N° 441

SÉNAT

SESSION ORDINAIRE DE 2008-2009

Annexe au procès-verbal de la séance du 27 mai 2009

RAPPORT D´INFORMATION

FAIT

au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par le groupe de travail (2) relatif au **respect** *de la* **vie privée** *à l'heure des* **mémoires numériques**,

Par M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER,

Sénateurs.

(1) Cette commission est composée de : M. Jean-Jacques Hyest, *président ;* M. Nicolas Alfonsi, Mme Nicole Borvo Cohen-Seat, MM. Patrice Gélard, Jean-René Lecerf, Jean-Claude Peyronnet, Jean-Pierre Sueur, Mme Catherine Troendle, M. François Zocchetto, *vice-présidents ;* MM. Laurent Béteille, Christian Cointat, Charles Gautier, Jacques Mahéas, *secrétaires ;* M. Alain Anziani, Mmes Éliane Assassi, Nicole Bonnefoy, Alima Boumediene-Thiery, MM. Elie Brun, François-Noël Buffet, Pierre-Yves Collombat, Jean-Patrick Courtois, Mme Marie-Hélène Des Esgaulx, M. Yves Détraigne, Mme Anne-Marie Escoffier, MM. Pierre Fauchon, Louis-Constant Fleming, Gaston Flosse, Christophe-André Frassa, Bernard Frimat, René Garrec, Jean-Claude Gaudin, Mmes Jacqueline Gourault, Virginie Klès, MM. Antoine Lefèvre, Dominique de Legge, Mme Josiane Mathon-Poinat, MM. Jacques Mézard, Jean-Pierre Michel, François Pillet, Hugues Portelli, Roland Povinelli, Bernard Saugey, Simon Sutour, Richard Tuheiava, Alex Türk, Jean-Pierre Vial, Jean-Paul Virapoullé, Richard Yung.

(2) Ce groupe de travail est composé de : M. Yves Détraigne et Mme Anne-Marie Escoffier.

S O M M A I R E

Pages

Mesdames, Messieurs,

Toutes les époques, depuis la nuit des temps, ont vécu des révolutions sociales, techniques, culturelles, industrielles…. qui ont bouleversé l'ordre des choses. Si ombre et lumière, les « *éternelles voix de la connaissance* » selon Zoroastre, ont toujours accompagné le progrès engendré par l'ingéniosité de l'homme, elles n'ont pas manqué de s'imposer dans l'actuelle révolution numérique qui transforme notre relation aux autres et aux choses.

De résolutions de difficultés en solutions, le législateur a œuvré pour que la notion de vie privée, intégrée depuis la philosophie des Lumières à notre patrimoine historique, culturel et identitaire, reste, dans notre société démocratique, indissociable de l'existence de l'individu et de l'exercice des libertés : la société reconnaît à l'individu le droit de disposer d'un espace privé, distinct de la vie collective de la communauté.

Comment, dès lors, concilier les nouveaux pouvoirs que font peser sur chaque individu les nouvelles technologies avec ce droit à la vie privée ?

Comment éviter que des institutions, publiques ou privées, ou même des individus n'utilisent ces formidables « *mémoires numériques* » au détriment de notre vie privée pour porter atteinte à nos libertés et à notre capacité d'autodétermination ?

L'Homme n'ignore pas que sa mémoire, tout au fond de ses « *entrailles* » (le mot « *mémoire* » a pour origine en hébreu la racine « *mem* » qui signifie « *entrailles* ») l'accompagnera, même altérée, jusqu'à son dernier souffle.

Il nous faut être conscients, nous, homo sapiens devenus « *homo numericus* », du risque qui nous guette d'être pris au piège des mémoires numériques qui jouent le même rôle que notre propre mémoire : toujours présentes, même si elles paraissent enfouies au plus profond d'un système dont nous ne pouvons pas mesurer l'envergure, elles sont là dans une posture qui peut nous porter alternativement de la progression à la régression selon l'usage que nous en faisons.

Il nous revient donc d'être ces **veilleurs vigilants** face aux grands enjeux « informatique et liberté » pour que le respect de la personne humaine, de sa vie privée et de sa dignité reste toujours un principe absolu.

Telles sont les raisons pour lesquelles la commission des lois a décidé, au cours de sa réunion du 22 octobre 2008, de créer un groupe de travail sur la vie privée à l'heure des mémoires numériques.

Composé de vos deux rapporteurs, il a procédé à quelque vingt-cinq auditions et effectué quatre déplacements (Madrid, Bruxelles, Grenoble et Roissy).

Réunie le mercredi 27 mai 2009, la commission a autorisé la publication du présent rapport qui formule quinze recommandations.

LES QUINZE RECOMMANDATIONS DU GROUPE DE TRAVAIL

FAIRE DU CITOYEN UN « HOMO NUMERICUS » LIBRE ET ÉCLAIRÉ, PROTECTEUR DE SES PROPRES DONNÉES

Recommandation n° 1 - Renforcer la place accordée à la sensibilisation aux questions de protection de la vie privée et des données personnelles dans les programmes scolaires

Recommandation n° 2 - Promouvoir l'organisation et le lancement d'une campagne d'information à grande échelle destinée à sensibiliser les citoyens aux enjeux liés à la vie privée et à la protection des données à l'heure du numérique ainsi qu'à les informer des droits que leur reconnaît la loi « informatique et libertés »

Recommandation n° 3 - Promouvoir rapidement la création de labels identifiant et valorisant des logiciels, applications et systèmes offrant des garanties renforcées en matière de protection des données personnelles

RENFORCER LES MOYENS ET LA LÉGITIMITÉ DE LA CNIL

Recommandation n° 4 - Créer une redevance, de faible montant, acquittée par les grands organismes, publics et privés, qui traitent des données à caractère personnel

Recommandation n° 5 - Déconcentrer les moyens d'actions de la CNIL par la création d'antennes interrégionales

Recommandation n° 6 - Renforcer la capacité d'expertise et de contrôle de la CNIL

Recommandation n° 7 - Rendre obligatoires les correspondants informatique et libertés pour les structures publiques et privées de plus de cinquante salariés

Recommandation n° 8 - Rendre publiques les audiences et les décisions de la formation restreinte de la CNIL

COMPLÉTER LE CADRE JURIDIQUE ACTUEL

Recommandation n° 9 - Soutenir la dynamique en cours tendant à la définition de standards internationaux dans le domaine de la protection des données personnelles

Recommandation n° 10 - Affirmer sans ambiguïté que l'adresse IP constitue une donnée à caractère personnel

Recommandation n° 11 - Créer *a minima* une obligation de notification des failles de sécurité auprès de la CNIL

Recommandation n° 12 - Réunir sous une seule autorité, la CNIL, les compétences d'autorisation et de contrôle en matière de vidéosurveillance

Recommandation n° 13 - Réserver au législateur la compétence exclusive pour créer un fichier de police

Recommandation n° 14 - Réfléchir à la création d'un droit à « l'hétéronymat » et d'un droit à l'oubli

Recommandation n° 15 - Inscrire dans notre texte constitutionnel la notion de droit au respect de la vie privée

I. LA VIE PRIVÉE, UNE VALEUR FONDAMENTALE MENACÉE ?

A. LE DROIT AU RESPECT DE LA VIE PRIVÉE, FONDEMENT DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES

1. La vie privée, un fondement des sociétés modernes

La notion de vie privée constitue l'un des fondements de nos sociétés modernes et démocratiques.

La légitimité de la notion de sphère privée découle en effet de la philosophie des Lumières et des principes posés par les théoriciens du libéralisme politique. Au lendemain de la Révolution, Benjamin Constant montre que, contre la « *liberté des Anciens* » qui pensent que l'homme n'est libre que par sa participation active au pouvoir collectif, la « *liberté des Modernes* » se conçoit comme la préservation des droits de l'individu et de sa sphère privée face aux immixtions de la puissance publique :

« ***Il y a au contraire une partie de l'existence humaine, qui, de nécessité, reste individuelle et indépendante, et qui est de droit hors de toute compétence sociale.*** *La souveraineté n'existe que d'une manière limitée et relative. Au point où commencent l'indépendance et l'existence individuelles, s'arrête la juridiction de cette souveraineté* »[1].

De son coté, Alexis de Tocqueville analyse la notion de vie privée au regard de l'« *égalisation croissante des conditions* » et de la diffusion de la démocratie, qu'il définit avant tout comme un « *état social* ». Cette égalité des conditions s'accompagne de la montée de l'**individualisme**, que Tocqueville décrit comme « *un sentiment réfléchi et paisible qui dispose chaque citoyen à s'isoler de la masse de ses semblables et à se retirer à l'écart avec sa famille et des amis* »[2].

La notion de vie privée est ainsi, dans une société démocratique, indissociable de l'existence de l'individu et de l'exercice des libertés : la société reconnaît à l'individu le droit de disposer d'un espace privé, distinct de la vie collective de la communauté.

Ces analyses demeurent aux fondements de notre ordre politique, même si leur appréhension a évolué au cours du temps.

Tout d'abord, le caractère central de la sphère privée a été remis en cause au cours du XX^{ème} siècle par des régimes totalitaires qui ont entendu soumettre l'individu à la réalisation d'une unité fantasmée fondée sur la race, l'histoire ou l'idéologie, et qui fonctionnaient précisément sur la négation de l'existence et de la légitimité de la sphère privée (comme l'a récemment

---

[1] *Principes de politique, chapitre premier, cité par Pierre Manent dans son Histoire intellectuelle du libéralisme, Hachette Littératures, 1987, page 186.*
[2] *De la démocratie en Amérique, tome 2, seconde partie, chapitre II.*

illustré le film *La Vie des Autres*, écrit et réalisé par Florian Henckel von Donnersmarck).

Au cours des auditions auxquelles ils ont procédé, **vos rapporteurs ont ainsi pu mesurer combien la sensibilité à la question de la vie privée,** et plus particulièrement à la protection des données personnelles, **était profondément ancrée dans cet arrière-plan historique** et dans les souvenirs encore traumatisants de la vie sous ces régimes. Il leur a semblé pouvoir expliquer ainsi la vigilance extrême accordée à la question de la protection des données en Espagne ou en Allemagne par exemple, ainsi qu'en France où la mémoire de l'Occupation reste vive, alors qu'à l'inverse, et de façon extrêmement schématique, les pays anglo-saxons accorderaient une attention moins « épidermique » à cette problématique[1].

En outre, les craintes que suscite aujourd'hui le développement des nouvelles technologies peuvent être comprises à partir des analyses de Michel Foucault sur le pouvoir, dont Foucault montre qu'il n'est pas circonscrit au pouvoir politique, mais qu'il s'exerce au contraire de façon diffuse à travers des micro-pouvoirs répartis à tous les niveaux de la société et qui trouvent leur source dans le savoir.

Au cours des dernières décennies, l'attention s'est ainsi portée sur les menaces que pourrait représenter pour l'individu la mise à disposition d'autres acteurs privés (employeurs, assureurs, etc.) d'informations concernant sa vie privée. Comme l'écrit le professeur Yves Poullet, faisant référence au *1984* de G. Orwell, dans un récent article consacré à la protection des données à l'heure de l'Internet, « *l'information représente pour ceux qui la détiennent un pouvoir vis-à-vis de ceux sur lesquels l'information est détenue. Celui qui détient l'information sur autrui peut adapter sa décision en fonction de la connaissance que l'information collectée et traitée lui donne d'autrui. Il prévoit son attitude et peut donc répondre à sa demande ou influencer celle-ci* »[2]. **L'attention apportée à la protection de la vie privée et, plus précisément, à la protection des données personnelles, s'expliquerait ainsi par la crainte de voir des institutions, publiques ou privées, ou même des individus, utiliser des informations relatives à notre vie privée pour porter atteinte à nos libertés et à notre capacité d'auto-détermination :** « *la crainte de voir l'homme s'emparer totalement de l'homme est devenue le cœur de toutes les angoisses* »[3].

---

[1] *Ce qui ne signifie pas que ces pays, patries du libéralisme politique, ne fassent pas preuve d'une vigilance extrême à l'égard de toute mesure susceptible d'accroître les capacités d'intervention des pouvoirs publics dans la sphère privée des individus. Pour une présentation détaillée de la conception américaine de la protection des données, voir infra.*

[2] *Yves Poullet, Jean-François Henrotte, La protection des données (à caractère personnel) à l'heure de l'Internet, in Protection du consommateur, pratiques commerciales et T.I.C., collection Commission Université-Palais, volume 109, pp. 197-245.*

[3] *M. Contamine-Raynaud, Le secret de la vie privée, ouvrage collectif, L'information en droit privé, LGDJ 1978, page 454, n° 36.*

2. Une protection juridique reconnue au niveau national et international

a) Le respect de la vie privée, une composante des droits de l'homme

Au lendemain de la Libération et de la prise de conscience des menaces qu'ont fait peser sur les droits des individus les atteintes à leur intimité, la protection de la vie privée a fait l'objet d'une reconnaissance internationale :

- Ainsi, **l'article 12 de la Déclaration universelle des droits de l'homme du 10 décembre 1948** dispose que « *nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ».

Une rédaction similaire a été reprise lors de l'élaboration de l'article 17.1 du Pacte international relatif aux droits civils et politiques du 16 novembre 1966, qui est entré en vigueur le 23 mars 1976.

- **L'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales,** adoptée le 4 novembre 1950, stipule quant à lui que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

La notion de respect de la vie privée apparaît alors comme **la source d'une double obligation pour les Etats** : non seulement **celle de ne pas s'immiscer de façon arbitraire dans la sphère privée des individus,** mais également **celle de mettre en œuvre l'ensemble des mesures propres à prévenir les atteintes à la vie privée** des individus par des acteurs privés. La Cour européenne des droits de l'homme a ainsi considéré, dans une affaire *Marckx c. Belgique* datée du 13 juin 1979, qu'à l'inverse des particuliers auxquels incombe la seule interdiction de s'immiscer dans la vie privée d'autrui, la reconnaissance du droit au respect de la vie privée imposait aux Etats d'édicter un ensemble de dispositions législatives permettant d'en assurer la protection.

De la protection de la vie privée a découlé la reconnaissance au niveau international d'un droit à la protection des données personnelles : ainsi **la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (dite « convention 108 »)**, adoptée dans le cadre du Conseil de l'Europe et

entrée en vigueur le 1er octobre 1985, garantit-elle spécifiquement « *à toute personne physique […] le respect […] de son droit à la vie privée à l'égard du traitement automatisé des données à caractère personnel la concernant* ».

b) En France : une protection ancienne, une reconnaissance récente

En France, paradoxalement, alors que le principe de respect de la vie privée irrigue notre droit depuis le XIX^{ème} siècle[1], il a fallu attendre 1970 pour que cette notion soit inscrite expressément dans notre législation. Auparavant, **on considérait que la protection de la vie privée découlait implicitement du principe constitutionnel plus large de liberté individuelle :** c'est d'ailleurs ce qu'a expressément reconnu le Conseil constitutionnel dans sa décision 99-416 DC du 23 juillet 1999, en affirmant dans son considérant 45 sur la carte vitale que « *la liberté proclamée par (l'article 2 de la Déclaration des droits de l'homme et du citoyen*[2]*) implique le respect de la vie privée*[3] ».

La loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens a néanmoins inséré dans le Code civil un article 9 qui dispose que « *chacun a droit au respect de sa vie privée* », la notion de respect recouvrant tout à la fois celle d'intimité (la légitimité de l'existence d'une sphère réservée, qui échappe à toute immixtion extérieure) et celle d'autonomie (« *le droit pour une personne d'être libre de mener sa propre existence comme elle l'entend avec un minimum d'ingérences de l'extérieur* » : Conclusions Cabanes prises dans CA Paris, 7ème chambre, 15 mai 1970) : le droit au respect de la vie privée s'apparente ainsi à un droit **à la tranquillité**[4].

Notion fondamentale de notre droit, elle n'en demeure pas moins **une notion aux contours imprécis.** Comme le relevait notre excellent collègue Robert Badinter en 1968, « *s'agissant de la vie privée, […] plutôt que de définir le contenu, les juristes français se sont plus volontiers attachés à dépeindre le contenant. Depuis Royer-Collard, le célèbre mur de la vie privée se découpe bien nettement sur l'horizon juridique, mais quant au domaine qu'il enclot, ses dimensions s'avèrent singulièrement variables* »[5].

Ainsi, à titre d'illustration, le juge a considéré qu'un bailleur qui communique à l'employeur d'un individu le montant des loyers impayés

---

[1] Par exemple, en juin 1858, le Tribunal civil de la Seine affirmait : « nul ne peut sans le consentement formel de la famille reproduire et livrer à la publicité les traits d'une personne sur son lit de mort, quelle qu'ait été la célébrité de cette personne ».

[2] « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression. »

[3] Dans sa décision n° 94-352 DC du 18 janvier 1995, le Conseil constitutionnel avait déjà considéré que « la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle ». Dans sa décision plus récente n° 2008-562 DC du 21 février 2008, il a affirmé que « la liberté d'aller et venir et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789 », faisaient partie des libertés constitutionnellement garanties.

[4] Voir notamment J. Carbonnier, Droit civil, vol. 1, PUF, 2004, p. 518.

[5] R. Badinter, Le droit au respect de la vie privée, JCP G 1968, I, 2136.

portait atteinte à la vie privée de ce dernier[1] ; constitue également une violation de la vie privée la description des poubelles d'une personne permettant de connaître des détails relevant de sa vie intime (prise de médicaments, choix de ses menus, informations sur ses sous-vêtements, etc.)[2] ; dans un arrêt daté du 2 octobre 2001, la Chambre sociale de la Cour de cassation a par ailleurs considéré que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; celle-ci implique en particulier le secret des correspondances* » ; le juge estime également que « *l'autorisation administrative permettant aux réalisateurs d'un reportage télévisé de pénétrer dans un établissement pénitentiaire ne les dispense pas d'obtenir du détenu qu'ils filment le consentement qu'il a seul le pouvoir de donner* »[3] ; etc.

S'agissant de la notion de vie privée, la jurisprudence est donc appelée à jouer un rôle essentiel, notamment lorsqu'il s'agit de **concilier cette notion avec d'autres principes fondamentaux tels que le droit à la liberté de l'information.** Dans ce cas, le juge considère qu'en cas d'invocation concomitante du droit au respect de la vie privée et du droit à la liberté d'expression, ces deux notions revêtant, eu égard aux articles 8 et 10 de la Convention européenne des droits de l'homme et de l'article 9 du Code civil, une identique valeur normative, il lui appartient de rechercher un équilibre, et, le cas échéant, de privilégier la solution la plus protectrice de l'intérêt le plus légitime[4].

