Fichiers privés ou publics, « *vos informations personnelles ont de la valeur, ne vous en fichez pas !* »[1] - Rapport CNIL

Le 9 juillet dernier, la Commission Nationale Informatique et Libertés (CNIL) a présenté son 27ème rapport d'activité pour l'année 2006.

A cette occasion, son Président, Alex Türk, a lancé une alerte sur « *la société de surveillance* » (parfois invisible) qui « *menace notre capital de protection des données et nos libertés* ».

La CNIL a ainsi relevé 3 grandes tendances à risque en matière de protection des données et a présenté sa nouvelle politique de contrôle et de sanction.

- **Les 3 grandes tendances :**

➢ **La convergence des technologies (biométrie, vidéosurveillance et géolocalisation)**

Selon le Président de la CNIL « *la grande menace c'est qu'à échéance, il y ait une conjugaison de l'ensemble de ces dispositifs. C'est pour cela que je crains l'endormissement : les gens ne se rendent pas compte qu'il y a mise en place autour d'eux d'un certain nombre de technologies, qui peuvent être invasives (...). Et cela ne se voit pas* »[2].

- Les demandes d'autorisation de mise en œuvre de dispositifs biométriques ont été multipliées par 10 en un an[3].

Les finalités les plus courantes de ces traitements sont : le contrôle de l'accès aux locaux sur les lieux de travail[4], la gestion des horaires et de la restauration des salariés[5], l'accès au restaurant scolaire[6].

Pour ces trois finalités, la CNIL a publié des autorisations uniques, qui permettent aux responsables des traitements de les mettre en place après une simple déclaration de conformité, dès lors que le dispositif respecte les exigences technologiques imposées (contour de la main ou empreinte digitale exclusivement enregistré sur un support individuel).

---

[1] Conférence de presse 9 juillet 2007 : Présentation du 27ème rapport d'activité de la CNIL 2006.

[2] « chat » du journal Le Monde avec Alex Türk, http://www.lemonde.fr/web/chat/0,46-0@2-3224,55-934028,0.html.

[3] 40 demandes en 2005, 360 en 2006, 200 depuis le début de l'année 2007.

[4] Autorisation unique n°AU-008 - Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail.

[5] Autorisation unique n°AU-007 - Délibération n°2006-101 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail.

[6] Autorisation unique n°AU-009 - Délibération n°2006-103 du 27 avril 2006 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire.

En revanche, les systèmes biométriques reposant sur la reconnaissance de l'empreinte digitale dans une base centralisée font l'objet d'une demande d'autorisation auprès de la CNIL, et doivent être justifiés par un « *fort impératif de sécurité* ».

Concernant les traitements publics, un article paru dans le journal « Le Monde » s'inquiète des évolutions du Fichier national automatisé des empreintes génétiques (Fnaeg). Initialement limité aux seules infractions de nature sexuelle, ce fichier a été considérablement élargi. Il concerne désormais trois quarts des affaires traitées devant les tribunaux français, « *à l'exception notable de la délinquance financière, ou encore de l'alcoolisme au volant* »[7]. De surcroît, une circulaire du ministère de la justice du 31 mai dernier[8] tend à simplifier sa gestion afin d'en réduire les coûts humains et financiers, au détriment de la sécurité et donc de la protection des libertés. Aujourd'hui, le Fnaeg recenserait près de 500 000 profils génétiques[9], contre 6 000 en 2003.

Pour l'avenir, de nouveaux fichiers publics seront débattus, notamment, avec le retour annoncé du projet INES. Il s'agit des futures cartes nationales d'identité électroniques qui devraient intégrer les empreintes digitales.

- 880 déclarations relatives aux systèmes de vidéosurveillance (300 en 2005).

La CNIL constate une évolution de ces dispositifs vers la vidéosurveillance dite « IP », qui utilise les technologies internet (filaire ou Wi-Fi) pour la transmission des images. Certains systèmes enregistrent simultanément son et image, et analysent les mouvements (détection d'un colis abandonné, comptage du nombre de clients entrant et sortant).

