié ultérieurement.

De qui se fiche-t-on ?

- En Grande-Bretagne, les données personnelles concernant la moitié de la population britannique ont été égarées. Le Trésor public anglais a en effet perdu deux disques durs contenant la base de données des allocations familiales (avec noms, dates de naissance, numéros de sécurité sociale et coordonnées bancaires des bénéficiaires). Cette perte a pour conséquence une augmentation pour de 11 millions d'euros du budget de l'ICO (autorité Britannique de protection des données, « CNIL Britannique »). Cette augmentation est égale au budget total de la CNIL.

- En Italie, une fuite de déclarations de revenus a été organisée par le gouvernement. Le temps de quelques heures (et d'une grosse colère du président de la Cnil italienne) les feuilles d'impôts des 40 millions de contribuables italiens ont été mises en ligne et consultables par tout un chacun. Selon le vice-ministre à l'économie Vincenzo Visco, diffuser ces informations personnelles se justifiait par une loi de 1972 sur le libre accès aux informations fiscales.

- En France, la société Réputation defender vous permet d'entretenir votre réputation sur le net en effaçant des traces de votre identité numérique, comme par exemple vos commentaires sur des blogs ou des forums. A l'origine d'un tel type de service, ce constat : en moyenne 77% des recruteurs effectuent des recherches en ligne sur les candidats à l'emploi et 35% en ont déjà éliminé en se basant sur les résultats de ces recherches.

- Une société américaine a lancé le passeport « safe sex » garantissant qu'un internaute draguant en ligne n'a pas de maladies sexuellement transmissibles. Une personne souhaitant vérifier que son partenaire potentiel est bien « sain » n'aura qu'à téléphoner à un laboratoire d'analyse avec le numéro de passeport qui aura été échangé.

La surveillance des personnes vulnérables : une vraie question de société

Bracelets électroniques pour les nouveau-nés et les personnes atteintes de la maladie d'Alzheimer, services de géolocalisation des enfants, capteurs de mouvement ou de température placés au domicile des personnes âgées, biométrie pour les travailleurs handicapés, les outils de surveillance électronique des personnes vulnérables (enfants, personnes âgées, personnes handicapées) se développent.

Le progrès technique, le contexte sécuritaire et les impératifs de gestion incitent au développement de tels dispositifs, dans le but, louable, d'assurer la sécurité des personnes vulnérables. Si envisagés au cas par cas, ces dispositifs peuvent se justifier (éviter les rapts d'enfants, permettre le maintien à domicile des personnes âgées, préserver la liberté d'aller et venir des personnes victimes de troubles du discernement …), on touche là pourtant à un changement dans les modes de vie qui nécessite un débat de société.

A défaut d'approche globale en effet, on risque de laisser se construire insidieusement, sans bruit et sans d'ailleurs que l'on puisse prêter aux intéressés de mauvaises intentions, une société de contrôle qui modifie les relations des individus entre eux et soulève des interrogations de fond au regard des principes de protection des données.

Une tendance se dessine, en effet, en faveur de la substitution de réponses techniques aux comportements humains de vigilance et le risque existe d'une déresponsabilisation des acteurs concernés (famille, personnels soignants, assistants sociaux…).

Il y a sans doute une distinction à opérer au sein des dispositifs de surveillance électronique des personnes fragiles, selon qu'ils concernent des enfants, qui font l'apprentissage de l'autonomie et des personnes en perte d'autonomie. Dans le second cas, en effet, c'est principalement la dignité des personnes qui est en cause, dans le premier, c'est plus radicalement la liberté inhérente à la construction et à l'épanouissement des individus.

Autant d'enjeux essentiels qui nécessitent une réflexion de fond que la CNIL, pour sa part, a décidé d'engager. Il n'est pas inutile à cet égard de rappeler l'article 1er de la loi « Informatique et Libertés » qui prévoit que l'informatique doit être au service de chaque citoyen, elle ne doit pas porter atteinte à l'identité humaine !

Antivols pour nouveau-nés : pour ou contre les bracelets électroniques dans les maternités ?

La mise en place, dans plusieurs maternités, de bracelets électroniques fixés à la cheville des nouveau-nés pour prévenir les risques d'enlèvement a donné lieu, le 10 avril 2008, à une communication en séance plénière et à un débat plus large sur la surveillance électronique des personnes vulnérables.

Compte tenu des enjeux, la Commission a décidé de lancer une réflexion de fond sur ce thème afin de définir à quelles conditions il est ou non admissible de mettre en place de tels dispositifs.

La Commission a été saisie de la mise en place au sein de plusieurs maternités d'un dispositif consistant à attacher un bracelet électronique à la cheville des nouveau-nés afin de prévenir toute tentative de kidnapping.