De son coté, le Conseil constitutionnel s'est régulièrement fondé sur ce droit au respect de la vie privée pour examiner la constitutionnalité de dispositions législatives tendant à la création de fichiers : à titre d'exemple, l'encadrement législatif des fichiers de police judiciaire STIC et JUDEX[5] ou encore la création du dossier médical personnel[6], ont été examinées sous l'angle du respect de la vie privée et de la proportionnalité de la mesure au regard des objectifs poursuivis par la loi.

c) Le droit à la protection des données dans l'Union européenne : d'une déclinaison du droit au respect de la vie privée à la reconnaissance d'un droit autonome

Par un arrêt *E. Stauder c. Ville d'Ulm* daté du 12 novembre 1969, la Cour de justice des communautés européennes **a reconnu le droit au respect de la vie privée comme un principe général du droit communautaire** (car fondé sur la tradition constitutionnelle commune aux Etats de la Communauté économique européenne) dont elle assure le respect.

---

[1] *Cour de cassation, première chambre civile, 12 octobre 1976.*
[2] *CA Paris, 30 mars 1995.*
[3] *TGI Paris, 13 avril 1988.*
[4] *Cour de cassation, première chambre civile, 9 juillet 2003.*
[5] *Décision n° 2003-467 du 13 mars 2003 relative à la loi pour la sécurité intérieure.*
[6] *Décision n° 2004-504 du 12 août 2004 sur la loi relative à l'assurance maladie.*

La plupart des Etats-membres de l'Union européenne ont en effet inscrit le droit au respect de la vie privée dans leur Constitution. C'est notamment le cas de l'Espagne, dont la Constitution du 29 décembre 1978 dispose dans son article 18 que « *le droit à l'honneur, à l'intimité personnelle et familiale et à sa propre image est garanti. […] La loi limitera l'usage de l'informatique pour garantir l'honneur et l'intimité personnelle et familiale des citoyens et le plein exercice de leurs droits* ». **Le droit à la protection des données est ainsi apparu, dans un premier temps, comme une déclinaison du droit au respect de la vie privée.** C'est ce qui ressort également de la lecture du considérant n° 10 de la directive 95/46/CE du 24 octobre 1995, qui rappelle que « *l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire* ».

Dans un second temps, on a assisté à **une autonomisation du droit à la protection des données personnelles.** Ainsi, **la Charte européenne des droits fondamentaux du 7 décembre 2000,** susceptible d'acquérir force juridique contraignante dès l'entrée en vigueur du Traité de Lisbonne, reconnaît, à côté du droit au respect de la vie privée et familiale, garanti par son article 7[1], **un droit à la protection des données à caractère personnel, qui fait l'objet de son article 8 :**

« *1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.* ».

Parallèlement, treize Etats-membres ont expressément reconnu le droit à la protection des données personnelles comme principe à valeur constitutionnelle. Tel est notamment le cas de la Grèce, dont la Constitution dispose dans son article 9 A que « *chaque individu a le droit d'être protégé contre la collecte, le traitement et l'utilisation, en particulier par voie électronique, de ses données personnelles, selon des conditions prévues par la loi. La protection des données personnelles est assurée par une autorité indépendante, qui est constituée et fonctionne selon des conditions prévues par la loi* »[2]. En Espagne, l'arrêt 292-2000 de la Cour constitutionnelle, s'inspirant des travaux préparatoires de la Charte européenne des droits

---

[1] *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».*

[2] *Voir à ce sujet l'intervention de M. Alex Türk, président de la CNIL, le 25 mai 2008, devant les membres du comité présidé par Mme Simone Veil.*

fondamentaux, a également reconnu explicitement le droit fondamental à la protection des données à caractère personnel comme un droit autonome.

B. UNE VALEUR FONDAMENTALE QUI FAIT AUJOURD'HUI L'OBJET D'UNE TRIPLE REMISE EN CAUSE

Bien que reconnue et protégée au plus haut niveau de leur ordre juridique par l'ensemble des Etats européens, la notion de vie privée fait aujourd'hui l'objet d'une triple remise en cause, sous l'effet conjugué des enjeux de sécurité de l'après-11 septembre, du confort apporté par des nouvelles technologies par ailleurs intrusives, ainsi que d'une tendance sociologique profonde au narcissisme et à « l'exposition de soi ».

1. Une demande accrue de sécurité

La révolution numérique, le développement de nouvelles applications et l'émergence d'Internet ont démultiplié les sources de données à caractère personnel tant en nombre que dans leur nature. Les capacités de stockage des données sont désormais illimitées et chaque individu est devenu un producteur de données. De plus en plus de gestes de la vie quotidienne laissent désormais une trace numérique. Parfois, cette trace ne subsistera que quelques instants. Mais souvent, elle persistera.

Les évolutions en cours renforcent incontestablement la capacité des acteurs privés à constituer des bases de données très précises sur les habitudes de consommation ou de déplacement des individus, ainsi que sur leurs pensées. Néanmoins, il convient de ne pas perdre de vue que **le seul acteur capable de rassembler toutes ces données demeure l'Etat, lequel poursuit des finalités beaucoup plus complexes.**

La tentation pour l'Etat est d'autant plus grande que **depuis une décennie, la demande de sécurité dans la société a relevé le seuil de tolérance vis-à-vis des systèmes de surveillance et de contrôle.**

a) Un nouvel équilibre entre sécurité et liberté

Depuis l'adoption de la loi du 6 janvier 1978 consécutivement au scandale du projet SAFARI, **un climat de consentement social** en faveur de plus de sécurité s'est installé.

Cette tendance n'est pas propre aux problèmes de délinquance. De manière générale, la tolérance face aux risques de tous ordres a reculé.

Cette primauté de la sécurité s'est traduite notamment par des arbitrages en défaveur du droit à la vie privée. Les nouvelles technologies sont perçues comme de nouvelles possibilités de lutte contre l'insécurité et de nombreuses personnes ne voient pas d'inconvénient majeur à être tracées ou surveillées dès lors qu' « *elles n'ont rien à se reprocher, ni à cacher* ».

Le déplacement du point d'équilibre entre sécurité et liberté explique des glissements sémantiques. Certains parlent désormais de « vidéoprotection » et non de vidéosurveillance.

Les attentats du 11 septembre 2001 ont accéléré cette évolution de fond, mais ils n'en sont pas la cause. En revanche, ils ont légitimé **des dispositifs de sécurité préventifs**. La nature même du terrorisme oblige à élaborer des stratégies de prévention de ces actes. Cette évolution de la menace implique une détection précoce afin d'évaluer la dangerosité d'un individu et de le placer sous une surveillance étroite avant le passage à l'acte.

Outre le besoin de sécurité, d'autres arguments sont souvent avancés pour justifier le renforcement des moyens de surveillance et de contrôle, en particulier :

- le respect des obligations internationales, par exemple en matière de passeport biométrique ;

- l'efficacité et la rationalisation des procédures.

Pour les représentants de l'association IRIS, ce second argument est aussi puissant que le besoin de sécurité. Mme Meryem Marzouki, présidente, a souligné la puissance de « la logique managériale » préoccupée de fluidifier des flux et de simplifier des procédures.

L'exemple des aéroports internationaux est très éclairant. Vos rapporteurs ont pu constater, lors de leur déplacement à l'aéroport de Roissy-Charles de Gaulle, que ces lieux concentraient désormais de multiples technologies de surveillance dans un double souci de sécurité et de simplification des contrôles. Le recours bientôt massif à la biométrie (passeports et visas biométriques tendent à se généraliser) permet de concilier ces deux objectifs, sans que l'on sache toujours lequel prévaut.

Cette logique de rationalisation peut expliquer la tendance à étendre à la lutte contre la criminalité des dispositifs initialement conçus pour la lutte contre le terrorisme. Ces dispositifs sont très onéreux et il est rationnel de souhaiter rentabiliser l'investissement.

Ainsi, la collecte systématique des données PNR (pour « *Passenger Name Record* ») par les Etats-Unis à partir de 2004 fut justifiée par la lutte contre le terrorisme. Mais l'accord conclu entre les Etats-Unis et l'Union européenne le 19 octobre 2006 pour encadrer le transfert des données détenues par les compagnies aériennes européennes vers les Etats-Unis autorise leur utilisation pour d'autres finalités, en particulier la lutte contre la criminalité organisée. L'Union européenne semble prendre la même voie puisque la Commission européenne a présenté le 21 novembre 2007 une proposition de décision-cadre relative à l'utilisation des données PNR. Cette proposition

permettrait l'utilisation de ces données pour de très nombreuses finalités, même si l'objectif mis en avant demeure la lutte contre le terrorisme[1].

Le consentement en faveur de plus de surveillance peut aussi s'expliquer par le caractère souvent indolore et invisible des procédés utilisés. Installer une caméra dans chaque lieu public ne produit pas la même impression que d'affecter un policier à chaque coin de rue.

Enfin, **ce climat de consentement social produit un « effet cliquet » très important.** Si parfois les mesures annoncées sont présentées comme des mesures d'exception prises à titre provisoire et soumises à évaluation régulière, en pratique les retours en arrière sont inexistants. La menace terroriste crée une pression qui interdit de prendre le risque de baisser la garde.

b) Des données potentiellement à la disposition de l'Etat

La croissance exponentielle des informations sur le *web* ainsi que des données à caractère personnel conservées sur tout support accroît dans les mêmes proportions les sources d'information que l'État peut utiliser pour assurer deux missions : la justice et le renseignement.

S'agissant de l'autorité judiciaire, celle-ci a toujours la faculté de requérir l'ensemble des données dont elle estime avoir besoin pour l'enquête ou l'instruction. Sur le principe, rien ne change. En pratique, cette explosion des données et des traces numériques laissées par chacun de nous dans l'espace physique ou virtuel met à la disposition de la justice une mine d'informations qui n'existait pas auparavant.

Le téléphone portable, la vidéosurveillance, les cartes bancaires ou le télépéage sur autoroute, dans les transports en commun ou pour accéder à des lieux collectifs tels que cantine ou bibliothèque vont situer un individu dans l'espace. Les appels et courriels émis ou reçus, votre profil Facebook ou les données PNR renseigneront sur vos relations. Les requêtes auprès d'un moteur de recherche formulées sur votre ordinateur éclaireront sur vos centres d'intérêt au cours des derniers mois.

Vos rapporteurs ne contestent pas que le juge puisse accéder à ces données dans le cadre d'une procédure judiciaire. Sa légitimité est certaine. Mais, il est troublant de concevoir, au rythme où nos traces numériques se développent, la possibilité théorique de reconstituer chaque instant d'une existence.

A côté de la justice, les activités de renseignement sont les seconds bénéficiaires de ces données. De nombreux Etats se sont dotés de moyens de surveillance des réseaux et des télécommunications.

---

[1] *La commission des lois du Sénat a adopté une proposition de résolution n° 402 (2008-2009) relative à cette proposition de décision-cadre. Pour plus de détails, voir le rapport n° 401 (2008-2009) de votre co-rapporteur Yves Détraigne au nom de la commission des lois (http://www.senat.fr/rap/l08-401/l08-4011.pdf). Cette proposition de résolution deviendra résolution du Sénat.*

Les Etats-Unis, en association avec d'autres Etats, ont mis en œuvre le programme Echelon d'écoute des télécommunications sur l'ensemble de la planète. La France possède également des capacités d'écoute, mais d'une moindre ampleur.

Ces méthodes, qui dérogent naturellement au principe du secret des correspondances et portent atteinte à la vie privée, n'ont pas suscité de réactions d'ampleur. Peut-être est-ce parce que chacun de ces Etats prend soin de ne pas surveiller ses propres citoyens.

A côté de l'exploitation de ces sources fermées, les services de renseignement ainsi que les services de police exploitent de plus en plus les sources ouvertes, en particulier sur Internet.

Les réseaux sociaux permettent parfois d'en apprendre plus sur un individu, les personnes avec lesquelles il est en contact, son environnement que les fichiers de police.

Un autre exemple est le lancement en avril 2007 d'un appel d'offres par le ministère de la Défense pour se doter d'un outil capable de surveiller à des fins militaires tous les réseaux ouverts. Ce projet s'intitule Herisson pour « Habile extraction du renseignement d'intérêt stratégique à partir de sources ouvertes numérisées ».

c) La collecte de données spécifiques à titre préventif

Certaines données ne sont pas conservées très longtemps par les acteurs qui les possèdent. En effet, le principe de proportionnalité impose des durées de conservation adéquates en fonction notamment de la finalité. De nombreuses données sont conservées uniquement à des fins commerciales ou techniques et peuvent rapidement ne plus être utiles à l'opérateur qui les a générées ou conservées.

Toutefois, ces données peuvent présenter un intérêt particulier pour la police ou la justice. Le risque est qu'elles aient été effacées.

Telle est la raison pour laquelle sont apparues depuis quelques années des obligations légales particulières de conservation de données collectées par des acteurs privés à des fins commerciales ou de services, afin que ces données puissent aussi servir à des fins de prévention et de répression d'infractions.

Ces dispositifs font songer à des « filets dérivants » capturant de nombreuses données relatives à des citoyens ordinaires afin, d'une part, de détecter des activités terroristes ou criminelles et, d'autre part, de pouvoir réveiller ces données en cas de besoin.

Cette démarche est distincte de celle des fichiers de police traditionnels qui ont pour objet d'accumuler des données sur des personnes déjà connues des services.

Le principal reproche fait à ces collectes indifférenciées de données est de considérer chaque utilisateur comme un suspect *a priori*. Ses données personnelles sont conservées au cas où elles se révèleraient intéressantes ultérieurement.

Deux grands ensembles de données jugées stratégiques sont ainsi soumis à une obligation de conservation ou de transmission spéciale :

- les données techniques de connexion conservées par les opérateurs de communications électroniques[1] (opérateurs de téléphonie fixe et mobile et fournisseurs d'accès à Internet) et les hébergeurs de site Internet (voir *infra*) ;

- les données PNR détenues par les compagnies aériennes et les agences de voyage[2].

On observera à ce propos que si des divergences importantes subsistent entre Européens et Américains sur les modalités de l'utilisation des données PNR (nombre de données collectées, durée de conservation, finalités poursuivies…), il y a désormais une convergence sur l'opportunité d'utiliser ces données aux fins de lutter contre le terrorisme et la criminalité organisée.

Dans un ordre d'idée similaire, le motif parfois avancé en faveur de l'installation d'un système de vidéosurveillance est de conserver des images permettant, en cas d'infractions, de pouvoir connaître *a posteriori* les circonstances dans lesquelles elles ont été commises.

Enfin, rappelons que la loi du 23 janvier 2006 relative à la lutte contre le terrorisme a pérennisé et étendu la possibilité de mettre en place des dispositifs de contrôle des données signalétiques des véhicules et de leurs passagers. En tous points du territoire national, notamment les zones frontalières, portuaires et aéroportuaires et les grands axes de transit, peuvent être installés des dispositifs fixes ou mobiles de contrôle automatisé des plaques minéralogiques. Ce traitement de données est interconnecté avec le fichier des véhicules volés et le système d'information Schengen. Les finalités sont la lutte contre le terrorisme, les infractions criminelles et le vol de véhicules.

La CNIL avait émis de fortes réserves à l'époque, estimant que ce dispositif conduirait « *à pouvoir soumettre à une surveillance automatique l'ensemble des déplacements des personnes en France utilisant le réseau routier, ce qui serait de nature à porter atteinte au principe fondamental de la liberté d'aller et venir* ». Elle ajoutait que la collecte systématique de la photographie des passagers pourrait conduire à l'instauration d'un contrôle d'identité à l'insu des personnes.

---

[1] Loi du 15 novembre 2001 relative à la sécurité quotidienne, complétée par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. Voir le rapport n° 117 (2005-2006) de notre collègue Jean-Patrick Courtois au nom de la commission des lois.

[2] Voir le rapport n° 401 (2008-2009) précité de votre co-rapporteur Yves Détraigne au nom de la commission des lois.

d) Des fichiers de police de plus en plus nombreux

Au même titre que les entreprises, l'Etat a fait des données à caractère personnel la matière première à partir de laquelle il personnalise ses services et améliore sa performance.

Cette logique n'est pas propre aux questions de sécurité. L'ensemble des services de l'Etat est concerné.

Ainsi, le pré-remplissage des déclarations de revenu est un service très apprécié des contribuables. Mais il suppose un croisement et une exploitation beaucoup plus intenses des données transmises par les organismes sociaux et les établissements bancaires.

Cette logique s'exprime pleinement à propos des fichiers de police. Plus nombreux –58 recensés par le rapport d'information de la commission des lois de l'Assemblée nationale sur les fichiers de police[1]–, ils intègrent aussi de nouvelles données comme les données biométriques et recensent un nombre croissant d'individus.

Le STIC (système de traitements des infractions constatées)[2] recensait en décembre 2008 36,5 millions de procédures, 37,9 millions d'infractions, 5,5 millions d'individus et 28,3 millions de victimes. En 2001, moins de quatre millions de personnes y figuraient.

Il en va de même pour les fichiers d'identification judiciaire comme le FAED (Fichier automatisé des empreintes digitales) et le FNAEG (Fichier national des empreintes génétiques). Le premier compte 3 millions de personnes enregistrées[3] en 2009 contre un million en 1998. Le second, créé seulement en 1998 mais dont le champ a été considérablement élargi par la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, comportait un peu plus de 800.000 individus fin 2008 contre moins de 3.000 en 2002.

Cette montée en puissance a fait des fichiers de police un outil de travail quotidien et indispensable pour l'ensemble des forces de sécurité.

Une autre tendance est **l'interconnexion**, notamment entre les données de masse collectées à titre préventif (données PNR, plaques minéralogiques des véhicules) et des fichiers à vocation judiciaire comme le fichier des personnes recherchées (FPR) ou le fichier des véhicules volés (FVV).

---

[1] *Rapport d'information n° 1548-XIIIe législature de Mme Delphine Batho et M. Jacques Alain Benisti, députés.*

[2] *Ce fichier répertorie des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause dans ces procédures et les victimes des infractions concernées. Il facilite la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Il permet également d'élaborer des statistiques. Ce fichier est géré par la police nationale. La gendarmerie nationale possède son pendant appelé JUDEX.*

[3] *Ainsi que 171.000 traces non identifiées.*

Vos rapporteurs attirent aussi l'attention, à la suite de la CNIL et du rapport d'information précité sur les fichiers de police, **sur les risques de dérive en cas d'usage des fichiers de police à d'autres fins,** comme la réalisation d'enquêtes administratives.