Actuellement, le Royaume-Uni est le pays au monde ayant le plus de caméras de surveillance par habitant : une pour 14 Britanniques, dont certaines ont désormais la parole … ! L'ICO, l'équivalent de la CNIL outre-manche, préoccupée par cette évolution, a publié un rapport sur la société de la surveillance[10].

- Les traitements de géolocalisation des véhicules de salariés.

La géolocalisation des salariés par GPS ou téléphonie mobile a diverses finalités : assistance à la navigation, gestion en temps réel des moyens humains et en véhicules d'entreprises, contrôles des prestations, etc …

Dans sa recommandation du 16 mars 2006[11], la CNIL précise que ce dispositif ne doit pas conduire à un contrôle permanent des employés. Il doit être possible de désactiver ce système en dehors des heures de travail pour les véhicules également utilisés à des fins privées. De

---

[7] Propos de Olivier Joulin, du Syndicat de la magistrature *in* La justice simplifie le fichage génétique, Jean Marc Manach, Le monde, 3 juillet 2007.

[8] Disponible sur le site de la Ligue des droits de l'homme de Toulon : http://www.ldh-toulon.net/spip.php?article2090.

[9] D'après Philippe Mallet qui dirige le -service central de l'identité judiciaire, fin mai 2007, le Fnaeg contenait près de 500 000 profil : http://www.ldh-toulon.net/spip.php?article2090.

[10] A Report on the Surveillance Society, septembre 20006, http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

[11] Délibération n°2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public.

plus, il est interdit de collecter les données relatives aux dépassements de limitation de vitesse.

Le Commissaire de la CNIL en charge du secteur a précisé que la Commission réalisera une série de contrôle sur ces dispositifs et que quelques plaintes sont d'ores et déjà en cours de traitement.

Dans le cadre de sa mission de conseil, la CNIL a travaillé avec la ville de Paris pour garantir la liberté d'aller et venir anonymement dans le cadre de l'abonnement VELIB[12] (système de location de vélos de la ville de Paris).

➢ La profusion des réglementations françaises et européennes relatives à la lutte anti-terroriste

Ces réglementations, « *qui de manière invisible peuvent s'interconnecter* »[13], posent le problème de la difficile conciliation entre les impératifs de sécurité publique et le respect des libertés individuelles et collectives.

La loi anti-terroriste du 23 janvier 2006 a par exemple étendu les possibilités d'exploitation, par les services de police, des données de connexion internet et de téléphonie mobile, notamment en élargissant la définition des personnes tenues de conserver ces données.

Le 30 mai 2006, la CNIL a rendu un « *avis très circonstancié* » sur un projet de décret précisant les conditions de réquisitions judiciaires par voie électronique[14], dans la mesure où ces dispositions ne comportaient pas de garanties suffisantes concernant la liste des organismes publics ou privés susceptibles de faire l'objet de telles réquisitions. En effet, ce projet vise des administrations et des organismes de sécurité sociale qui sont exclus du champ des réquisitions électroniques par le Code de procédure pénale, car gérant des données protégées par le secret professionnel.

Au niveau de l'Union européenne, le Parlement européen[15] a amendé le projet de base centrale VIS (système d'information sur les visas) dans le but de renforcer les garanties en matière de protection des données, notamment, en imposant des modalités d'accès aux autorités chargées de la sécurité intérieure des Etats membres. Ce traitement sera la plus grande base biométrique du monde (photos et empreintes digitales des demandeurs de visas de l'espace Shengen), soit 70 millions de personnes au maximum[16].

➢ La tension des relations entre les Etats-Unis et l'Union européenne.

---

[12] "Les vélos en toute liberté" respectent-ils vos libertés ?, http://www.cnil.fr/index.php?id=2237&news[uid]=478&cHash=75a72c1fc6.

[13] « chat » du journal Le Monde avec Alex Türk, http://www.lemonde.fr/web/chat/0,46-0@2-3224,55-934028,0.html.

[14] Projet de décret relatif à l'article 60-2 du code de procédure péanle.