Ces bracelets sont équipés d'émetteurs reliés à un ordinateur central, les récepteurs répartis dans la maternité permettant à tout moment de localiser le bébé dans le service, de détecter les sorties du service et d'alerter en conséquence le personnel par une alarme.

Dans les dossiers présentés à la CNIL, ils permettent une surveillance électronique des déplacements du nouveau-né limitée à trois jours dans un rayon qui ne dépasse pas la maternité.

Lors de l'examen de ces dispositifs, la Commission, tout en constatant que ce type de service peut répondre à une attente des parents et apparaître justifié dans certaines situations à risque, s'est interrogée sur le caractère réellement proportionné, par rapport aux risques encourus, de la généralisation du bracelet à l'ensemble des nouveau-nés.

Si l'on fonde la légitimité du dispositif sur la seule vulnérabilité de l'enfant n'aura-t-il pas vocation à s'étendre ? On équipe aujourd'hui les maternités, il faudra demain équiper les crèches et les écoles, au risque d'habituer l'individu dès son plus jeune âge à une forme de contrôle quasi-permanent dont il ne sera plus à même de percevoir le caractère intrusif.

La CNIL a donc décidé d'engager une réflexion de fond sur le sujet et plus largement sur la surveillance électronique des personnes vulnérables, en auditionnant différents acteurs impliqués dans ces enjeux. A l'issue de ces auditions, elle rendra publiques ses conclusions sur le sujet. Cette réflexion est placée sous la responsabilité d'Anne Debet.

Cette réflexion est d'ailleurs commune à l'ensemble des autorités de protection des données puisque ce thème est inscrit à l'ordre du jour de la 30ème Conférence mondiale des commissaires à la protection des données à Strasbourg du 15 au 17 octobre 2008 « L'homme assisté : ange ou démon numérique ? ».

« Protéger la vie privée dans un monde sans frontières »
30ème conférence mondiale des commissaires à la protection des données et à la vie privée
15 au 17 octobre 2008 - Strasbourg

La 30ème conférence mondiale de protection des données et de la vie privée se tiendra à Strasbourg, lieu hautement symbolique de l'histoire du 20ème siècle, dans l'hémicycle du Conseil de l'Europe, du 15 au 17 octobre prochain. Elle portera sur le thème « Protéger la vie privée dans un monde sans frontières ». Cette conférence est organisée, pour la première fois, conjointement par les Commissions française et allemande qui fêtent, ensemble, leur 30 ème anniversaire en 2008. En outre, le Président de la CNIL a été élu Président du groupe des « CNIL européennes », succédant à la Présidence assurée par l'autorité allemande du BfDI, pendant 4 ans. Elle interviendra également au moment où la France assurera, à partir de juillet prochain, la présidence de l'Union européenne. La conférence fait ainsi partie du programme officiel de la Présidence de l'Union Européenne, et elle est placée sous le haut patronage du Président de la République française.

L'objectif est d'identifier les défis majeurs qui se dressent en matière de respect de la vie privée, dans un contexte international marqué par de fortes évolutions technologiques, politiques, juridiques et économiques. Des représentants du secteur public, des autorités de contrôle, mais aussi des entreprises, des associations de consommateurs et de défense des libertés vont ainsi pouvoir échanger leurs préoccupations et leurs visions de la protection de la vie privée. Ces débats se dérouleront dans un esprit de concertation et avec la volonté de rechercher des solutions communes à l'échelle internationale.

Le site de la conférence www.privacyconference2008.org sera disponible à partir de juin 2008 et permettra l'inscription en ligne avec tous les détails pratiques

Qu'est-ce que c'est ?

La Conférence mondiale des Commissaires à la protection des données et à la vie privée

Cette conférence, qui se tient chaque année à l'automne, réunit les 78 autorités et commissaires à la protection des données et à la vie privée de tous les continents. Ouverte aux acteurs du monde économique, du secteur public et de la société civile, elle constitue le seul temps fort consacré à la protection des données personnelles et à la vie privée.

Pour en finir avec les idées fausses…

Idée fausse n°1

Depuis la modification de la loi intervenue en 2004, l'avis de la CNIL ne serait que consultatif pour la création des fichiers de police, alors qu'avant 2004, de tels fichiers étaient soumis à un avis conforme de la CNIL. C'est Alex Türk, rapporteur du projet de loi en 2004, qui aurait introduit cette disposition.

Cette disposition figurait dans le projet adopté par l'Assemblée nationale en 2002 et présenté par le Gouvernement de M. Lionel Jospin. Ce n'est donc pas Alex Türk qui l'a introduite lorsqu'il était rapporteur du texte en 2004.