La loi du 15 novembre 2001 relative à la sécurité quotidienne a explicitement prévu la possibilité d'une consultation des fichiers STIC et JUDEX dans le cadre de certaines enquêtes administratives. Les informations contenues dans ces fichiers peuvent donc avoir un impact direct sur la vie quotidienne des personnes fichées. Un emploi pourra ainsi leur être refusé. Selon la CNIL, la consultation du STIC à des fins d'enquête administrative est susceptible de concerner aujourd'hui plus d'un million d'emplois, en particulier dans le secteur de la sécurité privée.

L'exactitude et la mise à jour des données enregistrées doivent être irréprochables. Or, les contrôles de la CNIL montrent de graves insuffisances. Ainsi, le taux des données non effacées à la suite d'un classements sans suite pour insuffisance de charges ou infraction insuffisamment caractérisée était, pour les 34 tribunaux de grande instance interrogés, de 6,96 % en 2005, 5,89 % en 2006 et 21,5 % en 2007, soit plus d'un million d'affaires non mises à jour en 3 ans.

Enfin, la coopération policière européenne et internationale tend de plus en plus à permettre l'interrogation réciproque des fichiers de police nationaux, notamment dans le cadre du traité de Prüm[1].

e) Un sous-encadrement de l'Etat ?

Lors de son audition, maître Alain Bensoussan, avocat, **a opposé à une phase de sur-régulation de l'Etat entre 1978 et 2004, une phase actuelle de sous-encadrement.** La CNIL serait accaparée par le contrôle du secteur privé et l'Etat s'autorégulerait.

Ce retournement, alors que la loi « informatique et libertés » fut votée en réaction au projet SAFARI d'interconnexion des fichiers de l'Etat et de la sécurité sociale, serait en particulier la conséquence de la loi du 6 août 2004 qui a modifié les règles relatives à la création de traitements de données par l'Etat.

Cette analyse est partagée par l'association IRIS et la Ligue des droits de l'homme pour lesquelles la suppression de l'avis conforme de la CNIL pour la création de fichiers de police est une régression fondamentale.

Qu'en est-il exactement ?

Il est vrai que les traitements de données intéressant la sécurité, la sûreté de l'Etat et la répression des infractions pénales sont hors du champ de la directive européenne du 24 octobre 1995 « Protection des données

---

[1] *Le traité de Prüm, signé en mai 2005 et intégré depuis 2008 au droit de l'Union européenne, permet aux États membres d'échanger des données telles que les empreintes génétiques et digitales, ou encore les immatriculations des véhicules.*

personnelles ». Elle ne s'applique qu'aux traitements de données relevant du premier pilier de l'Union européenne.

Le seul texte de l'Union européenne en la matière est la décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Il ne porte toutefois que sur les données à caractère personnel qui « *sont ou ont été transmises ou mises à disposition entre les Etats membres ou entre des systèmes d'informations européens et des Etats membres* ». Sont en outre exclus de son champ les « *intérêts essentiels en matière de sécurité nationale et des activités de renseignement spécifiques dans le domaine de la sécurité nationale* ».

Au niveau européen, le seul texte contraignant doit être recherché du côté du Conseil de l'Europe. Outre la Convention européenne des droits de l'homme et la Convention STE 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard des données à caractère personnel, la Recommandation R.(87) 15 du Comité des ministres du Conseil de l'Europe[1] fait partie intégrante des règles encadrant l'exploitation des fichiers de police que la France s'est engagée à respecter. Les grands principes de la protection des données sont pour l'essentiel applicables.

La **Cour européenne des droits de l'homme** a prononcé plusieurs arrêts fixant un cadre pour les fichiers de police.

Ainsi, dans un arrêt *Amman contre Suisse* du 16 février 2000, elle a rappelé que les dispositions devaient être suffisamment claires et détaillées pour assurer une protection adéquate contre les ingérences des autorités dans le droit du citoyen à sa vie privée.

Plus récemment, dans un arrêt *S. et Marper contre Royaume-Uni* du 4 décembre 2008, la Cour a condamné le Royaume-Uni à propos de son fichier d'empreintes génétiques. Elle a considéré que « *le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions* ***mais non condamnées****, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'Etat défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique* »[2]. Cet arrêt rendu à l'unanimité de la Grande chambre condamne la conservation illimitée des données de toute personne impliquée dans une procédure judiciaire, quel que soit ensuite l'issue de cette procédure. Précisons que les requérants étaient mineurs à l'époque des faits.

---

[1] *Recommandation du 17 septembre 1987 concernant l'utilisation des données à caractère personne dans le secteur de* ***la police****. Elle a été complétée par un protocole additionnel du 8 novembre 2001.*

[2] *Considérant n° 125.*

On notera également avec intérêt un considérant d'ordre plus général : « ***La protection offerte par l'article 8 de la Convention (droit au respect de sa vie privée) serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part*** ».

A côté de ce corpus léger, mais clair dans ces principes, de règles européennes, notre législation nationale apparaît plus étoffée. Rappelons que la loi « Informatique et libertés » a dès l'origine eu pour objet principal les fichiers de l'Etat, et en particulier les fichiers de police. La loi du 6 août 2004 qui a transposé la directive européenne du 24 octobre 1995 n'a pas retranché de la loi du 6 janvier 1978 les dispositions relatives aux fichiers intéressant la sécurité, la sûreté de l'Etat ou la répression des infractions pénales.

D'où provient donc ce sentiment que depuis 2004, l'Etat se serait affranchi partiellement des grands principes régissant la protection des données ?

La principale explication tient à **la modification de la nature de l'avis de la CNIL rendu sur les décisions de création d'un fichier de police.**

Avant 2004, l'avis de la CNIL était un avis conforme. Il liait les pouvoirs publics, qui ne pouvaient passer outre que par un décret pris sur avis conforme du Conseil d'Etat. Désormais, il s'agit d'un **avis simple**. Il est toutefois rendu public.

Lors de la révision de la loi du 6 janvier 1978, l'argument avancé était que la publicité des avis suffirait à dissuader les pouvoirs publics de ne pas suivre les recommandations de la CNIL[1].

Toutefois, le bilan à cet égard est mitigé. A plusieurs reprises, le gouvernement est passé outre l'avis de la CNIL. Ce fut le cas par exemple à propos du projet de passeport biométrique. La CNIL s'opposait à la constitution d'une base nationale des empreintes digitales.

A l'appui de la nouvelle règle, on rappellera que la CNIL n'avait jamais eu recours à ce pouvoir de blocage, alors que d'importants fichiers de police, tels que ceux des renseignements généraux en 1991 –l'ancêtre du fichier EDVIGE finalement retiré au profit du futur fichier EDVIRSP– ou le STIC en 2001, ont été créés pendant cette période.

On peut aussi supposer qu'il y avait négociation préalable pour que le fichier soit conçu de telle façon qu'il n'y ait pas de problèmes justifiant le veto de la CNIL.

---

[1] *Cette nouvelle disposition figurait dans le projet de loi adopté en Conseil des ministres et déposé à l'Assemblée nationale le 18 juillet 2001.*

2. Les facilités offertes par les nouvelles technologies

Les auditions ont permis de mesurer à quel point les facilités apportées par certaines nouvelles technologies pouvait entraîner les individus, par ignorance ou par indifférence, à mettre de côté la protection de leur vie privée. Plusieurs exemples peuvent être mis en avant.

a) La géolocalisation : un traçage par nature

Les technologies de géolocalisation, qui visent à déterminer la localisation précise d'un individu, connaissent depuis quelques années un développement très important et tendent désormais à se banaliser dans le grand public.

Leurs applications sont multiples : guidage des véhicules par le système du GPS[1], personnalisation des services offerts à des utilisateurs nomades, suivi du déplacement d'un véhicule pour adapter le montant d'une prime d'assurance-automobile à la réalité des déplacements, surveillance des déplacements d'une personne pour la retrouver immédiatement, etc.

Ces technologies, qui apportent un **confort certain** à leurs utilisateurs, ne sont toutefois pas sans risques sur le droit à la vie privée. Puisque, par nature, elles visent à suivre ou « tracer » les déplacements des individus, elles sont en effet susceptibles de porter atteinte à l'une de ses deux composantes, à savoir « *le droit pour une personne à mener sa propre existence comme elle l'entend avec un minimum d'ingérences de l'extérieur* » (cf. *supra*).

b) La biométrie

La biométrie désigne l'ensemble des **technologies de reconnaissance physique ou biologique des individus**. En effet, chaque être humain se distingue de ses « semblables » par un ensemble de caractéristiques morphologiques et biologiques qui rendent son identification possible.

Comme l'a montré la mission d'information de la commission des lois consacrée à la nouvelle génération de documents d'identité et la fraude documentaire[2], dont nos collègues Charles Guené et Jean-René Lecerf étaient respectivement président et rapporteur, les technologies biométriques fonctionnent de façon similaire au **cerveau humain**, lequel effectue en permanence des opérations de reconnaissance biométrique, notamment de reconnaissance faciale : lorsque nous croisons un individu, nous mesurons inconsciemment l'écartement des yeux, la taille du nez, la position des oreilles. Ces informations sont comparées à notre mémoire afin d'y associer un nom.

---

[1] *Pour Global Positionning System.*

[2] *Rapport du Sénat n° 439 (2004-2005) consultable sur le site du Sénat à l'adresse suivante : http://www.senat.fr/rap/r04-439/r04-4391.pdf.*

Couplée à des traitements informatisés de plus en plus puissants, la biométrie peut **permettre l'identification d'un individu parmi plusieurs millions avec certitude**, en se basant sur la morphologie du visage, les empreintes digitales ou palmaires, la forme de la main, la reconnaissance de l'iris, les empreintes génétiques ou encore le dessin du réseau veineux de la main, étant précisé, en outre, que **la biométrie est universelle et immuable**, chaque être humain pouvant être identifié de la sorte quels que soient sa culture et son âge.

C'est pourquoi la biométrie est de plus en plus souvent utilisée pour garantir **l'authentification** d'une personne : en particulier, les Etats privilégient désormais cette technologie pour **limiter le risque de fraude aux titres d'identité.**

A titre d'exemple, à la suite des attentats du 11 septembre 2001, l'Organisation de l'aviation civile internationale, l'Union européenne et de nombreux Etats, au premier rang desquels les Etats Unis, ont décidé d'insérer dans les passeports des puces électroniques sécurisées comportant des données biométriques numérisées, notamment la photographie, pour identifier avec certitude leurs détenteurs.

De même, dans le cadre du projet d'identité nationale électronique sécurisée, appelé « projet INES », le Gouvernement français envisage d'équiper également les cartes nationales d'identité de puces électroniques sécurisées qui contiendraient des données biométriques numérisées (la photographie et les empreintes digitales).

Si l'on comprend la finalité ultime de ces technologies biométriques -lutter contre l'immigration clandestine, l'insécurité, le terrorisme[1]- il n'en demeure pas moins que, fondées sur le traitement de données éminemment sensibles, elles sont porteuses de risques nouveaux au regard du droit à la vie privée.

c) Les puces RFID ou le « sans contact »

L'identification par radiofréquence (en anglais « *Radio Frequency Identification* » ou RFID) est une technologie qui permet d'identifier et de localiser **sans contact** des objets ou des personnes grâce à une micropuce (également dénommée étiquette ou *tag*) qui dialogue par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à une dizaine de mètres.

Cette technologie, en plein essor, est utilisée dans un grand nombre d'applications :

- dans la distribution, notamment pour assurer la traçabilité des produits tout au long de la chaîne logistique ;

- dans les nouveaux titres d'identité sécurisés, comme les passeports ;

---

[1] *Même si la CNIL souligne que la biométrie n'est pas un système infaillible.*

- dans le domaine des transports, qu'il s'agisse des péages routiers ou des titres de transport, par exemple, le passe Navigo pour la RATP ou la carte Vélib' pour le système de vélos en libre service mis en place à Paris ; dans ces deux cas, les cartes doivent être approchées à quelques dizaines de centimètres du lecteur pour déclencher l'identification du titulaire et permettre ainsi, si ce dernier est en règle, l'accès à la station de métro ou l'emprunt d'un vélo.

Mais **l'avenir promet des applications encore plus diversifiées.** Les puces RFID pourraient ainsi être utilisées pour :

- connaître instantanément le contenu d'un caddie au supermarché et calculer immédiatement le prix global à payer ;

- distinguer les contrefaçons des produits authentiques ;

- assurer la traçabilité des produits de santé, tels que les médicaments ou les poches de sang ;

- améliorer la ponctualité des vols en localisant dans l'aérogare les passagers en retard, et ce au moyen de leur carte d'embarquement (projet Optag lancé par la commission européenne).

A moyen terme, le développement du « sans contact » devrait accompagner l'essor de **l'Internet des objets**. Si les applications futures ne sont pas encore clairement discernables, il faut imaginer que notre environnement sera de plus en plus peuplé d'objets communiquant avec le réseau par l'envoi et la réception d'informations et interagissant entre eux.

Or, si ces technologies sont sans conteste sources de progrès (gain de temps, lutte contre les atteintes à la propriété intellectuelle, plus grande efficience dans la gestion des produits de santé, meilleure fluidité du transport aérien, etc.), elles constituent **un défi nouveau au regard du droit à la vie privée.**

En effet, ces puces, qui, dans certains cas, « racontent une portion de vie d'un individu » **comportent des données personnelles** telles que le profil de consommation, des convictions religieuses ou politiques, etc., et il convient d'éviter que des tiers non autorisés puissent y avoir accès.

Aux Etats-Unis, les risques de la technologie RFID pour le respect de la vie privée sont d'ailleurs débattus depuis plusieurs années. La Federal Trade Commission[1] a remis plusieurs rapports, et l'association EPIC[2] a transmis en octobre 2008 une série de mesures tendant à renforcer la réglementation encadrant la technologie RFID. L'une d'entre elles est de **rendre visibles ces puces** pour les clients et d'alerter ces derniers par un son, une lumière ou un signal lorsque la puce est lue.

---

[1] *Voir notamment son rapport de mars 2005 consultable à l'adresse suivante : http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.*

[2] *Electronic Privacy Information Center. Cette association est la principale association de protection des données personnelles et des libertés civiles aux Etats-Unis.*

En effet, la **miniaturisation** de ces puces les rend toujours moins détectables tout en permettant d'y stocker des données plus nombreuses, voire de les doter de senseurs et de capacités de calcul.

Vos rapporteurs ont d'ailleurs pu constater, en se rendant au Minatec de Grenoble, que cette miniaturisation était aujourd'hui poussée à l'extrême dans le cadre de la nanotechnologie, technologie fondée sur l'étude, la fabrication et la manipulation de structures, de dispositifs et de systèmes matériels à l'échelle du nanomètre, c'est-à-dire du millionième de mètre (ou du millième de millimètre).

d) Les panneaux publicitaires communicants

Depuis un peu plus d'un an se développe une publicité d'un nouveau genre sur la voie publique.

Comme l'explique le rapport d'activité de la CNIL pour 2008, la publicité sur les téléphones mobiles par la technologie sans fil *Bluetooth* permet d'envoyer des messages publicitaires sur les téléphones portables à partir de panneaux publicitaires intégrant des bornes utilisant cette technologie. En pratique, dès qu'une personne s'approche de ce type d'affiche, elle reçoit un message l'invitant à accepter la réception d'une publicité sur son téléphone, dès lors que la fonctionnalité *Bluetooth* de celui-ci est activée.

Dans un registre proche, la société Majority Report[1], dont les dirigeants ont été entendus par vos rapporteurs, développe aussi des panneaux publicitaires auxquels est intégré un module de **mesure d'audience**. Ce module se compose en particulier de deux caméras. Les images ainsi captées ne sont ni enregistrées, ni transmises à des tiers, ni même visibles par les différents prestataires. Un algorithme permet d'isoler au sein de ces images les visages et de mesurer la durée du regard.

e) L'apparition d'outils de profilage statistique

Des offres de techniques automatisées de comptage, de repérage et de profilage des consommateurs à destination des acteurs de la grande distribution commencent à apparaître. Le fonctionnement est le suivant : un système complet de caméras est implanté dans l'ensemble de l'espace du point de vente ; ces caméras « captent » le visage des consommateurs et le convertissent, à partir d'un algorithme simple, en une série de chiffres ; le code ainsi créé est ensuite utilisé par la base de données pour retracer les déplacements du consommateur au sein du supermarché et établir ainsi des profils-types de comportements d'achats. Les concepteurs de ces solutions insistent bien sur le fait qu'un tel système a une finalité exclusivement

---

[1] *Le nom de cette société fait écho à la nouvelle de Philip K. Dick, Minority Report, portée à l'écran en 2002 par S. Spielberg et dans laquelle sont évoquées à la fois la prévention du crime par la détection précoce et la neutralisation des futurs auteurs de crimes et la reconnaissance individuelle obligatoire des clients entrant dans un magasin par des panneaux qui s'adressent à eux et leur proposent des marchandises en lien avec leurs anciens achats.*

statistique et commerciale, et qu'il ne s'agit en aucune manière de tracer nommément des individus, dont l'identité n'est à aucun moment collectée.

Vos rapporteurs sont tout à fait conscients de l'intérêt, sur le plan économique, du développement de ce type de système. Il apparaît néanmoins qu'il fonctionne en règle générale sur le principe « un code = un visage », et qu'il conserve en mémoire l'ensemble des déplacements et achats effectués par un « code » pendant l'ensemble de la durée de l'étude, laquelle peut atteindre plusieurs mois. Dès lors, il suffirait qu'à un moment donné, on puisse relier l'un de ces « codes » à une personne réelle pour être en mesure de retracer l'ensemble de ses déplacements et achats au cours de plusieurs mois au sein de ce supermarché.

Dans ces conditions, vos rapporteurs soulignent que **de telles techniques peuvent être ressenties comme intrusives par un certain nombre de nos concitoyens.**

f) Le cas particulier de la vidéosurveillance

Comme le souligne un récent rapport de la commission des lois du Sénat[1], la vidéosurveillance, après une phase de démarrage relativement lente, en raison notamment des craintes de l'opinion quant au respect des libertés individuelles et de la vie privée, **connaît aujourd'hui un essor important, en particulier sur la voie publique,** qui répond à l'émergence d'une demande forte de la population, convaincue que ce système joue un rôle dans la prévention des vols, agressions et mouvements de foule.

D'après le rapport précité, le nombre de caméras autorisées s'élevait, selon le ministère de l'Intérieur, à 396.000 à la fin de l'année 2007, réparties approximativement de la façon suivante :

- 80 % dans des établissements privés recevant du public ;

- 14 % dans les transports ;

- 6 % sur la voie publique.