[15] Résolution législative du Parlement européen du 7 juin 2007 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour COM(2004)0835. Après accord politique du Conseil (12 juin 2007) sur le règlement et la décision VIS, attente de la décision finale au Conseil ou signature.

[16] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/802&format=HTML&aged=&language=fr&guiLanguage=en.

Depuis le 11 septembre 2001, les relations transatlantiques sont marquées par les surenchères sécuritaires de l'administration américaine qui portent atteintes au droit communautaire relatif à la protection des données personnelles des européens.

- L'affaire SWIFT (révélée par le New York Times en juin 2006).

SWIFT est une société coopérative interbancaire de droit belge qui gère les transactions financières mondiales de 8007 établissements financiers établis dans 207 pays. En 2008, SWIFT sera au cœur du futur Système européen de paiement (SEPA), et deviendra *de facto* le réseau par lequel transitera l'intégralité des ordres de paiement de l'Union européenne.

Or, depuis les attentats de 2001, la CIA et le Trésor américain (UST) accèdent via les serveurs SWIFT à l'ensemble des transferts financiers européens, sans accord et information préalable des autorités européennes et nationales compétentes.

A défaut d'accord international envisageable, des règles d'usage ont été formalisées par le Trésor américain, qui devrait prochainement les adopter officiellement. Dans ce document unilatéral, l'UST s'est engagé à encadrer l'accès aux données SWIFT et à les traiter uniquement dans le cadre de la lutte contre le terrorisme et son financement.

Toutefois, le groupe de l'article 29 (organe européen regroupant les « CNIL » des Etats membres), estime qu'un certain nombre de ces règles sont trop vagues, et donc inaptes à garantir le principe de proportionnalité du traitement.

Le risque d'espionnage économique est donc toujours présent.

Dans un autre cadre et afin de sécuriser des données stratégiques, les gouvernements français et allemand ont récemment interdit l'utilisation des « Blackberry » (assistant personnel : téléphone et courriers électroniques ».

- Le nouvel accord Passager Name Record (PNR).

Depuis le 11 septembre 2001, les compagnies aériennes européennes ont l'obligation de permettre l'accès des données PNR[17] (centralisées sur le serveur AMADEUS) aux autorités américaines dès lors que leurs avions survolent le territoire US.

En 2004, la Commission européenne avait conclu un accord avec l'administration Bush afin de légaliser ces transferts de données.

En 2006, cet accord a été annulé par la Cour de justice européenne, au motif que la procédure reposait sur une base juridique erronée.

Le nouvel accord conclu en octobre 2006 légalise le transfert des données PNR au FBI et à la CIA, et autorise une durée de conservation de trois ans et demi. Les données PNR transmises sont limitées à 34 catégories, les informations dites « sensibles » (préférences alimentaires, état de santé, convictions religieuses, ...) sont interdites. Cet accord doit être renégocié avant le 31 juillet 2007, date à laquelle un troisième compromis devra être signé.

[17] Nom, adresse, email, siège, mode de paiement, contacts téléphoniques, itinéraire, agence et agent de voyage, statut de voyage du passager, aller-simple, remarques générales, assurance, nombre de bagages, informations diverses sur le voyage, etc…

La CNIL a exprimé de nombreuses craintes à ce sujet. En effet, le nouvel accord qui entrera en vigueur le 1er août 2007 restreindra certainement les faibles garanties existantes :

- Augmentation du nombre d'autorités américaines accédant aux données PNR.
- La finalité (lutte anti-terroriste) pourra varier unilatéralement en fonction de l'évolution de la législation des Etats-Unis.
- En cas de nécessité, les autorités US auront accès aux données dites « sensibles » (origine raciale, ethnique, opinions politiques, état de santé, …).
- La durée de conservation est étendue à 15 ans, sans garantie de destruction au terme du délai.
- Le passage au système « push » (envoi des données par les compagnies aériennes)[18], déjà prévu dans l'accord de 2006, est reporté au 1er janvier 2008 sous réserve de l'acceptation des conditions techniques par les Etats-Unis.