A ce propos, M. Gérard Gouzes, député socialiste et alors rapporteur de la commission des lois de l'Assemblée nationale ne disait-il pas : *« si le projet de loi propose de remplacer l'avis conforme par un avis simple pour les fichiers mis en œuvre dans le domaine de la défense, de la sûreté ou de la sécurité publiques, il n'affaiblit pas, pour autant, les pouvoirs de la CNIL, car la publicité donnée à cet avis sera telle qu'il sera difficile pour l'administration de s'en affranchir. »*

Enfin, rappelons que, en 25 ans, la CNIL n'a jamais eu recours à cette possibilité alors même que d'importants fichiers, tels que ceux des renseignements généraux en 1991 ou le STIC en 2001, ont été créés pendant cette période.

Idée fausse n°2

Avec l'exonération de déclaration accordée aux correspondants informatique et libertés, la CNIL ne contrôlerait plus la création de milliers de fichiers.

C'est la loi de 2004 qui a permet aux organismes privés et publics de désigner, en leur sein, des correspondants, chargés de veiller à la bonne application de la loi informatique & libertés. Ces correspondants existent déjà dans d'autres pays européens et en Allemagne depuis 30 ans.

La CNIL a enregistré depuis sa création en 1978 plus de 1 200 000 fichiers. Cela peut paraître surprenant mais il y a sans doute autant, voire plus, de fichiers toujours non déclarés. Faute d'être suffisamment informées, de nombreuses entreprises ou collectivités locales font l'impasse sur leur déclaration.

Ne vaut-il pas mieux alléger les formalités préalables, souvent perçues comme des démarches lourdes et bureaucratiques, et inciter, en contrepartie, à la mise en place de personnes qui vont diffuser une culture informatique et libertés qui conduira à une meilleure défense des droits des individus (salariés, clients, administrés) ?

La CNIL le constate souvent lorsqu'elle a engagé une procédure de sanction à l'encontre d'un organisme : la désignation d'un correspondant lui aurait évité cette mésaventure car il aurait été à même de régler la difficulté en amont des plaintes qui ont fondé l'intervention de la CNIL. Parce que la loi est complexe et méconnue par les entreprises et nombre d'administrations, la désignation d'un correspondant permet d'éviter les nombreux pièges qu'elle recèle malgré elle. C'est pourquoi la CNIL a également et directement engagé un important travail d'information et de formation des correspondants qui se déroule dans ses locaux.

Enfin, l'exonération ne concerne que les déclarations les plus courantes. Les fichiers sensibles (tels que les interconnexions, la biométrie ou encore les « listes noires ») restent soumis à l'autorisation préalable de la CNIL.

Idée fausse n°3

Depuis la loi de 2004, la CNIL aurait moins de pouvoirs.

Cette idée est doublement fausse :
D'abord, **sous l'empire de la loi de 1978, la CNIL était compétente exclusivement** pour réglementer et réguler les fichiers mis en œuvre par le **secteur public**, quel que soient l'organisme concerné et la nature du fichier. **En revanche, tous les fichiers** mis en œuvre par **le secteur privé n'étaient soumis à aucun contrôle** et devaient simplement faire l'objet d'une déclaration à la CNIL.

Cette distinction reposait sur l'idée que les dangers pour les libertés résidaient davantage dans les développements de l'informatique publique que privée. Avec la généralisation de l'utilisation de l'informatique dans la société française, ce postulat de la loi 1978 était devenu contestable car moins protecteur des libertés. En effet, le secteur privé développe de nombreuses applications potentiellement intrusives et dangereuses pour les libertés telles que les « listes noires » de mauvais payeurs qui sont susceptibles de priver des personnes de l'accès à un bien ou à un service (par exemple au logement ou au crédit).

La loi de 2004 tire les conséquences de cette évolution puisqu'elle soumet **désormais** les fichiers potentiellement les plus dangereux pour les droits des personnes à **l'autorisation préalable et expresse de la CNIL**, **que l'organisme soit privé ou public**. Ce pouvoir d'autorisation préalable expresse, dont le non-respect est un délit puni de 5 ans d'emprisonnement et de 300 000 euros d'amende, **n'existait pas dans la loi de 1978**. C'est indéniablement un progrès et un pouvoir supplémentaire donné à la CNIL dans des matières que le Législateur a jugé les plus sensibles (biométrie, « liste noires », interconnexions, fichiers d'infractions pour ne citer que ces quelques exemples).

Ensuite, **l'un des principes de la modification de 2004** réside dans un **rééquilibrage des pouvoirs de la CNIL au profit** du renforcement **du contrôle *a posteriori***. En effet, la CNIL dispose désormais d'un pouvoir de **contrôle sur place et sur pièces**, dans les horaires des perquisitions judiciaires, soit de 6 heures du matin à 21 heures. Elle peut faire une copie de tous les documents qu'elle juge utile à l'exercice de sa mission. Le fait de s'opposer à son contrôle est constitutif d'un délit d'entrave puni d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende. Alors que la CNIL effectuait moins de 12 « visites » par an avant 2004, le nombre des contrôles effectués en 2007 a été de plus de 160.