Toutefois, le développement de la vidéosurveillance pose les mêmes questions que celui, évoqué plus haut, de la géolocalisation en ce qui concerne sa nécessaire conciliation avec le droit à la vie privée : puisque la vidéosurveillance a pour fonction de suivre les déplacements des individus, elle est en effet **susceptible de mettre à mal leur liberté d'aller et venir anonymement et tranquillement.**

De manière générale, les facilités offertes par ces technologies tendent à s'imposer d'autant plus à tous qu'il devient très difficile d'y échapper. L'individu qui s'affirmerait comme un « objecteur de conscience » de ces nouvelles technologies aurait en pratique les plus grandes difficultés à les fuir. Certains services ne sont désormais accessibles que par Internet[2] et,

---

[1] *Rapport d'information n° 131 (2008-2009) de nos collègues Jean-Patrick Courtois et Charles Gautier au nom de la commission des lois du Sénat et consultable à l'adresse suivante : http://www.senat.fr/rap/r08-131/r08-1311.pdf*

[2] *Les inscriptions universitaires par exemple.*

dans de nombreux cas, tout est fait pour décourager le recours aux guichets classiques (offres commerciales moins avantageuses, surcoûts…).

3. Une tendance croissante à « l'exposition de soi » : Internet et les réseaux sociaux

Internet offre aux institutions des opportunités de traçage des individus dans une mesure qui échappe très largement au contrôle, voire parfois à la connaissance, de ces derniers.

Toutefois, vos rapporteurs ont également été particulièrement sensibles à une nouvelle forme de traçage susceptible d'affecter le droit au respect de la vie privée des individus, apparue récemment avec le développement des nouvelles formes de sociabilité sur le *web* s'exprimant par le biais de *blogs* ou de réseaux sociaux (tels que Facebook, MySpace, etc.). Cette nouvelle forme de traçage se différencie radicalement des risques précédemment identifiés, en ce qu'**elle naît précisément de l'exposition consciente et volontaire, par les individus, de pans entiers de leur vie privée sur Internet.** De ce point de vue, elle met en jeu des dynamiques sociales radicalement nouvelles, dont les autorités et l'opinion publique commencent tout juste à prendre conscience.

a) Réseaux sociaux : description du phénomène

Les réseaux sociaux sont des services proposés par des sociétés de l'Internet et qui offrent aux individus la possibilité, d'une part, de se constituer une page personnelle (un « profil ») sur laquelle ces derniers déposent un certain nombre d'informations les concernant et, d'autre part, d'entrer en communication avec d'autres utilisateurs (appelés « contacts » ou « amis ») du même réseau avec lesquels ils peuvent échanger des messages ou des fichiers (photos, vidéos, etc.).

Les réseaux sociaux offrent ainsi de nouvelles opportunités d'échanges, de socialisation et de communication entre les personnes, sur un mode largement informel et « décontracté » qui privilégie la mise en relation d'individus partageant les mêmes centres d'intérêt. On estime par exemple qu'un utilisateur de Facebook est en moyenne relié à 120 « amis ».

Apparus à la fin des années 1990, ces réseaux sociaux ont connu depuis une croissance exponentielle. A titre d'exemple, Facebook affirme avoir 8 millions d'utilisateurs en France et 150 millions dans le monde. 70 % de ses utilisateurs français se situent dans la tranche des 18-34 ans, 15 % ont entre 13 et 17 ans. MySpace, de son côté, fait état de 230.000 utilisateurs dans le monde entier.

Le fonctionnement même des réseaux sociaux encourage leurs utilisateurs à dévoiler un grand nombre d'informations sur leur vie privée. On considère ainsi qu'un profil-type sur Facebook contient en moyenne 40 informations à caractère personnel, parmi lesquelles figurent nom, date de naissance, sexe, opinions politiques et religieuses, préférences

sexuelles, livres et films préférés, parcours scolaire, universitaire et professionnel, le tout accompagné de photographies, et parfois même de vidéos[1].

Or, **une fois qu'ils ont mis en ligne ces informations, les utilisateurs sont confrontés à un risque de perte de contrôle sur l'utilisation de ces données :** d'une part, ces informations peuvent être vues ou lues par des personnes ne figurant pas parmi les contacts de cet utilisateur ; d'autre part, elles peuvent être réutilisées à leur insu par d'autres membres de ce réseau.

b) Les risques liés à la visibilité

Comme l'explique le sociologue Dominique Cardon, alors que nous concevons la visibilité sur le *web* sur le modèle des medias traditionnels (tout ce qui y est publié est considéré comme unanimement et uniformément public, Internet serait un espace transparent d'informations accessibles à tous, en tous lieux et à tout moment), les utilisateurs des réseaux sociaux tendent à considérer Internet comme **un espace en clair-obscur**, comportant des zones d'ombre dans lesquelles les internautes pensent pouvoir rester en petits groupes et communiquer librement à l'abri des regards indiscrets. Cette conception du *web* comme un espace en clair-obscur incite les utilisateurs de réseaux sociaux à dévoiler un grand nombre d'informations sur eux-mêmes, dans la mesure où ils ont l'impression (à tort) que ces informations ne seront lues que par leurs proches. Les utilisateurs de réseaux sociaux livrent ainsi sur Internet des informations concernant leur vie privée de la même manière qu'ils pourraient tenir à voix haute des conversations privées en plein milieu d'une foule bruyante : la probabilité qu'un inconnu entende ce que l'on est en train de dire est infime. Pourtant, cette probabilité existe, et, depuis quelques mois, on assiste à une multiplication de mésaventures rencontrées par des utilisateurs de réseaux sociaux, « piégés » par les informations qu'ils avaient publiées sur Internet.

Voici quelques illustrations de mésaventures dont ont fait l'expérience des utilisateurs de *blogs* ou de réseaux sociaux au cours de ces dernières années ou de ces derniers mois :

- il y a quelques années, un étudiant américain s'est vu refuser un stage dans une grande entreprise pour avoir fait figurer « fumer des joints » parmi ses centres d'intérêt sur son profil Facebook ;

- en septembre 2008, la candidature d'une jeune femme est rejetée par un employeur potentiel, au motif que son C.V. contenait un lien vers son *blog* personnel, sur lequel, quelques jours avant l'entretien d'embauche, la jeune fille avait expliqué qu'elle se sentait « flemmarde »… ;

- il y a quelques semaines, des avocats ont utilisé, dans le cadre d'une affaire correctionnelle, des informations publiées sur Facebook pour discréditer l'une des

[1] *Pour une étude approfondie sur ce sujet, voir « Facebook and the Social Dynamics of Privacy », James Grimmelmann, Associate Professor of Law, New York Law School, étude disponible en libre accès sur Internet.*

parties au procès, produisant des photographies –sans aucun rapport avec l'affaire– représentant cette personne entourée de plants de cannabis… ;

- très récemment encore, une jeune femme, en arrêt maladie pour cause de migraines aigües, a été licenciée après que son employeur eut constaté qu'elle continuait à mettre à jour son profil Facebook depuis son domicile, ce qui tendait à démontrer, selon lui, qu'elle était apte à travailler.

Les concepteurs des réseaux sociaux ont pris conscience de ces risques et ont mis en place un système assez complet de « *privacy settings* », ou **« paramètres de confidentialité »**. Le but de ces outils de paramétrage est d'offrir aux utilisateurs les moyens de disposer d'un contrôle effectif sur les données personnelles qu'ils mettent en ligne, en leur permettant, pour chaque groupe de contacts, de définir avec précision quelles seront les informations accessibles à un large nombre d'utilisateurs et quelles seront les informations qui ne seront consultables que par ses « amis ». Ces options de paramétrage sont définies dans les conditions générales d'utilisation du site. Par exemple, les profils des utilisateurs mineurs de MySpace (13-17 ans) sont par défaut privés, alors que les profils des adultes sont par défaut publics, à charge pour ces derniers de paramétrer leur profil de façon plus stricte en fonction de leurs souhaits.

En dépit de leur caractère attrayant (les internautes auraient le plein contrôle de leurs données personnelles), ces options de paramétrage présentent en réalité deux failles majeures :

- La première est leur **mutabilité** : les conditions générales d'utilisation des réseaux sociaux font périodiquement l'objet de modifications, lesquelles ne sont qu'imparfaitement notifiées à leurs utilisateurs. A titre d'illustration, les utilisateurs de Friendster ou de Facebook ont ainsi tout d'abord bénéficié de profils totalement privés, avant qu'une partie de leurs informations personnelles ne soient rendue publiques par le gestionnaire du réseau social et ainsi accessibles à tous *via* les moteurs de recherche (et ce, faute pour l'utilisateur d'avoir fait la démarche d'activer une option d'« *opt out* »).

- La seconde est leur **ineffectivité** : des études réalisées aux Etats-Unis en 2007 ont montré que moins d'un tiers des utilisateurs de Facebook prenaient la peine de prendre connaissance des conditions générales d'utilisation du site avant de s'y inscrire. Ce désintérêt pour la politique de confidentialité mise en œuvre par les réseaux sociaux se double d'une tendance plus profonde à l'exposition de soi : selon Dominique Cardon, 69 % des photographies publiées sur Flickr sont rendues publiques par celui qui les met en ligne, alors même que celui-ci a la possibilité de les réserver à un espace privé. De même, 61% des utilisateurs de Facebook et 55 % des membres de Friendster choisissent, en dépit des outils de paramétrage qui leur sont offerts, de se rendre visibles à tous.

Ces éléments ont conduit vos rapporteurs à s'interroger sur **les mutations de la notion de vie privée** que ces réseaux sociaux révèlent, ainsi que sur les réponses nouvelles que de telles pratiques appellent (voir *infra*).

c) Les risques du fait d'autrui

Même lorsqu'il fait usage de l'ensemble des outils qui lui sont offerts par les réseaux sociaux pour protéger son intimité, l'utilisateur n'est pas à l'abri d'atteintes à sa vie privée causées par autrui. Tel est notamment le cas lorsque des informations, paramétrées au départ pour n'être visibles qu'à nos « amis », sont rendues accessibles aux « amis » de nos « amis », qui peuvent n'être à nos yeux que de vagues connaissances, voire de parfaits étrangers. **Dans les faits, la mise en œuvre de nos décisions en matière de confidentialité des informations à caractère personnel que nous mettons en ligne repose tout autant sur la discrétion ou le respect des autres que sur nos propres choix.**

A l'extrême limite, les risques d'atteinte à la vie privée peuvent concerner des personnes qui ont choisi de ne pas être membres d'un réseau social, puisque, en pratique, rien n'empêche un individu de publier des informations me concernant sur son profil, sans mon autorisation, voire même sans même que j'en sois informé.

Face à ces difficultés, les solutions proposées ne sont que partielles. La plus fréquemment citée concerne le « détaggage » des photographies : lorsqu'un internaute met en ligne des photographies sur lesquelles figurent un certain nombre de personnes nommément désignées (et donc facilement « traçables » grâce aux moteurs de recherche, pour peu que ces photographies aient été rendues publiques), un individu qui ne souhaiterait pas apparaître ainsi publiquement peut demander à Facebook de « détagger » la photographie (comprendre : supprimer la référence explicite à ses nom et prénom). Toutefois, s'il peut obtenir la suppression de la mention de son nom, il ne peut obtenir le retrait de la photographie elle-même, à moins d'obtenir gain de cause auprès de la personne qui l'a mise en ligne. Encore faut-il, s'il n'est pas membre du réseau, que cet individu ait eu connaissance de la publication de ces photographies…

En outre, comme l'ont relevé les Commissaires à la protection des données et de la vie privée, réunis à Strasbourg en octobre 2008, « *il existe actuellement très peu de protection contre la copie de toute sorte de données personnelles des profils d'utilisateurs (par d'autres membres du réseau concerné, ou par des tiers non autorisés extérieurs au réseau) et de leur utilisation ultérieure pour constituer des profils personnels ou bien même republier les données ailleurs.* ***Il peut être très difficile, et parfois même impossible, de retirer complètement l'information du Web une fois qu'elle est publiée*** *: même après la suppression sur le site d'origine (par exemple le site de réseau social), des copies peuvent être conservées chez des tiers ou des prestataires de service de réseaux sociaux. Les données personnelles des profils peuvent également « déborder » du réseau quand elles sont indexées*

par des moteurs de recherche. En outre, certains fournisseurs de service de réseaux sociaux donnent accès aux données d'utilisateurs à des tiers par des interfaces de programmation, ces tiers peuvent alors contrôler ces données. […] Parmi les autres dangers déjà identifiés figurent ***les risques d'usurpation d'identité****, favorisés par la large disponibilité des données personnelles dans les profils, et* ***le possible piratage de profils*** *par des tiers non autorisés* ».

d) De la vie privée à la vie publique

Dans son rapport précité sur la loi du 6 janvier 1978, notre ancien collègue Jacques Thyraud pressentait un des bouleversements majeurs induit par la révolution numérique : « *L'informatique a apporté essentiellement un changement de dimension : elle a introduit, en effet, une capacité de mémorisation considérable au point que certains peuvent craindre qu'elle ne porte atteinte à l'un des droits les plus fondamentaux de l'être humain : le droit à l'oubli* ».

De la même façon que l'invention de l'écriture ou de l'imprimerie ont transformé le rapport de l'homme à la mémoire, la numérisation et Internet créent les conditions d'une **hypermnésie de nos sociétés**.

Cet amenuisement du droit à l'oubli interroge moins notre vie privée que notre vie publique.

Tout d'abord, **la vie privée tend à se déverser dans la vie publique**, dès lors qu'un individu diffuse au public des informations relatives à sa vie privée. Les raisons sont multiples : banalisation de l'usage des techniques, stratégies de projection de soi, arbitrage en faveur d'une vie sociale riche (la « course aux amis » sur les réseaux sociaux), nouveau rapport à la pudeur, décloisonnement des cercles relationnels, sensibilisation insuffisante aux risques d'une exposition de soi et des autres sur Internet, etc.

Certes, à la suite des travaux de M. Dominique Cardon, entendu par vos rapporteurs, il convient de nuancer la véracité des faits relevant de la vie privée qui peuvent se retrouver délibérément sur des *blogs* ou des réseaux sociaux.

Ce dernier estime ainsi que la réussite des réseaux sociaux « *doit beaucoup au fait que les personnes prennent des risques avec leur identité en rendant publiques des informations sur elles-mêmes. Les réseaux sociaux exploitent une double dynamique […] : un processus de subjectivation qui conduit les personnes à extérioriser leur identité dans des signes qui témoignent moins d'un statut incorporé et acquis que d'une capacité à faire (écrire, photographier, créer…) ; et* ***un processus de simulation qui conduit les personnes à endosser une diversité de rôles exprimant des facettes multiples, et plus ou moins réalistes, de leur personnalité*** »[1].

---

[1] *Extrait de l'article « Pourquoi sommes-nous si impudiques ? » de M. Dominique Cardon, mis en ligne le 12 octobre 2008.*
Consultable à l'adresse suivante : http://www.arhv.lhivic.org/index.php/2008/10/12.

Si vos rapporteurs sont conscients qu'**une identité numérique** est aussi **une image construite** et gérée selon des stratégies diverses, il n'en reste pas moins que, pour un regard extérieur, il n'est pas aisé de faire la part des choses. Une fausse information peut être aussi pénalisante qu'une vraie. Par ailleurs, ce premier pas peut être perçu par des tiers comme **un consentement tacite** à d'autres révélations relatives à la vie privée. Brouiller les frontières est un jeu risqué. Il n'y a plus de ligne rouge.

Simultanément, à l'autre bout de la chaîne, la vie publique est devenue « hyper publique ».

Autrefois –puisque c'est désormais ainsi qu'il faut parler de l'ère avant Internet–, la vie publique recouvrait l'ensemble des faits n'entrant pas dans le champ de la vie privée, au sens où l'entend la Cour de cassation lorsqu'elle interprète l'article 9 du code civil.

M. Nicolas Bonnal, vice-président du Tribunal de grande instance de Paris et président de la 17ème chambre, a rappelé à vos rapporteurs que la jurisprudence de la Cour de cassation tendait à limiter le champ de la vie privée à la sphère familiale ou amicale -les autres informations étant diffusables par des tiers car relevant de la vie publique d'une personne.

Cette dichotomie a été forgée dans un monde où, malgré les progrès des communications, la création de bases de données de plus en plus grandes et le développement des média de masse, la reconstitution de la vie publique d'un individu demeurait un travail lourd et complexe.

Exceptée la situation particulière des personnages publics, la vie publique des individus demeurait confidentielle de facto ou, à tout le moins, accessible à un cercle restreint. En outre, le temps faisant son œuvre, la mémoire de la vie publique d'un individu s'effaçait, sauf à engager des recherches ciblées.

Désormais, Internet et l'utilisation de moteurs de recherche de plus en plus puissants permettent à chacun de nous d'interroger instantanément, à tout moment et n'importe où l'ensemble des informations mises en ligne sur la « toile ». **Ce qui autrefois exigeait une volonté résolue, des efforts et du temps ne requiert aujourd'hui qu'un peu de curiosité et une connexion Internet.** Les moteurs de recherche permettent d'agréger des sources d'information qu'il aurait été quasi-impossible de réunir auparavant.

A cet égard, l'expérience publiée dans la revue Le Tigre en décembre 2008 est particulièrement éclairante[1]. Un journaliste de cette revue a pu reconstituer une grande partie de la vie publique et privée d'un individu, qu'il n'avait jamais rencontré, à partir des seules données accessibles sur le web.

---

[1] *Revue Le Tigre. Volume 28 de novembre-décembre 2008 (également accessible dans le rapport d'activité pour 2008 de la CNIL).*

La vie publique, qui était en pratique discrète ou perdue de vue, est susceptible de se retrouver en pleine lumière, y compris pour des faits très anciens.

A n'en pas douter, ces évolutions changent la nature de la vie publique. **De la même façon qu'un individu a un besoin vital de vie privée pour se développer, on peut se demander dans quelle mesure un individu peut tolérer durablement une « hyper vie publique ».**

e) Une récente prise de conscience des autorités

Les autorités chargées de la protection des données personnelles ont récemment pris conscience des difficultés réelles liées à cette érosion du champ de la vie privée sous l'effet d'Internet et des réseaux sociaux.

Ainsi **la trentième Conférence mondiale des Commissaires à la protection des données et de la vie privée,** réunie à Strasbourg en octobre 2008, a-t-elle adopté **une résolution consacrée à la protection de la vie privée dans les services de réseaux sociaux.** Outre l'invitation à réaliser une large campagne d'information impliquant le plus grand nombre possible d'acteurs publics et privés, et destinée à prévenir les risques liés à l'utilisation des « services sociaux », les Commissaires ont adopté un certain nombre de recommandations à destination, d'une part, des utilisateurs de réseaux sociaux, et, d'autre part, des fournisseurs de tels services, insistant notamment sur la nécessité pour ces services de respecter pleinement la législation du pays dans lequel se trouve l'utilisateur, sur l'octroi d'un droit effectif d'accès et de rectification sur l'ensemble des données personnelles détenues par le réseau social ou encore sur l'éducation des utilisateurs au respect de la vie privée des autres.