Sous couvert de lutte anti-terroriste légitime, les outils mis en œuvre présentent donc des risques excessifs aux regards des libertés individuelles.

La CNIL a ainsi été saisie par un citoyen français, incarcéré sans motif à son arrivée à l'aéroport de Houston, puis contraint d'embarquer le lendemain pour un vol à destination de Paris. Il ressort des investigations de la Commission, que ce passager était inscrit à tord dans le fichier américian « no fly list », qui recense les personnes interdites de vol à destination des Etats-Unis. A ce jour, aucune garantie de rectification n'a été apportée par l'administration qui gère ce fichier. Selon le ministère américain de la sécurité intérieure, près de 9000 personnes auraient obtenu la rectification de leurs données dans ce fichier.

- **Les contrôles et sanctions en 2006 :**

L'année 2006 fut également marquée par la volonté de la CNIL d'exercer pleinement son pouvoir de contrôle (127 contrôles[19] : + 35% par rapport à 2005) et ses nouveaux instruments de sanctions :

- 94 mises en demeure (dont 31 suite aux contrôles),
- 4 avertissements (dont 1 suite aux contrôles),
- 7 injonctions de cesser ou modifier un fichier,
- 11 sanctions financières pour un montant total de 168 300 € (dont 5 suite aux contrôles).

La CNIL a constaté l'efficacité de la procédure de mise en demeure de faire cesser un manquement à la loi « Informatique et Libertés ». En effet, dans 82% des cas les organismes se conforment à ses demandes, ce qui clôt la procédure de sanction engagée.

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

Typologie des sanctions pécuniaires (amendes de 300 à 45 000 €) :

[18] Actuellement la collecte des données PNR est en système « pull » : extraction des données par les autorités US.
[19] La « CNIL » espagnole a effectué 600 contrôle en 2006.

- 2 banques françaises pour inscription abusive dans le fichier national des incidents de remboursement des crédits aux particuliers (FICP).
- 5 sociétés pour non respect du droit d'opposition (prospection commerciale).
- 1 prestataire internet pour SPAM.
- 1 étude d'huissiers pour commentaires abusifs sur des débiteurs dans la zone « note bloc » du logiciel de gestion client.
- 1 société pour transfert irrégulier de son fichier de gestion des ressources humaines hors union européenne.

La CNIL a également utilisé son pouvoir de publicité en rendant public les sanctions financières à l'encontre du Crédit Lyonnais et du Crédit Agricole Centre France pour manque de coopération et de transparence.
Selon le Commissaire de la CNIL en charge du secteur, cette publicité « *a eu des répercussions positives au sein de l'ensemble de la profession bancaire* ».

En 2007, l'action de la CNIL continue… 6 sociétés ont été condamnées à des sanctions financières pour un total de 120 000 €.

□□□

Devant ces nouveaux défis et avec 570 % d'augmentation de son activité en 3 ans, le Président de la CNIL, Alex Türk, demande une revalorisation et une « *sanctuarisation* » de son budget[20] correspondant à la réalité de ses nouvelles missions (adoptées par le législateur en août 2004).

A titre de comparaison, la CNIL dispose de 95 agents, contre 113 en République Tchèque[21], 115 en Pologne[22], 270 au Royaume-Uni et 400 en Allemagne.

Le Président de la Commission constate aussi que le second décret d'application de la loi « informatique et Libertés » (25 mars 2007) a fortement remis en cause l'action et l'existence même de la CNIL. Les dispositions du décret tendent en effet « *à alourdir à l'excès les procédures, à allonger les délais de réponse des administrations aux citoyens et, parfois, à limiter l'autonomie de fonctionnement de la CNIL* ».

Nicolas Samarcq
Juriste TIC
www.lexagone.com
Membre de l'AFCDP
(Association Française des Correspondants aux Données Personnelles)

[20] En 2006, lors de la discussion de la loi de finance 2007, un amendement (retiré par la suite) proposait de réduire de 50% les crédits de fonctionnement de la CNIL
[21] 10 millions d'habitants.
[22] Chiffre en 2004.