Par ailleurs, dans la suite logique de ce pouvoir de contrôle, la CNIL dispose également d'un **pouvoir de sanction qui n'existait pas auparavant**. A l'issue d'une procédure contradictoire, en la présence d'avocats défendant l'organisme mis en cause, la CNIL peut prononcer différentes sanctions qui vont de l'avertissement, à la sanction financière d'un montant maximal de 300 000 euros en passant par l'insertion dans la presse de sa décision. Ces nouveaux pouvoirs « quasi-juridictionnels » ont été récemment reconnus par **le Conseil d'Etat qui a considéré que, au vu de ses missions et de sa composition, la CNIL devait être considérée comme une « tribunal** » au sens de la Convention européenne de sauvegarde des droits de l'Homme.
En 2007, 120 procédures de sanctions ont été engagées par la formation contentieuse de la CNIL et le montant cumulé des sanctions financières qu'elle a prononcé atteint près de 300 000 euros.

Idée fausse n°4

La CNIL freinerait la lutte contre la fraude sociale car elle empêcherait les croisements de fichiers

On impute souvent à la CNIL une part de responsabilité dans le manque d'outils pour lutter contre la fraude. C'est bien commode mais inexact.

En effet, aucun principe de protection des données personnelles n'interdit les interconnexions. La Commission est simplement là pour appliquer la loi qui découle elle même de la directive européenne du 25 octobre 1995. Cette loi prévoit que les fichiers doivent recueillir des données *« proportionnées »* aux buts poursuivis et que ces buts doivent être *« légitimes ».*

La CNIL n'a jamais contesté la légitimité de cet objectif de contrôle et de lutte contre la fraude, mais elle a systématiquement recommandé que la mise en place des interconnexions soit transparente grâce à une parfaite information des personnes et *« proportionnée »* dans son ampleur.

La CNIL est également particulièrement vigilante sur les mesures de sécurité des systèmes d'information car une faille dans un système interconnecté peut être lourde de conséquences pour les personnes dont les données se trouveraient ainsi divulguées.

De tels croisements de fichiers existent et ont été autorisés par la CNIL.

Idée fausse n°5

La CNIL est-elle pour ou contre ?

Bien souvent, on demande à la CNIL si elle est « pour ou contre » certains fichiers. Les décisions de la CNIL sont plus complexes et n'entrent pas dans ce classement manichéen. La CNIL analyse les dossiers qui lui sont soumis en fonction de leur conformité à la loi « informatique et libertés » qu'elle est chargée de faire appliquer. Rien de plus mais rien de moins.

Ses décisions ne relèvent donc pas de jugements de valeur a priori mais de l'analyse du fichier en termes d'objectif poursuivi, de proportionnalité des informations collectées, de durée de conservation, de sécurité et de respect du droit des personnes concernées.

Les fichiers qui lui sont soumis pour avis par les Ministères sont analysés en ces termes. Il en est de même pour les fichiers « sensibles », que la CNIL peut autoriser ou refuser, mais uniquement sur le fondement des critères prévus par la loi et non en pure opportunité, parce qu'elle serait « pour ou contre ».

Fort heureusement, la CNIL n'est pas là pour dire aux entreprises, aux administrations, aux collectivités locales, ce qu'elles doivent faire pour se développer commercialement, améliorer leur service aux usagers etc... Elle est là pour les conseiller, leur expliquer les contraintes et les possibilités prévues par la loi lorsqu'elles envisagent de créer un nouvel outil informatique.
Face à un tel projet de fichier, elle doit leur indiquer s'il peut être légalement créé, s'il doit être modifié et dans quelle mesure. Pour les fichiers devant être préalablement autorisés par la CNIL, celle-ci peut évidemment les refuser. Plusieurs dizaines de fichiers le sont chaque année pour des motifs tenant, à titre d'illustration, aux défauts de sécurité des systèmes, à l'absence de proportionnalité entre l'objectif poursuivi et les informations collectées ou entre les données collectées et leur durée de conservation.

En cas de refus, ces fichiers ne peuvent légalement exister. La peine encourue est lourde : 5 ans d'emprisonnement et 300 000 euros d'amende. De plus, la CNIL effectue des contrôles pour vérifier cela.

Idée fausse n°6

Étant donné le peu de moyens dont elle dispose, la CNIL ne servirait plus à rien.