Le 28 janvier 2009, à l'occasion de la troisième journée de la protection des données, M. Jacques Barrot, vice-président de la Commission européenne, a pour sa part consacré une partie de son intervention aux risques d'atteintes à la vie privée suscités par une utilisation déraisonnée des services offerts par les réseaux sociaux.

Vos rapporteurs ne peuvent que se féliciter de cette récente prise de conscience et espèrent que le présent rapport d'information contribuera à alimenter le débat sur les risques d'atteintes à la vie privée suscités par une utilisation déraisonnée et imprudente des réseaux sociaux. De ce point de vue, leur but n'est pas de pointer du doigt ces services qui offrent des possibilités formidables d'échanges et de partages entre les individus. Leur but est au contraire de **réfléchir aux moyens de promouvoir une utilisation responsable et respectueuse d'autrui de ces nouveaux outils de communication.** Au-delà d'une sensibilisation générale des individus à la notion de données à caractère personnel, ces réflexions ont conduit vos rapporteurs à s'interroger sur l'opportunité de reconnaître aux individus un droit de propriété sur leurs données personnelles, ainsi que sur les modalités selon lesquelles pourrait être mis en œuvre un « *droit à l'oubli* ». Ces réflexions font l'objet de la dernière partie du présent rapport.

II. UN CADRE JURIDIQUE PROTECTEUR À L'ÉPREUVE DE LA GLOBALISATION ET D'INTERNET

Les craintes d'atteintes à la vie privée qui viennent d'être exposées trouvent un grand nombre de réponses dans le dispositif de la loi « informatique et libertés » du 6 janvier 1978 et dans la directive 95/46/CE du 24 octobre 1995 qui en a repris, au niveau communautaire, l'essentiel des dispositions. **L'ensemble des personnes entendues se sont**, à cet égard, **accordées pour considérer que ces deux textes constituaient un cadre juridique adapté et satisfaisant.** Néanmoins, il est apparu que ce cadre juridique ne répondait qu'imparfaitement aux enjeux liés à la globalisation ainsi qu'aux spécificités d'Internet.

A. DES CRAINTES PARTIELLEMENT LEVÉES PAR UN CADRE JURIDIQUE SOUPLE ET PROTECTEUR

1. Les principes généraux de la loi « informatique et libertés » : des principes universels et intemporels

La loi du 6 janvier 1978 est née dans un contexte précis, à la suite du scandale du projet de fichier SAFARI[1] qui prévoyait l'institution d'un identifiant unique – le numéro de sécurité sociale également appelé numéro INSEE – afin d'interconnecter l'ensemble des fichiers de l'administration. L'informatique individuelle n'existait pratiquement pas et les principaux utilisateurs étaient l'administration et les grandes sociétés. La constitution de **fichiers administratifs géants** était la crainte principale.

Toutefois, le législateur de l'époque avait conscience de légiférer pour un avenir laissant présager un développement extraordinaire et imprévisible de l'informatique. Notre ancien collègue Jacques Thyraud, rapporteur de la loi « informatique et libertés », soulignait dans son rapport que « *la tâche du législateur consiste à faire des lois les plus générales et les plus claires possible afin de permettre, dans l'application, une certaine souplesse. Cette exigence est d'autant plus forte que le secteur auquel s'applique la loi est plus technique et évolutif* ».

Cette philosophie a inspiré les rédacteurs de la loi du 6 février 1978 autant que ceux de la directive européenne 95/46/CE du 24 octobre 1995 et de la loi du 6 août 2004 qui l'a transposée.

Elle a conduit à dégager quelques principes généraux applicables à toutes les technologies et applications informatiques, plutôt qu'à multiplier des dispositifs particuliers pour chacune d'entre elles.

---

[1] *Système Automatisé pour les Fichiers Administratifs et le Répertoire des individus.*

M. Alex Türk, président de la CNIL, a distingué quatre grands principes : les principes de **finalité**, de **proportionnalité**, de **sécurité** et d'**accès aux informations**.

La loi « informatique et libertés » adoptée le 6 février 1978 ne les énonçait pas tous. Ils transparaissaient néanmoins en filigrane et ont été clairement affirmés depuis par la directive du 24 octobre 1995 et la loi du 6août 2004.

a) Le principe de finalité

Le premier principe est celui de finalité. La loi adoptée en 1978 ne le formulait pas explicitement, mais l'utilisation d'un traitement à d'autres fins que celles définies lors de sa création était déjà constitutive d'un délit puni de cinq ans d'emprisonnement. L'article 6 de la loi du 6 février 1978 en vigueur dispose depuis 2004 que les données à caractère personnel « *sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* ».

b) Le principe de proportionnalité

Ce principe est à la fois distinct et connexe du principe de finalité. Ce principe général du droit ne figure pas littéralement dans la loi du 6 février 1978 modifiée. Mais il inspire sans ambiguïté son article 6 qui dispose que les données à caractère personnel doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » et ne peuvent être conservées que « *pendant une durée (n'excédant) pas la durée nécessaire aux finalités* ».

c) Le principe de sécurité des données

L'article 34 de la loi du 6 février 1978 modifiée[1] impose à tout responsable d'un traitement de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

d) Le droit d'accès et de rectification

Le dernier principe est celui du droit d'accès et de rectification. Il fut affirmé explicitement dès 1978, l'article 3 disposant alors que « *toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés* ». Ces droits d'accès et de rectification, lorsque les données sont « *inexactes, incomplètes, équivoques, périmées* », ont été repris par les articles 39 à 43 de la loi du 6 février 1978 modifiée.

---

[1] *Article 29 du texte adopté en 1978.*

e) Les autres droits reconnus par la loi « informatique et libertés »

A ces quatre principes qui s'appliquent peu ou prou à l'ensemble des traitements de données à caractère personnel, il faut ajouter d'autres droits essentiels mais d'application circonscrite.

Il en va ainsi du **droit à l'information** défini à l'article 32 de la loi du 6 janvier 1978 modifiée. En cas de collecte de données personnelles directement auprès de la personne concernée, celle-ci doit être informée de l'utilisation qui peut en être faite. Ces dispositions ne s'appliquent pas aux traitements intéressant la sûreté de l'Etat ou la sécurité publique.

En cas de **collecte indirecte** de ces données, ce droit à l'information existe théoriquement. Mais le responsable du traitement peut s'en exonérer si cette information « *se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche* ».

Le **droit d'opposition** à l'utilisation de ses données personnelles est également primordial. Il est le corollaire du droit à l'information. Affirmé dès 1978[1], il figure désormais à l'article 38 de la loi qui précise que toute personne physique « *a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur* ». Dans les autres cas, ce droit s'exerce sous réserve de « *motifs légitimes* ». Toutefois, ce droit d'opposition ne s'applique pas lorsque le traitement répond à une obligation légale.

La loi initiale du 6 janvier 1978 ne prévoyait pas **un droit au consentement préalable**. Ce nouveau droit n'a été affirmé qu'à la suite de la loi du 6 août 2004. L'article 7 de la loi du 6 janvier 1978 modifiée proclame désormais qu'« *un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée* ». Ce principe est toutefois assorti de dérogations si nombreuses qu'en pratique, le régime applicable est essentiellement celui du droit d'opposition précité.

2. La neutralité technologique de la loi « informatique et libertés »

Ces principes ont irrigué les différents textes nationaux, européens ou étrangers relatifs à la protection des données personnelles.

L'ensemble des personnes entendues par vos rapporteurs a souligné **la modernité de ces principes et leur extrême plasticité.**

Ils se révèlent applicables et adaptés à l'ensemble des nouvelles technologies numériques qu'elles aient pour effet principal[2] ou incident de collecter des données permettant de tracer un individu dans le temps et l'espace.

---

[1] *Article 26 du texte de 1978.*

[2] *La géolocalisation par exemple.*

La CNIL s'est affirmé comme **l'interprète vigilant de ces principes**. Elle a développé, à mesure que de nouvelles applications apparaissaient, une doctrine exigeante, avec pour souci principal d'éviter que les individus ne se voient imposer, pour des raisons de confort ou d'efficacité, des dispositifs excessivement intrusifs.

Elle s'est également attachée à démontrer **que l'éclosion de nouvelles technologies et applications n'ouvrait pas de vides juridiques**, la loi du 6 janvier 1978 modifiée et ses grands principes demeurant pertinents.

Vos rapporteurs ont ainsi acquis la conviction que les équilibres de la loi du 6 janvier 1978 devaient être préservés et qu'il serait préjudiciable de s'engager sur la voie de législations spécifiques pour certaines technologies ou applications.

Cette dernière solution qui pourrait apparaître séduisante dans l'instant présente en réalité plusieurs inconvénients :

- elle crée des vides juridiques à mesure que de nouvelles technologies apparaissent, le législateur ayant souvent un temps de retard dans ces domaines ;

- elle sera nécessairement partielle ou lacunaire ;

- elle peut bloquer des évolutions technologiques.

A l'inverse, en s'appuyant sur des principes universels, le législateur se met à l'abri d'être dépassé par la technique. En outre, comme le montre la CNIL, ces principes ménagent **un espace de négociation ou d'interaction** entre l'autorité compétente, les utilisateurs et les industriels.

Une technologie n'est pas mauvaise en elle-même. Cela dépend de l'usage qui en est fait ainsi que des modalités selon lesquelles elle est mise en œuvre.

Les industriels rencontrés par vos rapporteurs –Thalès, Sagem, Majority Report, Google, Microsoft, Facebook, My Space– ont fait part de leur dialogue constant et constructif avec la CNIL.

Une technologie ou un service qui pose des problèmes au regard du respect de la vie privée peut ne plus en poser quelques temps après. Le dialogue dynamique que permettent les grands principes pousse ainsi les industriels à développer des solutions techniques nouvelles plus respectueuses de la vie privée. Il évite aussi les réponses toutes faites.

Les exemples ci-après, parfois très récents, illustrent ces conclusions.

a) La géolocalisation

Certaines technologies de localisation posent peu de difficultés au regard du respect de la vie privée. Ainsi, en est-il de l'utilisation d'un navigateur GPS pour indiquer la meilleure route si les données collectées ne sont pas exploitées par un intervenant extérieur et si le navigateur n'est pas relié nominativement à son utilisateur. Dans ces conditions, l'anonymat est préservé.

En revanche, d'autres utilisations ont requis l'intervention de la CNIL qui a considéré que la loi du 6 janvier 1978 modifiée était applicable.

Plusieurs délibérations ont fixé un cadre.

La première fut une délibération du 17 novembre 2005[1] par laquelle **la CNIL s'est opposée à un projet de personnalisation des primes d'assurance en fonction de l'usage réel d'un véhicule.** En l'espèce, l'assureur proposait de réduire le montant de la prime en contrepartie de l'installation d'un système de géolocalisation à bord du véhicule afin de lui permettre de vérifier le cas échéant le respect des engagements contractuels. La géolocalisation devait permettre en particulier de contrôler le respect des vitesses maximales autorisées.

La CNIL s'y est opposée et a rappelé plusieurs principes issus de la loi du 6 janvier 1978 modifiée.

Tout d'abord, l'article 9 de cette loi ne permet pas à une personne de droit privé de mettre en œuvre un traitement relatif aux violations des limitations de vitesse. Un assureur ne peut donc pas enregistrer les excès de vitesse de ses clients.

Surtout, la délibération rappelle qu'il appartient à la CNIL « *d'apprécier, au regard de la loi du 6 janvier 1978 modifiée et notamment de son article 6, la proportionnalité des moyens mis en œuvre* ». Elle a alors considéré que la collecte systématique des données relatives à la localisation des véhicules utilisés à titre privé à des fins de modulation de tarifs d'assurance automobile était de nature « *à porter atteinte à la liberté d'aller et venir anonymement dans des proportions injustifiées* ».

Ces positions de la CNIL ont conduit les assureurs à repenser leurs offres, illustrant ce dialogue constructif permanent pour concilier des intérêts divergents. Dans son rapport d'activité pour 2008, la CNIL annonce qu'elle devrait adopter de nouvelles recommandations.

D'autres délibérations sont ensuite intervenues, notamment pour répondre à la demande croissante de géolocalisation dans les entreprises.

Le 16 mars 2006, la CNIL a ainsi adopté deux délibérations[2] relatives à la géolocalisation des véhicules des employés des organismes publics ou privés.

Elles précisent les finalités possibles de tels traitements. Si le suivi du temps de travail d'un employé peut se faire par ce moyen, encore faut-il que ce soit une finalité **accessoire** et que ce suivi ne puisse être réalisé par d'autres moyens.

---

[1] *Délibération n° 2005-278 du 17 novembre 2005 portant refus de la mise en œuvre par MAAF assurances SA d'un traitement automatisé de données à caractère personnel basé sur la géolocalisation des véhicules.*

[2] *Délibérations n° 2006-66 et n° 2006-67 portant adoption respectivement d'une recommandation et d'une norme simplifiée. Les traitements remplissant les conditions fixées par une norme simplifiée bénéficient d'un régime de déclaration allégée.*

Elles estiment également que le principe de proportionnalité justifie une conservation inférieure à deux mois, sauf exception.

Elles rappellent l'obligation d'information et de consultation des instances représentatives du personnel. Chaque employé doit être informé individuellement.

Enfin, elles recommandent que les employés puissent **désactiver** la fonction de géolocalisation des véhicules à l'issue de leur temps de travail lorsque ces véhicules peuvent être utilisés à des fins privées. C'est une des conséquences du principe de finalité.

b) La biométrie

En matière de biométrie, la CNIL a élaboré une grille d'analyse exigeante qui est désormais stable depuis quatre ans.

Cette grille **n'interdit pas le recours à la biométrie**. Elle oblige à **utiliser les systèmes biométriques strictement nécessaires à l'objectif poursuivi.** Sont ainsi privilégiés les identifiants biométriques ne laissant aucune trace et les systèmes sans base centrale de données biométriques. Le recours à la biométrie avec trace n'est autorisé que **si elle constitue le seul moyen d'atteindre le résultat recherché.**

Enfin, vos rapporteurs ont également relevé que la rigueur de la CNIL dans cette matière **avait poussé les industriels à mettre au point des systèmes biométriques plus respectueux de la vie privée et de l'anonymat**, notamment par l'utilisation de la cryptographie et de nouveaux identifiants biométriques comme le réseau veineux.

En sens inverse, la CNIL a autorisé en 2007 la mise en œuvre de trois programmes de recherche dans le domaine de la biométrie.

c) Les panneaux publicitaires communicants

Saisie de cette publicité d'un genre nouveau, la CNIL a exigé **le recueil du consentement préalablement à l'envoi de ces messages publicitaires par Bluetooth.** Une solution, afin que seules les personnes réellement intéressées par le contenu publicitaire soient sollicitées, est d'obliger celles-ci à approcher leur téléphone à quelques centimètres de l'affiche. Ce geste volontaire atteste de leur consentement.

Dans un registre proche, les dirigeants de la société Majority Report, qui développe notamment des panneaux publicitaires auxquels est intégré un module de mesure d'audience (cf. *supra*), ont indiqué être en contact avec la CNIL pour s'assurer du respect des principes de la loi du 6 janvier 1978. Dans un communiqué du 22 avril 2009, la CNIL s'est déclarée compétente, notamment pour vérifier que les images capturées étaient bien retraitées de manière à rendre impossible l'identification des personnes.

d) L'apparition d'outils de profilage statistique

Si un débat juridique peut exister sur l'applicabilité de la loi du 6 janvier 1978, compte tenu du fait que le traitement des images capturées ne permet pas d'identifier avec certitude les personnes concernées, le caractère intrusif ou à tout le moins ressenti comme tel de ces dispositifs d'un nouveau genre justifierait l'application des principes « informatique et libertés » au premier rang desquels le droit à l'information préalable et la durée de conservation limitée des données.

Enfin, la CNIL serait compétente pour s'assurer de l'irréversibilité de l'anonymisation.

e) Les puces RFID

Appliqués à la RFID, les grands principes de la protection des données demeurent pertinents.

L'exemple du Pass Navigo

La RATP a progressivement substitué au coupon magnétique mensuel (« carte orange ») une carte à puce RFID dénommée Pass Navigo.

M. Dominique Chaumet, correspondant informatique et libertés à la RATP, a indiqué que les premières discussions avec la CNIL avaient été nouées en 2002. Les motivations de ce nouveau système sont la lutte contre la fraude et la capacité de ce support à accueillir un plus grand nombre d'information.

Des discussions avec la CNIL, il est ressorti plusieurs décisions importantes pour limiter les risques d'atteinte à la vie privée et à la liberté d'aller et venir.

Tout d'abord, le système n'est pas configuré pour permettre de suivre les déplacements d'un abonné, y compris a posteriori. Les données relatives au lieu et à l'heure de validation du pass ne sont conservées que 20 minutes en station. Seuls le numéro du pass et le jour sont conservés pour détecter des fraudes –cas où une carte serait dupliquée et utilisée par des dizaines voire des centaines de personnes.

Ensuite, la CNIL a obtenu que la RATP propose à ses clients des pass Navigo anonymes. Il est toutefois à un peu plus cher (5 euros de plus lors de son achat, mais non à l'occasion de son rechargement) et, en cas de perte ou de vol, il n'est pas remplacé gratuitement. Ce pass anonyme est une concession importante pour la RATP, puisqu'il ne permet pas de détecter automatiquement une fraude à grande échelle.

Enfin, ce n'est pas la RATP qui conserve les données nominatives. La gestion des abonnements est assurée par une entité distincte, le GIE Commutitres, fondé par la SNCF, la RATP et l'association Optile.

Ainsi, le principe de finalité a inspiré l'affirmation d'« *un droit au silence des puces* ». Les puces RFID sont souvent utilisées pour suivre un produit tout le long de la chaîne logistique. Elles n'ont plus lieu d'être actives dès l'instant où le client final a acheté le produit. Ce droit peut se traduire de deux manières soit par la destruction de la puce, soit sa désactivation. Dans ce dernier cas, le consommateur pourrait choisir de réactiver la puce, notamment s'il en attend un service particulier.

Sous l'impulsion de la présidence française de l'Union européenne, **le Conseil des ministres Telecoms du 27 novembre 2008 a reconnu ce « droit au silence des puces »**. Il pourrait inspirer de futures législations, notamment en matière de droit de la consommation.