Il est vrai que la CNIL, en comparaison avec ses homologues des autres pays européens pourtant plus jeunes, ne dispose pas de moyens suffisants pour effectuer pleinement sa mission, notamment en matière de sensibilisation du grand public. Plutôt que le « confort » du silence, Alex Türk a choisi de parler franc afin d'alerter les pouvoirs publics sur cette insuffisance budgétaire. Valait-il mieux continuer à se taire ?

Un effort a été accompli lors du vote de la loi de finances pour 2008 afin de permettre le rattrapage du retard pris depuis de nombreuses années. Ainsi, depuis 2004, 40 postes ont été créés. Cet effort, indéniable, doit évidemment se poursuivre mais il serait malhonnête de le passer sous silence.

En matière de moyens, le mieux est l'ennemi du bien. Parce que la CNIL est parfois débordée en raison de l'insuffisance de ses moyens est-elle pour autant inutile ? Il conviendrait de l'expliquer aux :

- 4 500 plaignants qui chaque année s'adressent à la CNIL,
- 2 660 personnes qui lui ont demandé de contrôler les informations qui les concernent détenues dans les fichiers de police (STIC et autres) et dont le maintien ou l'accès à l'emploi en dépend parfois et auxquelles la CNIL a répondu,
- 1 850 000 internautes qui consultent le site chaque année,
- 650 correspondants « informatique et libertés » qui ont reçu une formation organisée par la CNIL afin de les familiariser à leurs nouvelles fonctions,
- 350 entreprises et administrations qui ont vu leur fichier autorisés l'année dernière,
- 120 organismes a l'encontre desquels une procédure de sanction a été engagée l'année dernière, bien souvent à la suite de plaintes,
- 155 organismes (de formation, universitaires, professionnels) qui ont sollicité et bénéficié de l'intervention d'un agent de la CNIL en 2007,
- 27 autres CNIL européennes qui ont élu à leur tête le Président de la CNIL française.

Affirmer que la CNIL souffre d'une insuffisance de moyens est une chose, indéniable sur le fond. En déduire que tout ce qu'elle peut faire ne sert à rien est un curieux paradoxe. Supprimer la solution à des problèmes n'a jamais entraîné la suppression des problèmes eux-mêmes. Supprimer tous les médecins ne supprimera pas toutes les maladies.

Idée fausse n°7

La CNIL favoriserait le développement des technologies et du fichage en général.

En décembre 2007, les locaux de la CNIL ont été envahis par des membres de mouvements « alternatifs » pour proposer la suppression de la CNIL. Ils lui reprochent de ne pas entraver le développement de technologies comme la biométrie, la géolocalisation, les puces RFID et de ne pas s'opposer à la création de fichiers, parfois décidés pas la loi.

Il n'est pas de la responsabilité de la CNIL de s'opposer, par principe, à certaines technologies, alors même que leur utilisation n'est pas interdite par la loi. Aucune technique n'est bonne ou mauvaise en soi, tout dépend de l'usage qui en est fait.

C'est sur ce fondement qu'est bâtie la loi « informatique et libertés ». Cette loi est indifférente aux technologies employées, elle fait porter toute sa vigilance sur leur mise en œuvre concrète, les dangers que cette opération peut représenter pour les libertés et la vie privée.

C'est dans ce cadre que la loi investit la CNIL de la mission veiller à l'équilibre entre la technique et les libertés. Il lui revient le difficile exercice de mesurer la proportionnalité entre l'objectif poursuivi par le fichier et les moyens qui sont mis en œuvre, entre la fin et les moyens.

Cet exercice est nécessairement complexe, technique mais pragmatique, plus qu'une opposition de principe à toute technologie qui est simpliste, théologique et abstraite.

La CNIL regrette souvent d'être seule à évoquer la protection de la vie privée alors qu'un débat public devrait exister sur ces questions qui concerne chacun d'entre nous. Malheureusement, aujourd'hui rares sont les associations qui portent ces questions sur le devant de la scène.

Idée fausse n°8

La CNIL serait pour la création de statistiques ethniques.

Depuis un an, beaucoup d'encre a coulé, beaucoup de passions se sont exprimées sur le thème de la mesure de la diversité. En effet, notre pays s'interroge, depuis plusieurs années, sur l'efficacité de son modèle d'intégration républicain, sur la nécessité de lutter contre les discriminations. Or, pour lutter contre les discriminations, encore faut-il pouvoir les mesurer.

Pour cela, il est nécessaire de procéder à l'observation statistique des différences, de la diversité sociale, « ethnique », religieuse, culturelle… ? Mais alors, quels critères utiliser pour analyser cette diversité ? Quelles méthodes employer ? Qui peut le faire ?

Comment concilier cette nécessité de mieux connaître notre société avec l'interdiction prévue par la loi « informatique et libertés » de recueillir des données faisant apparaître *« directement ou indirectement les origines raciales ou ethniques »* des personnes ? Cette problématique est délicate car elle touche à l'essence même de ce qui fait notre identité, à notre conception de la République, à la façon dont on se perçoit et dont on est perçu par les autres.