Toutefois, vos rapporteurs estiment que si ces données sont considérées comme des données personnelles dès l'instant où elles racontent une portion de vie d'un individu et qu'elles sont utilisées par un tiers, la législation sur la protection des données à caractère personnel permet déjà de poser des garde-fous.

Le **droit au silence** serait le premier. Selon que la puce serait automatiquement désactivée ou désactivable, nous serions dans un cas de droit au consentement préalable ou de droit d'opposition.

Au regard du principe de proportionnalité, certains usages devraient être écartés. Ainsi, en Espagne, des puces RFID ont été injectées à la demande sous la peau pour servir de moyen de paiement dans certaines discothèques, ce qui apparaît tout à fait disproportionné. En revanche, dans certaines maternités, des expérimentations sont en cours pour équiper les nouveau-nés de bracelets RFID, afin d'éviter les kidnappings. Cette utilisation très temporaire apparaît déjà moins problématique.

Le **droit à l'information** impliquerait de rendre les puces visibles et de signaler clairement lorsqu'elles sont actives.

Le **principe de sécurité**, rejoignant ici le principe de finalité, imposerait qu'une puce ne soit pas lisible par n'importe qui lorsqu'elle est devenue porteuse d'une donnée personnelle.

f) Le cas particulier de la vidéosurveillance

Sauf exception, la vidéosurveillance des espaces publics ne relève pas de la loi du 6 janvier 1978. Les conditions d'utilisation de la vidéosurveillance sont fixées par l'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation pour la sécurité.

Toutefois, si la compétence de la CNIL est écartée, le législateur s'est directement inspiré des principes de la loi du 6 janvier 1978 pour bâtir un dispositif législatif conciliant les nécessités de la prévention de l'ordre public et la protection des libertés. Ces principes sont les suivants :

- principes de licéité et de finalité (les finalités sont limitativement énumérées) ;

- conservation limitée des enregistrements (30 jours maximum) ;

- droit d'accès des personnes filmées aux enregistrements ;

- protection des enregistrements ;

- information générale du public sur l'existence d'un système de vidéosurveillance ;

- protection de la vie privée avec l'interdiction de filmer des lieux assimilables à des « *informations nominatives sensibles* » : intérieur des immeubles d'habitation, y compris l'entrée de ces immeubles.

Fort de ce constat, le groupe de travail de la commission des lois sur la vidéosurveillance[1] **a préconisé de rapatrier la vidéosurveillance dans le champ de la loi du 6 janvier 1978 et de la CNIL.**

Vos rapporteurs partagent ces conclusions à l'heure de la convergence numérique. En outre, **les technologies étant de moins en moins utilisées isolément mais au contraire combinées entre elles** –par exemple la biométrie avec la vidéosurveillance–, **l'existence d'une législation unique reposant sur quelques principes est un facteur important de simplicité et de clarté de la loi.**

3. Les gardiens vigilants de la protection des données personnelles : la CNIL, le G29 et le contrôleur européen des données

Vos rapporteurs ont pu constater que le droit à la vie privée est aujourd'hui protégé de manière relativement satisfaisante, même à l'épreuve des nouveaux défis présentés dans la première partie du rapport, non seulement parce qu'il est largement consacré dans les textes et qu'il s'appuie sur des principes intemporels, mais aussi parce que **son respect est assuré par certaines autorités indépendantes**, aux premiers rangs desquelles figurent la CNIL, le G29 et le contrôleur européen des données.

a) La CNIL

(1) Une autorité administrative indépendante collégiale

La Commission nationale pour l'informatique et les libertés (CNIL) est une autorité administrative indépendante, créée par la loi de 1978 précitée.

Notons d'ailleurs que cette loi est la première à consacrer la notion d'autorité administrative indépendante. L'amendement créant cette nouvelle entité fut présenté par M. Jacques Thyraud, rapporteur au nom de la commission des lois du Sénat, à l'article 6 du projet de loi[2]. L'Assemblée nationale proposait à l'époque d'en faire un service du ministère de la Justice.

Comme la quasi-totalité des autorités administratives indépendantes, la CNIL est une instance collégiale ; elle est composée de quinze membres nommés pour cinq ans :

- 2 sénateurs,

- 2 députés,

---

[1] *Rapport d'information n° 131 (2008-2009) de nos collègues Jean-Patrick Courtois et Charles Gautier au nom de la commission des lois du Sénat et consultable à l'adresse suivante : http://www.senat.fr/rap/r08-131/r08-1311.pdf*

[2] *Cf. rapport n° 72, 1977-1978.*

- 2 conseillers d'Etat,

- 2 conseillers à la Cour de cassation,

- 2 conseillers à la Cour des comptes,

- 5 personnalités qualifiées désignées par le président du Sénat (1 personnalité), par le président de l'Assemblée nationale (1 personnalité) et le Conseil des ministres (3 personnalités).

(2) Ses missions au service de la protection de la vie privée

Jusqu'à la loi du 6 août 2004, la CNIL avait pour missions, aux termes de la loi de 1978, d'une part, d'effectuer des missions de contrôle ou de vérifications sur place (324 missions de ce type ont été enregistrées de 1978 à 2003), d'autre part, d'adopter, en séance plénière, des délibérations qui se déclinaient en :

- des avis sur des **projets de loi ou de décret** ;

- des avis sur des **traitements ou des fichiers** ;

- des **normes simplifiées** pour les traitements publics ou privés les plus courants qui ne comportent pas d'atteinte manifeste à la vie privée ou aux libertés. Entre 1978 et 2003, la CNIL a édicté quarante-deux normes simplifiées (voir par exemple la délibération n° 03 067 du 18 décembre 2003 sur la gestion et les négociations des biens immobiliers) ;

- des **recommandations**, qui, bien que dépourvues de force juridique contraignante, définissent une ligne de conduite dans des secteurs d'activité particuliers. Elles illustrent la mission de conseil et d'accompagnement de la CNIL à l'égard des responsables de traitements de données. Entre 1978 et 2003, la CNIL a publié une trentaine de recommandations, dont la délibération n° 03-036 du 1er juillet 2003 qui concerne la sécurité des systèmes de vote électronique ;

- des **avertissements** ou **dénonciations au parquet** : entre 1978 et 2003, cinquante-quatre avertissements et trente-quatre dénonciations au parquet ont ainsi été recensés.

La loi n° 2004-801 du 6 août 2004, modifiant la loi de 1978, a profondément enrichi les moyens d'action de la CNIL. Elle a en effet précisé et renforcé son pouvoir de contrôle, l'a dotée d'un pouvoir de sanction de nature quasi-juridictionnelle, d'un droit de veto a priori pour les traitements de données les plus sensibles et créé des correspondants informatique et libertés.

La CNIL, par l'intermédiaire de ses commissaires et de ses agents, dispose désormais de **pouvoirs de contrôle sur pièces et sur place**, dans les horaires des perquisitions judiciaires (6 heures à 21 heures). Pour garantir le bon exercice de cette mission, le législateur a créé un « délit d'entrave » qui punit d'un an d'emprisonnement et de 15.000 euros d'amende le fait de s'opposer à l'accomplissement d'une opération de contrôle de la CNIL.

Ces missions de contrôle s'inscrivent dans le cadre du **programme annuel des contrôles**, adopté par la Commission en fonction des thèmes jugés prioritaires au vu de l'actualité, ou répondent à des **besoins ponctuels** identifiées par la CNIL, dans les cas suivants :

• dans le cadre du prolongement des formalités préalables (le traitement mis en œuvre est-il conforme à la déclaration ou à l'autorisation ? le refus d'autorisation prononcé par la Commission est-il respecté ? quelles sont les pratiques des autres responsables de traitement ? les mesures de sécurité décrites sont-elles effectivement mises en place ? …) ;

• dans le cadre de l'instruction de plaintes significatives dont le contenu laisse à penser que le responsable de traitement est en infraction avec la loi de 1978 ;

• afin de vérifier le respect des recommandations ou normes simplifiées élaborées par la CNIL ;

• afin d'apporter des éléments d'information dans le cadre de groupes de travail constitués au sein de la CNIL.

En outre, jusqu'à la loi précitée de 2004, lorsque la CNIL constatait, à l'occasion d'un de ses contrôles, un manquement aux obligations prévues par la loi « informatique et libertés », elle ne pouvait que prononcer un avertissement ou dénoncer les faits au parquet.

Aussi le législateur a-t-il décidé, en 2004, conformément à la directive européenne de 1995, de doter la Commission d'un **pouvoir de sanction de nature quasi-juridictionnelle**. Il a ainsi créé une nouvelle structure, dénommée « formation restreinte », composée du président, des deux vice-présidents et de trois membres élus par la commission en son sein pour la durée de leur mandat.

Cette formation dispose de **trois niveaux d'intervention** : la mise en demeure, l'avertissement et, uniquement pour les entreprises, la sanction pécuniaire, décisions que la CNIL peut décider de rendre publiques.

Il faut noter que depuis l'entrée en vigueur de ces nouveaux pouvoirs, le décret d'application n° 2005-1309 étant paru le 20 octobre 2005, la CNIL a prononcé **trente-deux sanctions** représentant, au total, **520.400 euros d'amende**.

Un autre apport de la loi de 2004, en conformité avec la directive de 1995, a été de doter la CNIL **d'un droit de veto *a priori*** pour les traitements de données les plus **sensibles**, tels que les traitements biométriques, ceux portant sur des données génétiques, comportant des appréciations sur les difficultés sociales des personnes, ou encore les traitements susceptibles d'exclure des personnes du bénéfice d'un droit (article 25 de la loi de 1978 modifiée).

Le non-respect de l'autorisation préalable est passible de lourdes sanctions (cinq ans d'emprisonnement et 300.000 euros d'amende) en application des dispositions de l'article 226-16 du code pénal.

Enfin, le législateur a décidé en 2004, à l'initiative de M. Alex Türk, alors rapporteur au nom de la commission des lois du Sénat, de donner la possibilité aux entreprises et administrations publiques d'identifier, en leur sein, **des « correspondants informatique et libertés »**, relais de la CNIL et garants du respect de la loi de 1978. En contrepartie, les structures qui désignent un tel correspondant ne sont plus tenues d'adresser leurs déclarations à la CNIL car désormais le correspondant recense ces fichiers. Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à autorisation préalable de la CNIL.

S'il n'est pas prévu d'agrément par la CNIL, le correspondant devant simplement, selon la loi, bénéficier des « *qualifications requises pour exercer ses missions* », il apparaît que, le plus souvent, la personne désignée possède, en pratique, des compétences en informatique, droit, conseil et management (le correspondant a un rôle d'information et d'audit de l'organisme) ainsi que dans le domaine de la médiation et de la pédagogie (le correspondant vise à favoriser le dialogue entre le responsable du traitement, les personnes faisant l'objet du traitement et la CNIL).

Un correspondant peut exercer sa mission pour le compte de plusieurs organismes lorsqu'il est, par exemple, consultant, avocat, etc. : ainsi, au 31 mars 2009, la France comptait 1.273 correspondants représentant quelque 5.066 organismes.

b) Le G29 et le contrôleur européen des données

(1) Le G29

Le G29, créé par l'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation, est **un groupe de travail européen** rassemblant les représentants de vingt-sept autorités indépendantes de protection des données nationales.

Il est présidé, depuis février 2008, par M. Alex Türk, président de la CNIL.

Réuni à Bruxelles en séance plénière tous les deux mois environ, il a pour missions principales :

- de rendre des avis sur le niveau de protection dans les pays extra-communautaires ;

- 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 ;

- et d'adopter des recommandations générales dans ce domaine.

Sur ce dernier point, de nombreuses personnes entendues par vos rapporteurs ont souligné le rôle essentiel de cette instance, qui permet de définir, au niveau communautaire, des **positions harmonisées** dans le cadre des négociations avec les pays situés hors de l'Union européenne, et notamment les Etats-Unis, qu'il s'agisse de l'affaire PNR, SWIFT, ou encore Google (voir *infra*).

Aviser ne peut –ou que regretter, à la suite du dernier rapport d'activité de la CNIL, que cette instance soit « un colosse aux pieds d'argile ». En effet, elle ne dispose **pas de moyens propres** puisque son secrétariat est assuré par l'unité chargée de la protection des données à la direction générale « Justice, Liberté et Sécurité » de la Commission européenne.

(2) Le contrôleur européen des données

Le Contrôleur européen des données est une autorité de contrôle indépendante, créée en 2001, dont la principale mission est de contrôler les traitements de données à caractère personnel **effectués par l'administration de l'Union européenne.**

La fonction est aujourd'hui exercée par M. Peter Hustinx qui dispose d'une équipe de trente-cinq personnes et s'appuie sur l'existence d'un correspondant dans chaque administration communautaire.

B. UN CADRE NÉANMOINS PARTIELLEMENT INADAPTÉ AUX ENJEUX DE LA GLOBALISATION ET AUX SPÉCIFICITÉS D'INTERNET

1. La protection des données à l'épreuve de l'extraterritorialité

Vos rapporteurs ont pu constater que le cadre juridique actuel n'apporte pas toujours des réponses satisfaisantes aux nouveaux défis au regard du droit à la vie privée, notamment parce qu'il existe **des divergences d'interprétation** concernant **l'applicabilité du droit communautaire** aux traitements de données effectuées par des entreprises situées en dehors de l'Union européenne, en particulier aux Etats-Unis. Ces divergences prennent un relief particulier car Européens et Américains n'ont pas les mêmes approches en matière de protection des données personnelles.

a) La question du droit applicable

La question du droit applicable en matière de protection des données est particulièrement complexe.

Certes, la directive précitée de 1995 sur la protection des données comporte, en son article 4, une clause sur la loi applicable aux traitements de données à caractère personnel effectués par des entreprises. Toutefois, s'agissant des sites Internet, « *cette disposition n'est pas aisée à comprendre ou à manipuler* » comme l'a reconnu le G29 dans un document de travail adopté le 30 mai 2002.

En effet, l'article 4 de la directive prévoit les cas de figure suivants :

- si l'entreprise est établie sur le territoire de l'un des Etats-membres, la législation de cet Etat s'applique même si l'entreprise fournit des services à d'autres Etats-membres, et ce en application du **principe du pays d'origine**. Ce dernier est favorable aux entreprises, qui n'ont pas à être soumises à plusieurs législations nationales, sans pour autant mettre à mal la protection

des données personnelles dans l'Union européenne dans la mesure où, par l'effet de la directive de 1995, les lois nationales en matière de protection des données **offrent des protections équivalentes** ;

- si l'entreprise n'est pas établie sur le territoire de l'un des Etats-membres mais qu'elle recourt, à des fins de traitement de données à caractère personnel, à des « moyens » situés sur le territoire d'un Etat-membre[1], le droit de ce dernier s'applique[2]. La directive a donc repris un critère classique en droit international, à savoir le lien physique entre l'action et un système légal.

Ce second cas de figure soulève **des difficultés d'interprétation**, comme l'a illustré le différend entre le G29 et certains moteurs de recherche sur Internet établis aux Etats-Unis, concernant la durée de conservation des données collectées à l'occasion des requêtes.

Le 4 avril 2008, le G29 a en effet publié **un avis sur les moteurs de recherche**, affirmant l'applicabilité de la loi communautaire sur la protection des données, recommandant **une durée de conservation des données de six mois maximum** et indiquant que les internautes devaient consentir à l'exploitation de leurs données à des fins, notamment, de profilage.

Le G29 s'est appuyé sur le fait que les moteurs de recherche, pour établir des profils d'utilisateurs détaillés, utilisent des « *cookies* » (cf. *infra*) qui doivent être considérés comme des moyens de traitement des données à caractère personnel, au sens de la directive, ce qu'ont contesté certains moteurs de recherche.

Une solution pour résoudre ces difficultés d'interprétation pourrait être de réviser la directive de 1995 pour y inscrire expressément la notion de « cookies ». Toutefois, une telle initiative présenterait l'inconvénient majeur de mettre à mal la **neutralité technologique** de la directive, – neutralité que vos rapporteurs ont déjà eu l'occasion de saluer comme un gage de souplesse et de pérennité.

La question de savoir quel est le droit applicable se pose aujourd'hui avec d'autant plus d'acuité que la globalisation économique se traduit par **une intensification des flux transfrontaliers de données personnelles** et que les systèmes juridiques européen et américain se caractérisent par des différences d'approche en matière de protection des données personnelles.

b) Les différences d'approches entre les systèmes européen et américain en matière de protection des données personnelles

Lors d'un colloque organisé par la CNIL et l'université Panthéon-Assas-Paris II au Sénat les 7 et 8 novembre 2005, M. Robert Gellman, avocat auprès de la Cour suprême de Pennsylvanie et expert-conseil en protection des données, soulignait que la méthode américaine de régulation de la protection des données personnelles était éloignée de l'approche européenne, qui repose

---

[1] *« Sauf si ces moyens ne sont utilisés qu'à des fins de transit », précise la directive.*
[2] *Dans le cas contraire, le droit du pays où est établie l'entreprise est applicable.*

sur **des normes complètes de protection** et sur **l'existence d'une autorité indépendante de protection des données**[1].

Au cours de leurs auditions, vos rapporteurs ont pu en effet constater les points suivants :

- **les Etats-Unis ne disposent pas d'une autorité indépendante dédiée à la protection des données**. La Commission fédérale du commerce américaine (*Federal Trade Commission*) est en effet une agence fédérale non indépendante et dont les compétences vont bien au-delà de la protection de la vie privée (lutte contre les monopoles, la concurrence déloyale et la publicité mensongère, protection des consommateurs, répression des fraudes, etc.) ;

- à la différence du système européen, les Etats-Unis n'ont pas de cadre général de protection des données dans le secteur privé mais **des lois sectorielles**. A titre d'exemple, le « *Fair Credit Reporting Act* »[2], première loi fédérale de protection des données personnelles, voté en 1970, vise à encadrer les fichiers relatifs à la situation financière des individus compte tenu de leur importance pour l'accès au crédit, à un emploi ou à une assurance. De même, le « *Children's Online Privacy Protection Act* »[3], voté en 1998, fixe des règles régissant la collecte, l'enregistrement, l'usage et la diffusion des données personnelles obtenues en ligne d'enfants de moins de treize ans ; il prévoit en particulier le consentement des parents avant toute collecte. Enfin, dans le domaine de la santé, le régime de protection est complexe et fragmenté : certaines lois concernent les informations détenues par des agences fédérales, des employés de l'administration ou des élèves, d'autres protections s'appliquent à certaines maladies, telles que le SIDA. Une première étape dans la volonté d'élaborer une législation globale dans ce domaine a été marquée par la loi dénommée « *Health Insurance Portability and Accountability Act* »[4] votée en 1996 et pleinement applicable depuis avril 2003[5].

A contrario, **de nombreux fichiers utilisés dans les transactions commerciales courantes ne font l'objet d'aucune législation de protection des données personnelles.** Des commerçants de tous types, éditeurs de magazines, restaurants, agences de voyage, organismes caritatifs, etc., sont libres de collecter, d'utiliser ou de diffuser des informations personnelles qu'ils obtiennent des individus **sans aucune règle spécifique** fixée par la loi, même si les représentants de la chambre de commerce américaine, entendus par vos rapporteurs, ont objecté que les principes généraux du droit de la consommation, au premier rang desquels figure le **principe de loyauté**, pouvaient toujours trouver à s'appliquer ;

---

[1] Les actes du colloque sont disponibles sur Internet : http://www.senat.fr/colloques/colloque_cnil_senat/colloque_cnil_senat_mono.html.
[2] Loi sur l'évaluation du crédit discriminatoire.
[3] Loi portant protection de la vie privée des enfants sur Internet.
[4] Loi sur la transférabilité des régimes d'assurance-santé.
[5] Il semble, d'une manière générale, que les Etats-Unis tendent progressivement à privilégier une approche globale de protection des données, jugée plus simple que le système sectoriel.

- les Etats-Unis privilégient la régulation du marché à l'intervention de l'Etat, **régulation volontaire** par l'élaboration par les entreprises de leurs propres « *privacy policies* » (c'est-à-dire de codes de bonne conduite internes à l'entreprise), ou **régulation contractuelle** par le biais, par exemple, de conventions entre les opérateurs économiques et les consommateurs ;

- enfin, la philosophie américaine est beaucoup plus fondée qu'en Europe sur **la libre circulation de l'information** (« *free flow of information* ») garante du développement du commerce et de l'économie, ce qui a récemment fait dire à M. Alex Türk, président de la CNIL : « *il y a un fossé abyssal aujourd'hui entre la conception américaine des données personnelles qui sont pour eux des biens marchands et la conception européenne où il s'agit d'attributs de nos personnalités* ».

2. La protection des données à l'épreuve d'Internet

Quasiment inconnu lors de l'adoption de la loi « informatique et libertés » du 6 janvier 1978, d'utilisation encore confidentielle lors du vote de la directive 95/46/CE du 24 octobre 1995, Internet fait désormais partie de la vie quotidienne d'une majorité de nos concitoyens.

D'après l'étude réalisée et mise à jour en juin 2008 par le service des études et des statistiques industrielles du ministère de l'économie, des finances et de l'emploi[1], la proportion de ménages connectés à l'Internet à domicile a plus que doublé depuis 2001. Près de 60 % des Français disposent désormais d'une connexion à domicile ou sur leur lieu de travail ou d'études, et de plus en plus d'entre eux utilisent une connexion à haut débit[2] leur permettant de télécharger des fichiers audio et vidéo, voire d'avoir accès à la téléphonie et à la télévision par le biais d'Internet. De fortes disparités persistent néanmoins en fonction de l'âge, du diplôme, de la profession et du milieu social : **la « fracture numérique » demeure une réalité dans notre pays**.

Cette tendance se retrouve largement au niveau mondial : le nombre d'internautes dans le monde aurait ainsi atteint 1,3 milliard à la fin de l'année 2007, soit près de 20 % de la population mondiale[3].

Largement entré dans le fonctionnement ordinaire des entreprises et des administrations comme dans la vie quotidienne de nos concitoyens, Internet offre **des possibilités extrêmement riches d'échanges et de partages**, selon un fonctionnement largement décentralisé qui fait fi des frontières.

Néanmoins, vos rapporteurs ont également pris conscience des menaces que pourrait faire peser sur les libertés, et en particulier sur le droit au respect de la vie privée, une utilisation totalement dérégulée d'Internet. En

---

[1] *Disponible à l'adresse suivante : www.industrie.gouv.fr/sessi.*
[2] *Fin mars 2008, la France comptait 16,2 millions d'abonnements à l'Internet à haut débit.*
[3] *Chiffres Union internationale des télécommunications (UIT) et Cnuced.*

effet, **par le nombre potentiellement illimité de données qui sont collectées, enregistrées et mémorisées à chaque instant de la navigation**, Internet offre également des possibilités sans précédent de profilage, de traçage et *in fine* de contrôle sur l'ensemble des individus qui l'utilisent, et ce d'autant plus qu'il tend à rassembler en un réseau unique l'ensemble des technologies cloisonnées de télécommunications qui coexistaient jusqu'à présent (un réseau téléphonique, des satellites pour la télévision, un réseau « télex », des réseaux hertziens, etc.).

Ainsi, Internet présente, au regard de la protection des données, une spécificité fondamentale : **alors que dans le monde réel, l'anonymat est la règle et le traçage l'exception, sur Internet, tous les actes de la navigation sont, par nature, enregistrés et mémorisés.** L'enjeu, pour les Etats, consiste donc à **réguler l'usage d'Internet** afin d'y garantir, dans des conditions similaires à celles prévalant dans le « monde réel », le respect du droit à la vie privée, en vertu du **principe de neutralité technologique**.

a) Rester anonyme sur Internet : la délicate conciliation de principes parfois contradictoires

(1) L'anonymisation et l'effacement des données de connexion : principe et exceptions

De la même façon que, dans le monde réel, les individus doivent pouvoir se déplacer, s'exprimer et vivre en toute tranquillité, les internautes doivent pouvoir utiliser Internet sans que la moindre de leurs actions soit enregistrée, analysée et mémorisée. Telle est la raison pour laquelle, en France, le droit général applicable à la navigation et à la communication sur Internet repose sur **un principe général d'anonymisation et d'effacement des données de connexion**, posé à l'article L. 34-1 du code des postes et des communications électroniques (CPCE)[1].

Deux exceptions sont néanmoins apportées à ce principe général :

- D'une part, l'article L. 34-1 du même code reconnaît aux opérateurs le droit d'utiliser et de conserver un certain nombre de données techniques nécessaires à la facturation et au paiement des prestations de communications électroniques, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement. Cette finalité tend néanmoins à perdre de son utilité avec le développement des offres d'accès illimité à Internet.

- D'autre part, **pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre la mise à disposition de l'autorité judiciaire d'informations,**

[1] *L'article L. 34-1 du code des postes et des communications électroniques dispose, dans son paragraphe I, que les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, sont tenues d'effacer ou de rendre anonyme toute donnée relative au trafic.*

il peut être différé, **pour une durée maximale d'un an**, aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques.

Le champ d'application de cette disposition, introduite par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, a été étendu par la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme à l'ensemble des personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, ce qui inclut notamment les cybercafés. Une dérogation a également été introduite au principe selon lequel ces données ne peuvent être communiquées qu'à l'autorité judiciaire (voir *supra*).

Ainsi, sous réserve de quelques exceptions, liées notamment à notre législation anti-terroriste, **le traçage d'un internaute sur Internet ne peut être réalisé que *via* le recours à l'autorité judiciaire, et ce uniquement pour des motifs limitativement énumérés et sur une période n'excédant pas un an.**

Néanmoins, quelle que soit la finalité retenue, les données conservées et traitées ne peuvent porter que sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. **Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées,** sous quelque forme que ce soit, dans le cadre de ces communications.

(2) La position du Conseil constitutionnel et de la CJCE

Le cadre juridique ainsi défini a d'emblée fait l'objet de **contestations**, émanant en particulier de la société des auteurs, compositeurs et éditeurs de musique (SACEM) et du syndicat national de l'édition phonographique (SNEP), qui l'ont considéré comme **insuffisamment protecteur du droit de la propriété intellectuelle**. Ces deux organisations ont ainsi souligné la nécessité, dans le cadre de leurs actions de lutte contre le piratage sur Internet, de disposer de moyens efficaces pour repérer les transmissions illicites diffusées sur le réseau et connaître l'ampleur du trafic et de la fréquentation des sites offrant des œuvres protégées dans des conditions illicites.

Face à ces contestations, la loi n° 2004-801 du 6 août 2004 modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a élargi la liste des personnes autorisées, en application de l'article 9 de cette loi, à mettre en œuvre des « *traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté* ». Cette possibilité est désormais ouverte, en l'état actuel du droit, sous réserve de l'autorisation de la CNIL et aux seules fins d'assurer la défense des droits de leurs adhérents, aux sociétés de perception et de gestion des droits d'auteur et des droits voisins ainsi qu'aux organismes de défense professionnelle.

Dans sa **décision n° 2004-499 DC du 29 juillet 2004**, le Conseil constitutionnel a validé, avec des réserves d'interprétation, cette disposition, en considérant que :

- cette disposition tend à « *lutter contre les nouvelles pratiques de contrefaçon qui se développent sur le réseau Internet* » *et répond ainsi à « l'objectif d'intérêt général qui s'attache à la sauvegarde de la propriété intellectuelle et de la création culturelle* » ;

- néanmoins, « ***les données ainsi recueillies ne pourront****, en vertu de l'article L. 34-1 du code des postes et des communications électroniques,* ***acquérir un caractère nominatif que dans le cadre d'une procédure judiciaire et par rapprochement avec des informations dont la durée de conservation est limitée à un an*** » ;

- en application des dispositions de la loi du 6 janvier 1978, « *la création des traitements en cause est subordonnée à l'autorisation de la CNIL* » ;

- « *compte tenu de l'ensemble de ces garanties et eu égard à l'objectif poursuivi,* ***la disposition contestée est de nature à assurer, entre le respect de la vie privée et les autres droits et libertés, une conciliation qui n'est pas manifestement déséquilibrée*** ».

La Cour de justice des communautés européennes a fait valoir une position similaire lorsque elle a été appelée à se prononcer sur la possibilité, pour une association de gestion de droits d'auteur, d'obtenir la communication auprès d'un fournisseur d'accès à Internet, de données personnelles d'abonnés dans le cadre d'une procédure civile.

Dans sa **décision *Productores de Musica de España (Promusicae)* du 29 janvier 2008**, la Cour a ainsi souligné le fait que « *la présente demande de décision préjudicielle [soulevait]* ***la question de la conciliation nécessaire des exigences liées à la protection de différents droits fondamentaux, à savoir, d'une part, le droit au respect de la vie privée, et, d'autre part, les droits à la protection de la propriété et à un recours effectif*** ».

En l'espèce, la Cour a jugé que le droit communautaire n'imposait pas aux Etats-membres de prévoir l'obligation de communiquer des données à caractère personnel en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile. Elle a néanmoins considéré que la directive « vie privée et communications électroniques » n° 2002/58 du 12 juillet 2002 **ouvrait la possibilité aux Etats-membres de prévoir des exceptions à l'obligation de garantir la confidentialité des données à caractère personnel**, la protection du droit de propriété et les situations dans lesquelles les auteurs cherchent à obtenir cette protection dans le cadre d'une procédure civile pouvant entrer dans le cadre de ces exceptions.

Le projet de loi favorisant la diffusion et la protection de la création sur Internet adopté les 12 et 13 mai 2009 par le Parlement s'inscrit dans le prolongement de ces jurisprudences. Le champ de l'article L. 34-1 du code des

postes et des communications électroniques serait étendu au « manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle[1] » et les données de connexion pourraient être communiquées à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet. Cette Haute Autorité, dotée du statut d'autorité administrative indépendante, disposerait de garanties d'impartialité et d'indépendance, et les titulaires des droits n'auraient pas accès aux données personnelles des internautes[2]. Ce texte est actuellement en cours d'examen par le Conseil constitutionnel.

(3) Le débat sur le statut de l'adresse IP

Les débats qui accompagnent la conciliation du droit à la vie privée et des autres droits fondamentaux dans le cadre de l'utilisation d'Internet ont donné lieu à **une controverse sur le statut juridique de l'adresse IP**.

Qu'est-ce qu'une adresse IP ?

Sur Internet, les ordinateurs communiquent entre eux grâce au Protocole IP (*Internet Protocol*), qui utilise **des adresses numériques**, appelées adresses IP. Ces adresses sont composées de quatre nombres entiers compris chacun entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Chaque ordinateur relié à un réseau dispose d'une adresse IP unique, ce qui lui permet de communiquer avec les autres ordinateurs du même réseau. De même, chaque site Internet dispose d'une adresse IP, qui peut être convertie en nom de domaine. L'attribution des adresses IP publiques relève de l'ICANN (*Internet Corporation for Assigned Names and Numbers*).

Concrètement, chaque transmission de données sur le *web* donne lieu à l'envoi d'un « paquet de données » comprenant, quel que soit le type de communication (navigation sur le web, messagerie, téléphonie par Internet, etc.) l'adresse IP de l'expéditeur ainsi que celle du destinataire. Ainsi, lorsqu'un internaute consulte un site Internet, le serveur de ce dernier enregistre dans un fichier la date, l'heure et l'adresse IP de l'ordinateur à partir duquel la consultation a été effectuée, ainsi que les fichiers qui ont pu être envoyés. Le propriétaire du site a ainsi accès aux adresses IP des ordinateurs qui se sont connectés à son site. Dans le cas particulier des logiciels de « peer-to-peer » (logiciels permettant le partage de fichiers entre internautes), des tiers peuvent également récupérer assez facilement les adresses IP des internautes se livrant à la mise en ligne de fichiers piratés.

En soi, et contrairement à un numéro de téléphone par exemple, **l'adresse IP ne permet pas, la plupart du temps, d'identifier directement l'internaute.** En effet, à la différence des entreprises ou des grandes

---

[1] Article nouveau, créé par la loi, aux termes duquel la personne titulaire de l'accès à des services de communication au public en ligne aurait l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'oeuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.

[2] Rapport n° 53 (2008-2009) de M. Michel Thiollière, fait au nom de la commission des affaires culturelles, déposé le 22 octobre 2008, page 45.

institutions (type universités) qui disposent en général d'une adresse IP fixe, les particuliers se voient en général attribuer, par leur fournisseur d'accès, une adresse IP différente à chaque connexion. Aussi, **seul le fournisseur d'accès sera capable de relier une adresse IP à une personne physique, et à condition de disposer également de l'heure et de la date de connexion**[1].

Cette particularité de la distribution aléatoire des adresses IP par les fournisseurs d'accès à Internet a conduit la treizième chambre de la cour d'appel de Paris à considérer que l'adresse IP ne pouvait pas être considérée comme une donnée personnelle :

- dans un premier arrêt en date du 15 mai 2007, les juges ont considéré que « *cette série de chiffres [ne constituait] en rien une donnée indirectement nominative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon* » ;

- puis, dans un arrêt daté du 27 avril 2007, la cour a estimé que « *l'adresse IP ne [permettait] pas d'identifier le ou les personnes qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur d'accès l'identité de l'utilisateur* ».

Ces deux décisions ont donné lieu à un certain nombre de critiques fortes. En effet, considérer que l'adresse IP ne constitue pas une donnée personnelle aboutirait à exclure du champ d'application de la loi informatique et libertés du 6 janvier 1978 modifiée et du contrôle de la CNIL l'ensemble des traitements réalisés à partir de la collecte d'adresses IP.

Ces deux décisions ont suscité la réaction du G29, qui, dans un avis du 20 juin 2007, a rappelé qu'il considérait que l'adresse IP attribuée à un internaute lors de ses communications devait être regardée comme une donnée à caractère personnel.

Cette dernière position a été suivie par la CJCE lorsque celle-ci a été appelée à se prononcer sur une affaire relative à la lutte contre le piratage (arrêt *Promusicae* du 29 janvier 2008 précité)[2].

Cette solution a enfin été confirmée à l'occasion de la révision de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications

---

[1] *Tout cela sous réserve que l'adresse IP n'ait pas fait l'objet d'une usurpation de la part d'internautes malveillants, ce que permettent malheureusement à l'heure actuelle certains logiciels.*

[2] *Dans cette décision, la Cour a estimé que « la communication, sollicitée par Promusicae, des noms et des adresses de certains utilisateurs de KaZaA implique la mise à disposition de données à caractère personnel, c'est-à-dire d'informations sur des personnes physiques identifiées ou indentifiables, conformément à la définition figurant à l'article 2, sous a), de la directive 95/46 ».*

électroniques : **la directive 2006/24/CE[1] dispose désormais dans son article 2 que les données à caractère personnel incluent les données relatives au trafic et les données de localisation ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur**, ce qui inclut donc l'adresse IP.

En France, néanmoins, la question demeure confuse. Dans une décision rendue le 13 janvier 2009, la Chambre criminelle de la Cour de cassation a considéré que, lorsque la collecte des adresses IP s'effectue « à la main », et non au moyen d'un traitement informatique automatisé, l'autorisation de la CNIL n'est pas requise. Ce faisant, **la Chambre criminelle n'a pas tranché le débat relatif au statut de l'adresse IP,** ce qui semble particulièrement regrettable au regard du flou juridique qui subsiste sur cette question.

b) L'inflation de pratiques commerciales « anonymement intrusives »

L'attention de vos rapporteurs a par ailleurs été attirée sur les innombrables opportunités qu'offre Internet aux sociétés privées, régies publicitaires et moteurs de recherche en termes de profilage des internautes, à des fins commerciales. Cet aspect du traçage sur Internet doit être distingué de celui précédemment examiné en ce que, **dans la grande majorité des cas, ce traçage demeure anonyme** : le comportement de l'internaute sur Internet importe davantage que les informations relatives à son identité réelle. Il n'en demeure pas moins que **de telles pratiques de profilage, réalisées le plus souvent à l'insu des internautes, peuvent aboutir à la collecte d'informations nombreuses et être ressenties, à juste titre, comme véritablement intrusives.**

(1) Le profilage sur Internet

Comme le montre une étude réalisée récemment par la CNIL[2], il y a lieu de distinguer trois types de publicité ciblée sur Internet :

- **La publicité personnalisée « classique »** a pour but de cibler la publicité proposée à un internaute en fonction d'informations (âge, sexe, localisation, etc.) qu'il a lui-même renseignées. Ce type de publicité est aujourd'hui également utilisé par les réseaux sociaux en fonction des informations (qui peuvent être particulièrement nombreuses) fournies par leurs utilisateurs dans leurs « profils » (voir *infra*).

- **La publicité contextuelle** est une publicité qui est choisie en fonction du contenu immédiat consulté ou sollicité par l'internaute (contenu contextuel de la page consultée, relation avec le ou les mots-clés saisi(s) sur un moteur de recherche, etc.), cette information étant parfois complétée par

---

[1] Relative à la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE.

[2] « La publicité ciblée en ligne », communication présentée par M. Bernard Peyrat, rapporteur, en séance plénière le 5 février 2009, disponible sur le site Internet de la CNIL.

des informations de géolocalisation déduites de l'adresse IP de l'internaute (pays ou région d'origine, langue utilisée) ou, dans le cas d'un moteur de recherche, par la précédente requête formulée par l'internaute.