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

A l'issue de ces travaux, elle a publié, le 15 mai 2007, 10 recommandations dont l'une d'entre elles tendait à modifier la loi afin de faciliter les recherches en matière de mesure de la diversité des origines, de la discrimination et de l'intégration tout en améliorant la protection des personnes, de leurs données ainsi que le caractère scientifique des enquêtes.
Ces recommandations furent alors unanimement accueillies. Ceci conduisit deux parlementaires, membres de la Commission, à déposer un amendement en ce sens lors de la discussion au Parlement du projet de loi relatif « à la maîtrise de l'immigration, à l'intégration et à l'asile ».

Par sa décision du 15 novembre 2007, le Conseil constitutionnel a censuré cet amendement en estimant qu'il était *« sans lien »* avec la loi. Le Conseil a également considéré que *« si les traitements nécessaires à la conduite des études sur la mesure de la diversité des origines peuvent porter sur des données objectives, ils ne sauraient, sans méconnaître le principe énoncé par l'article 1er de la Constitution, reposer sur l'origine ethnique ou la race ».*

Soucieuse d'appliquer pleinement la décision du Conseil constitutionnel, comme se le doit toute autorité publique, la CNIL n'a pu que constater le désarroi des chercheurs face à la complexité de cette décision, certains organismes publics de renom abandonnant des recherches de crainte de ne pas la respecter. Un travail de pédagogie est donc nécessaire. Il doit être engagé sans tarder afin que la recherche française soit rassurée et puisse poursuivre, sereinement, ses travaux. Un récent ajout aux Cahiers du Constitutionnel (n° 23) s'y emploie.

Toute cette polémique a réussi à faire oublier l'essentiel.

La CNIL a toujours été, et demeure, hostile à la création d'un référentiel « ethno-racial », c'est à dire l'élaboration d'une nomenclature permettant de recenser toutes les personnes en fonction de leur origine réelle ou supposée à l'instar de ce qui existe dans le cadre du recensement au Royaume–uni.

En effet, il ne faut pas confondre l'étude des facteurs de la discrimination, au titre desquels peut figurer l'origine « ethno-raciale » vraie ou supposée des personnes, et leur comptage, puis leur « catégorisation », dans une nomenclature raciale que la CNIL persiste à considérer comme dépourvue de fondement scientifique et inopportune, comme elle l'a systématiquement affirmée depuis décembre 2005.

Diffusion des données personnelles sur internet : où est le problème ?

Nombreux sont les adolescents qui ne voient aucun problème à exposer leur vie privée sur Internet sur les blogs, les réseaux sociaux, les forums de discussion ou les sites communautaires. Les jeunes doivent pourtant prendre conscience que cet espace de liberté n'est pas un espace de non droit et qu'Internet peut aussi porter atteinte à la vie privée. Le sujet méritant débat, la CNIL propose, en partenariat avec Internet Sans Crainte, à l'occasion de la fête de l'Internet du 11 au 18 mai, un petit document avec quelques pistes pour lancer la discussion auprès des 12-17 ans.

À l'occasion de la Fête de l'Internet, 430 Espaces Publics Numériques de 250 communes se mobilisent pour sensibiliser les jeunes et leurs parents aux bons usages de l'Internet avec Internet Sans Crainte. L'opération est relayée au sein des écoles et collèges par le Ministère de l'Education Nationale.

- *Ça vous dirait que dans 10 ans votre futur employeur sache comment s'est passée votre dernière petit fête entre amis ?*
- *Cela ne vous dérange pas d'être une cible publicitaire ?*
- *Je peux publier ce que je veux ! Quand je veux ! Si je veux ! Sûr de çà ?*
- *Peut-on me retrouver même si je ne laisse aucune info personnelle ?*
- *Dans un combat contre un robot « aspirateur de mail », vous auriez le dessus ?*
- *L'intimité est-elle encore d'actualité à l'heure du web collaboratif ?*
- *Si ma liberté s'arrête là où commence celle des autres, où s'arrête ma liberté sur le web ?*

Internet Sans Crainte est le plan français de sensibilisation aux bonnes pratiques de l'Internet pour les enfants. Financé par la Commission Européenne, le projet s'inscrit dans le cadre du réseau européen Insafe (Safer Internet Action Plan –www.saferinternet.org), qui coordonne les actions européennes de sensibilisation à un Internet plus sûr. Internet Sans Crainte est piloté et soutenu par la la Délégation aux Usages de l'Internet, avec l'appui des ministères de l'Education nationale, et de l'Enseignement supérieur et de la Recherche.

Vidéosurveillance : la CNIL demande un contrôle indépendant

À l'heure où le Gouvernement a pour objectif de tripler d'ici deux ans le nombre de caméras de vidéosurveillance présentes dans les lieux publics, la CNIL vient d'adresser à Michèle Alliot-Marie, Ministre de l'Intérieur, une note soulignant la nécessité d'en clarifier le régime juridique.
Ce document préconise, notamment, le renforcement des droits des personnes en attribuant à la CNIL le contrôle de tous les systèmes de vidéosurveillance, quel que soit leur lieu d'implantation (lieu privé ou lieu public).
Simultanément, la CNIL a confié à IPSOS la réalisation d'une étude portant sur l'opinion des Français à l'égard de ces dispositifs.

Alors que le Gouvernement a fait part de son intention d'installer plus de 30 000 caméras de vidéosurveillance, la CNIL constate, d'ores et déjà un accroissement des déclarations, des demandes de conseil mais aussi des plaintes en cette matière. Ainsi, en 2007, la CNIL a reçu près de 1400 déclarations (contre 300 en 2005) et le nombre de plaintes est en augmentation constante au cours de cette même période. Conformément à sa mission, la CNIL a procédé à de nombreux contrôles sur place et prononcé plusieurs mises en demeure à l'encontre d'organismes ayant mis en œuvre des systèmes de vidéosurveillance sans avoir respecté les formalités prévues par la loi.

- **Un cadre légal complexe, source d'insécurité juridique**

Chaque jour, la CNIL reçoit de nombreuses demandes du public et de professionnels, qui attestent de la complexité des règles applicables et de leur incompréhension par nos concitoyens. En effet, les systèmes de vidéosurveillance peuvent relever de deux régimes juridiques distincts :
— **la loi du 21 janvier 1995** qui soumet les systèmes de vidéosurveillance visionnant les lieux ouverts au public à une autorisation préfectorale ;
— **la loi « informatique et libertés » du 6 janvier 1978, modifiée en 2004,** qui réglemente les systèmes de vidéosurveillance installés dans un lieu non ouvert au public, comme une entreprise, ou encore les systèmes implantés dans les lieux publics lorsqu'ils sont couplés à une technique biométrique (de reconnaissance faciale par exemple).

Dans la pratique, ce cadre juridique, difficilement compréhensible, tend à devenir **inapplicable** puisque la majorité des dispositifs de vidéosurveillance utilisent désormais des systèmes numériques qui relèvent de la compétence de la CNIL, et ce quel que soit leur lieu d'installation, comme le prévoit l'article 10.I de la loi du 21 janvier 1995. Or aujourd'hui, ces systèmes sont autorisés par les Préfectures, alors même que nombre d'entreprises ou d'administrations s'interrogent sur le point de savoir si une telle autorisation est nécessaire ou si elle doit se cumuler, ou bien être remplacée, par une formalité auprès de la CNIL ! **Cette question est lourde de conséquences** puisque le fait de mettre en œuvre un fichier, sans que les formalités auprès de la CNIL aient été accomplies, est puni d'une peine de 5 ans d'emprisonnement et de 300 000 euros d'amende en application de l'article 226-16 du code pénal.

- **Vidéosurveillance : le « oui mais » des Français**

Face à cette situation d'incertitude, voire d'insécurité, juridique, la CNIL estime nécessaire de clarifier rapidement le régime actuel de la vidéosurveillance. C'est en ce sens qu'elle a rédigé une note à l'attention du Ministre de l'Intérieur. En effet, au regard des objectifs ambitieux de développement affichés par le Gouvernement, un meilleur encadrement de la vidéosurveillance s'avère indispensable.

La question du contrôle, par un organisme véritablement indépendant, des dispositifs de vidéosurveillance, autrement dit **« le contrôle des surveillants »,** constitue désormais, dans les sociétés démocratiques modernes, **une exigence fondamentale, nécessaire pour asseoir la légitimité du développement de ces systèmes, offrant les meilleures garanties de prise en compte des droits et libertés des personnes.**

La mise en place de systèmes de **vidéosurveillance nécessite, dans la durée, une réelle adhésion de la population.** Si certaines études d'opinion montrent que la population est globalement favorable à la vidéosurveillance, pour autant les Français ne sont pas pour autant prêts à renoncer à la garantie de leurs droits individuels.

Ainsi, pour alimenter sa réflexion, la CNIL a confié à IPSOS la réalisation d'une étude sur l'opinion des Français à l'égard de la vidéosurveillance. L'étude réalisée en face-à-face du 14 au 17 mars 2008 auprès d'un échantillon de 972 personnes, représentatives de la population française âgée de 18 ans et plus, confirme, sans surprise, **qu'une large majorité de Français (71%) se déclarent favorables à la présence de caméras de vidéosurveillance dans les lieux publics**. 65% d'entre eux estiment que la multiplication des caméras permettra de lutter efficacement contre la délinquance et le terrorisme.

L'idée que les dispositifs de vidéosurveillance soient placés sous le contrôle d'un organisme indépendant pour parer à toute dérive séduit une large majorité des Français (79%). **Pour une majorité de Français, la CNIL est l'organisme indépendant le plus indiqué pour assurer ce contrôle.**

La CNIL, forte de son expérience en matière d'analyse de l'équilibre fondamental entre sécurité et libertés, est aujourd'hui l'autorité de contrôle la mieux à même d'encadrer et d'accompagner le développement de la vidéosurveillance.

C'est à la seule condition de disposer d'un régime de la vidéosurveillance encadré par des textes clairs et davantage protecteurs des droits des personnes que l'on pourra parler de « *vidéoprotection* » selon l'expression utilisée par Michèle Alliot-Marie.

Liens

- Etude IPSOS
- Note adressée à Michèle Alliot-Marie, ministre de l'Intérieur, de l'Outre-Mer et des collectivités territoriales.

Les « CNIL » européennes précisent les règles applicables aux moteurs de recherche

Le 4 avril 2008, le groupe des 27 « CNIL » européennes, a adopté à l'unanimité un avis précisant les règles applicables aux moteurs de recherche. Cet avis résulte d'une concertation avec les acteurs majeurs du secteur. Il précise notamment que les données personnelles enregistrées par les moteurs de recherche, doivent être effacées au plus tard au bout de 6 mois.

Après avoir procédé à la consultation des principaux moteurs de recherche, le groupe des « CNIL » européennes dit « G29 » a adopté, le 4 avril 2008, un avis sur la protection des données à caractère personnel applicable aux moteurs de recherche.

Cet avis précise les conditions d'application des règles juridiques communautaires et formule des recommandations, qui doivent améliorer la protection et le droit des utilisateurs des moteurs de recherche.

- **La loi européenne s'applique aux moteurs de recherche**

Le G29 souligne que les règles européennes de protection des données telles que définies par la directive 95/46 , qui protègent les citoyens européens, s'appliquent aux moteurs de recherche, même si leur siège social se trouve en dehors de l'Union européenne.

- **Les données enregistrées par les moteurs de recherche ne doivent pas être conservées plus de 6 mois**

  Le G29 considère que les données personnelles enregistrées par les moteurs de recherche doivent être effacées dès que possible, **et au plus tard au bout de 6 mois**. Il rappelle à cet égard que les moteurs de recherche étant des « services de la société de l'information », ils ne sont pas concernés par la directive 2006/24/CE relative à la conservation des données, contrairement aux fournisseurs d'accès internet ou aux opérateurs de télécommunications. Ceci signifie que les moteurs de recherche ne sont pas légalement obligés de conserver des informations sur les connexions des utilisateurs.

  En pratique, un moteur ne devrait pas conserver indéfiniment l'historique des requêtes effectuées et des sites consultés par un utilisateur. Cet historique peut révéler des informations très intimes, comme par exemple des problèmes conjugaux ou une opinion politique, à partir desquelles il est possible de déduire des habitudes de vie supposées ou un certain comportement. Il en va de la protection de notre vie privée.

- **Les européens doivent être informés de leurs droits**

L'avis du G29 rappelle que les internautes doivent être clairement informés de l'ensemble de leurs droits en application de la directive 95/46. En particulier, l'information doit préciser les finalités des traitements, c'est-à-dire leur objectif, ainsi que les modalités d'exercice des droits d'accès, de rectification et de suppression des données.

Concrètement, quand des données concernant une personne sont publiées sur un site web, celle-ci peut demander à accéder, rectifier ou supprimer ces données auprès de l'éditeur du site. En cas de refus de ce dernier, les personnes peuvent saisir leur autorité de protection des données, telle que la CNIL ou les juridictions judiciaires. Toutefois, comme les moteurs de recherche conservent temporairement une copie de toutes les pages indexées, la version cache d'une page peut encore être consultée via le moteur de recherche même si la page a été effacée par l'éditeur du site. Dans ce cas, un internaute peut aussi demander l'effacement de ces données auprès du moteur de recherche.

- **Le consentement des internautes est nécessaire pour qu'un profilage soit mis en oeuvre**
  Le G29 souligne que le consentement de l'internaute est requis que ce soit pour conserver l'historique des recherches qu'il a effectuées, enrichir son profil (à des fins de notamment de ciblage commercial) par croisement de données, ou encore pour l'utilisation de ses données par des moteurs spécialisés dans la « recherche de personnes ».

A présent, de nouvelles discussions vont s'engager avec les moteurs de recherche afin de déterminer comment mettre en œuvre l'ensemble de ces mesures.