▪ Enfin, **la publicité comportementale** est probablement la forme de profilage la plus élaborée, en ce qu'elle vise à observer le comportement de l'internaute à travers le temps, en établissant un profil de ce dernier en fonction des différents sites consultés, des mots-clés saisis et des contenus produits, et à lui proposer des publicités adaptées à ce profil. Parmi les différentes techniques permettant de constituer de tels profils, la plus connue et la plus employée est celle des « *cookies* ».

Que sont les « cookies » ?

Les « *cookies* » sont de petits fichiers d'une centaine d'octets que le navigateur utilisé par l'internaute (Internet Explorer, Opéra, etc.) installe sur le disque dur de ce dernier à la demande du site consulté. Créés en 1994 par des ingénieurs de Netscape, les « *cookies* » sont également appelés « mouchards électroniques » ou « témoins de connexion ». Leur objet est de **permettre au site qui les a envoyés de « reconnaître » l'internaute en stockant un certain nombre d'informations** : adresse IP, système d'exploitation et navigateur utilisés, pages consultées, nombre de visites du site, etc. En cela, les cookies **permettent de faciliter la navigation**, en mémorisant un certain nombre d'informations que l'internaute n'aura pas à ressaisir ultérieurement (par exemple, un cookie permettra à un internaute faisant ses achats en ligne de conserver en mémoire les produits placés dans le panier virtuel et de les présenter sur la facture finale). Toutefois, les cookies permettent également au fournisseur de contenu ou à la régie publicitaire de **conserver en mémoire un grand nombre d'informations relatives aux habitudes de navigation de l'internaute**, et ce même si ce dernier possède une adresse IP dynamique et variable (cf. *supra*), leur offrant ainsi la possibilité de lui proposer des publicités conformes à ses préférences (telles qu'elles auront été déduites des informations collectées).

(2) Des stratégies indissociables du modèle économique d'Internet

La publicité sur Internet représente un secteur en pleine expansion : selon une étude réalisée par le cabinet Precepta et rendue publique en avril 2009, le secteur de la publicité en ligne a généré 2,5 milliards d'euros de revenus en 2008, ce qui représente une augmentation de + 6,5 % sur un an. L'étude prévoit une croissance annuelle de ses revenus de 7 à 10 % d'ici à 2014, avant un ralentissement probable à partir de 2015, du fait de la baisse attendue des prix causée par la multiplication des espaces disponibles sur Internet et au comportement considéré comme « agressif » des régies publicitaires.

Une telle croissance n'est que **la contrepartie du modèle économique sur lequel fonctionne un certain nombre de sociétés de l'Internet**, celles qui offrent aux internautes des services dits « gratuits », financés en réalité de façon majoritaire par la publicité ciblée.

Par exemple, le service de messagerie électronique (gratuit) Gmail, fourni par Google, est financé par les publicités affichées en fonction du

repérage d'un certain nombre de mots-clés figurant dans le contenu des correspondances échangées. Il en est de même de l'ensemble des moteurs de recherche dits « gratuits ».

Ces sociétés se défendent de participer à l'instauration d'une société de surveillance dans la mesure où, font-ils valoir, la collecte de ces informations demeure anonyme : le but n'est pas d'épier les comportements d'utilisateurs identifiés mais de parvenir à une « personnalisation » des services proposés, au double bénéfice de l'internaute et de l'annonceur publicitaire.

Vos rapporteurs sont conscients du confort que peut représenter pour certains internautes une telle personnalisation des services proposés. Encore faut-il que ces derniers aient été pleinement informés des outils de profilage utilisés à leur encontre et qu'ils aient eu le moyen de s'opposer à ce que les données relatives à leur navigation fassent ainsi l'objet d'une collecte. Or, comme le montre la CNIL dans son étude précitée, « ***en l'absence de transparence de la part des fournisseurs de contenu ou de services sur les mécanismes de profilage et sur les données collectées, l'internaute peut percevoir ces mécanismes comme très intrusifs*** »[1].

Le G29 l'a également relevé dans son avis du 20 juin 2007 relatif au concept de données à caractère personnel : « *Sur l'Internet aussi, les outils de surveillance du trafic permettent de cerner facilement le comportement d'une machine, et, derrière celle-ci, de son utilisateur. On reconstitue ainsi la personnalité de l'individu pour lui attribuer certaines décisions. Sans même s'enquérir du nom et de l'adresse de la personne, on peut la caractériser en fonction de critères socio-économiques, psychologiques, philosophiques ou autres et lui attribuer certaines décisions, dans la mesure où le point de contact de la personne (l'ordinateur) ne nécessite plus nécessairement la révélation de son identité au sens étroit du terme. En d'autres termes,* ***la possibilité d'identifier une personne n'implique plus nécessairement la faculté de connaître son identité*** »[2].

Pour illustrer la possibilité d'identifier relativement aisément des utilisateurs à partir de données pourtant théoriquement anonymes, on peut citer « l'affaire AOL » : au cours de l'été 2006, ce prestataire de services a publié un échantillon des requêtes, accompagnées des liens cliqués pour chacune d'entre elles, effectuées par 650.000 utilisateurs sur une période de trois mois. AOL avait certes remplacé les noms des utilisateurs par des numéros.

Néanmoins, des journalistes ont rapidement découvert que ces résultats permettaient souvent de remonter aux différents utilisateurs, en

---

[1] *Op. cit., page 22.*

[2] *G29, avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, page 15.*

partant des « *recherches de vanité* » (les utilisateurs recherchent souvent des informations sur eux-mêmes) et des combinaisons de requêtes effectuées par un seul utilisateur[1].

(3) Le cas particulier des moteurs de recherche

Ce dernier exemple illustre par ailleurs les difficultés spécifiques soulevées par les moteurs de recherche en matière de droit au respect de la vie privée. Les moteurs de recherche constituent en effet un cas tout à fait particulier, du fait de leur **double fonction de prestataires de services et de fournisseurs de contenus**.

Les moteurs de recherche sont des services qui permettent aux internautes de trouver facilement des informations sur Internet. Leur fonctionnement est basé sur le traitement et la mise en ordre d'informations à partir de l'exploration et de l'indexation systématique des sites accessibles sur le *net*. Services « gratuits » dans l'immense majorité des cas, leur rentabilité dépend avant tout de l'efficacité de la publicité qui accompagne les résultats des recherches effectuées.

Comme l'explique clairement l'avis du G29 consacré aux aspects de la protection des données liés aux moteurs de recherche[2], « ***d'une part, en tant que prestataires de services aux utilisateurs, les moteurs de recherche collectent et traitent de grandes quantités de données d'utilisateur****, dont celles recueillies par des moyens techniques, tels que les « cookies ». Les données collectées peuvent aller de l'adresse IP des différents utilisateurs, ou d'historiques de recherche complets, ou encore de données fournies par les utilisateurs eux-mêmes lorsqu'ils s'inscrivent en vue d'utiliser des services personnalisés. […]* ***D'autre part, en tant que fournisseurs de contenus, les moteurs de recherche contribuent à rendre les publications sur Internet facilement accessibles aux quatre coins de la planète.*** *Certains moteurs de recherche republient des données dans ce que l'on appelle une « mémoire cache ». Or, en recherchant et en regroupant des informations courantes de divers types au sujet d'une personne, ils peuvent créer un nouveau profil, avec un risque beaucoup plus grand pour la personne concernée que si toutes les données publiées sur Internet restaient séparées les unes des autres.* ***Les capacités de représentation et d'agrégation des moteurs de recherche peuvent nuire considérablement aux individus, tant dans leur vie personnelle qu'au sein de la société, en particulier si les données à caractère personnel qui figurent dans les résultats de recherche sont inexactes, incomplètes ou excessives*** ».

---

[1] *A titre d'illustration, des journalistes du New York Times sont par exemple parvenus à identifier l'utilisateur « 4417749 », une veuve de 62 ans, grâce à la liste de ses requêtes (liées aux taxes locales en vigueur dans sa ville, à ses trois chiens, à sa santé, à son sentiment de solitude, etc.) ; le Guardian est parvenu de son côté à décrire la vie d'un homme, habitant d'une ville de Floride, fan de football portugais, qui apprend que sa femme a une relation extraconjugale et qui se met à boire avant de faire appel aux services d'un medium ; etc.*

[2] *G29, avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, adopté le 4 avril 2008.*

Les moteurs de recherche, considérés dans leurs fonctions de prestataires de services, ont récemment fait l'objet de l'attention soutenue du G29.

En effet, il est apparu que ces derniers conservaient un très grand nombre de données relatives à leurs utilisateurs[1] pendant des périodes excédant parfois une année (la durée de conservation varie en fonction des sociétés), les moteurs de recherche faisant valoir que la conservation de ces données est nécessaire à la qualité du service rendu, à la prévention des fraudes et à la sécurisation du système, ainsi qu'à des fins comptables et statistiques.

Dans son avis précité, le G29 n'a pas contesté les finalités ainsi mises en avant, mais il a dénoncé la durée, selon lui excessive, au cours de laquelle l'ensemble des données relatives aux utilisateurs étaient conservées. Le débat s'est ainsi recentré sur **la question des délais de conservation des données personnelles par les moteurs de recherche** (cf. *supra*).

L'activité des moteurs de recherche en tant que fournisseurs de contenus soulève davantage de difficultés. En effet, **en tant qu'intermédiaires** (les moteurs de recherche ne font que fournir à l'utilisateur les liens vers des informations que celui-ci recherche et qui sont publiées sur un certain nombre de sites *web*), **ils ne peuvent juridiquement être considérés comme les principaux responsables du traitement des données à caractère personnel effectué** : dans le cas de la publication d'une information concernant un internaute sur un site Internet, ce dernier doit se retourner vers le gestionnaire de ce site pour faire valoir ses droits d'accès, de rectification et d'opposition[2]. Tout au plus l'internaute peut-il solliciter la désindexation des sites contenant des informations lui portant tort[3]. Néanmoins, en l'absence de la coopération et de la bonne volonté du gestionnaire d'un site comportant des informations personnelles qu'une personne souhaiterait voir effacées, voire même de la capacité d'identifier ce gestionnaire (cette question se pose avec d'autant plus d'actualité si celui-ci est implanté en dehors du territoire européen et ne s'estime pas lié par la réglementation communautaire), **l'internaute peut se trouver dans l'incapacité de faire rectifier ou supprimer des informations lui portant**

---

[1] Par exemple, Google conserve systématiquement les données suivantes : termes de la requête, adresse consultée, adresse IP de l'internaute, heure et date de la recherche, système d'exploitation, type de navigateur, identifiant de cookie.

[2] Les exceptions sont l'existence d'une mémoire cache à long terme et les opérations à valeur ajoutée effectuées sur les données à caractère personnel, telles que les moteurs de recherche destinés à établir des profils de personnes physiques. Lorsqu'ils fournissent ce type de services, le G29 considère que les moteurs de recherche doivent être tenus pour entièrement responsables au regard des obligations que leur impose la directive 95/46/CE, et qu'ils doivent en respecter l'ensemble des dispositions.

[3] Ainsi, dans certains Etats membres de l'Union européenne, les autorités de protection des données ont spécifiquement réglementé l'obligation des fournisseurs de moteurs de recherche de retirer des données de contenu de l'index de recherche, sur la base du droit d'opposition consacré à l'article 14 de la directive 95/46/CE sur la protection des données et de la directive 2000/31/CE sur le commerce électronique.

tort et aisément disponibles *via* les moteurs de recherche. Cette difficulté a été évoquée par nombre des interlocuteurs rencontrés par vos rapporteurs, qui se sont interrogés **sur l'opportunité de consacrer un « droit à l'oubli »** (voir *infra*).

Faire supprimer une page web contenant des informations personnelles
(extrait du rapport d'activité de la CNIL pour 2007)

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

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

c) De la difficulté pour les internautes à faire valoir leurs droits

Internet offre ainsi des possibilités sans précédent de profilage et de traçage de ses utilisateurs, alors qu'à l'inverse, un certain nombre de contraintes techniques limitent en pratique la capacité des internautes à faire valoir leurs droits (information préalable, droits d'accès, de rectification et d'opposition) dans cet espace virtuel.

Prenons l'exemple des cookies. En théorie, et conformément aux dispositions de la loi informatique et libertés, l'internaute a la maîtrise de l'installation des cookies sur son ordinateur. Il dispose ainsi du droit d'être informé de l'installation sur son disque dur de ces témoins de connexion, et de celui de s'y opposer[1].

---

[1] *L'article 32 II de la loi dispose en effet que « toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :*
« - de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;
« - des moyens dont elle dispose pour s'y opposer. »

Dans la pratique, néanmoins, cette maîtrise se révèle le plus souvent illusoire. Comme le montre l'étude précitée réalisée par la CNIL :

- « *Si l'internaute bloque tous les cookies, il ne peut pratiquement utiliser aucun service aujourd'hui sur Internet.*
- *« Si l'internaute choisit d'autoriser individuellement chaque cookie au cas par cas, il se retrouve avec un nombre incessant de messages de confirmation qui deviennent vite pénalisants pour la navigation.*
- *« Enfin, l'alternative consistant à réaliser une suppression manuelle des cookies à chaque fin de session est également peu pratique.*

« Aujourd'hui, ces contraintes font ***qu'en réalité, la plupart des internautes n'optent pas pour une politique réelle de contrôle des cookies*** »[1].

En outre, la plupart du temps, les navigateurs sont configurés par défaut pour accepter les cookies. Qui plus est, la plupart des internautes ne sont le plus souvent pas conscients de la masse de données les concernant qui sont collectées à chaque instant de la navigation. En l'absence d'une information préalable claire et complète, ils se retrouvent *de facto* dans l'incapacité de prendre des décisions éclairées à ce sujet.

Prenons également l'exemple des réseaux sociaux : **alors qu'en théorie, l'ensemble du dispositif de la loi « informatique et libertés » trouve à s'appliquer, l'exercice par les individus de l'ensemble des droits que leur reconnaît la loi s'avère en pratique totalement illusoire.** Comment, par exemple, envisager qu'un individu fasse valoir ses droits d'autorisation préalable, de rectification et d'opposition concernant des données le concernant qu'aurait rendues publiques, *via* un réseau social, un ami, un collègue ou un parent ?

En pratique, les solutions proposées par le dispositif de la loi « informatique et libertés » ne sont ainsi que très imparfaitement satisfaisantes.

Un tel constat a convaincu vos rapporteurs, d'une part, de la nécessité de renforcer substantiellement l'information et la sensibilisation des internautes aux traces qu'ils laissent sur Internet (voir *infra*), et, d'autre part, du rôle essentiel joué par les autorités en matière de régulation des pratiques de traçage développées sur Internet.

A cet égard, vos rapporteurs ont pris connaissance avec satisfaction des récentes positions prises par un certain nombre de membres de la Commission européenne en faveur de la protection des données sur Internet. Alors que la commissaire en charge de la protection des consommateurs, Mme Meglena Kuneva, a demandé fin mars 2009 aux sociétés de l'Internet de définir des principes clairs et accessibles en matière de collecte d'informations personnelles à des fins commerciales, Mme Viviane Reding, commissaire

---

[1] *Op. cit., page 24.*

chargée de la société de l'information et des medias, s'est récemment inquiétée du développement des systèmes de publicité comportementale, déclarant notamment que « *nous ne pouvons pas […] avoir tous nos échanges surveillés, compilés et stockés, contre la promesse de publicités plus appropriées* ». Le même jour[1], la Commission européenne engageait une procédure d'infraction à l'encontre du Royaume-Uni, après avoir été informée par des internautes britanniques et des membres du Parlement européen de l'utilisation par des fournisseurs d'accès à Internet britanniques d'une technologie de publicité comportementale dénommée Phorm. Dans cette affaire, la Commission européenne reproche à la législation britannique de ne pas permettre aux autorités de disposer des pouvoirs nécessaires et des sanctions appropriées pour mettre en œuvre la législation communautaire en matière de confidentialité des communications.

Vos rapporteurs, qui ont eu l'opportunité de dialoguer avec un certain nombre de représentants de la Commission européenne à l'occasion de leur déplacement à Bruxelles, espèrent **que le renforcement de la protection des données personnelles continuera à figurer parmi les priorités de la prochaine Commission**, qui sera appelée à entrer en fonctions au second semestre 2009.

III. LES RECOMMANDATIONS DE VOS RAPPORTEURS

Au terme des auditions auxquelles ils ont procédé, vos rapporteurs ont acquis la conviction **qu'il était indispensable de conserver les grands principes fondateurs de la protection des données**, dont l'ensemble de leurs interlocuteurs ont souligné l'adaptabilité et la pertinence.

En revanche, il leur a semblé que trois pistes de réflexion méritaient d'être explorées :

- en premier lieu, il leur semble indispensable d'engager un important travail d'éducation et de sensibilisation de l'ensemble des citoyens, afin que ceux-ci aient la possibilité de se saisir pleinement des enjeux relatifs à la vie privée à l'heure du numérique ;

- en second lieu, il leur a semblé nécessaire de préconiser un renforcement des moyens de la CNIL, afin de lui permettre de faire face à des développements technologiques en progression constante et dans des domaines les plus variés ;

- enfin, un certain nombre de compléments et d'améliorations à la marge leur semblent pouvoir être apportés au dispositif de la loi « informatique et libertés ».

---

[1] *Le 14 avril 2009.*

A. FAIRE DU CITOYEN UN « HOMO NUMERICUS » LIBRE ET ÉCLAIRÉ, PROTECTEUR DE SES PROPRES DONNÉES

1. Renforcer l'éducation et l'information du citoyen

Comme le montre le Professeur Yves Poullet, en matière de nouvelles technologies, nous nous trouvons souvent dans la situation de Joseph K., le héros du *Procès* de F. Kafka, qui se retrouve un jour au centre d'un procès sans savoir qui sont ses accusateurs, quel est l'objet de la plainte ni quelles sont les charges retenues contre lui : l'opacité des systèmes d'information conduit ainsi à **une méfiance générale** des individus, qu'accompagne une tendance générale au **conformisme** et au **mimétisme social**.

Ces analyses se reflètent très largement dans les sondages. Ainsi, un sondage Eurobaromètre réalisé sur un échantillon de jeunes gens âgés de 15 à 24 ans montre que 33 % seulement d'entre eux ont conscience de leurs droits en matière de données à caractère personnel ; 18 % à peine connaissent l'existence des autorités nationales de contrôle de la protection des données, et 20 % seulement jugent sûre la transmission des données à caractère personnel par Internet. Or, en dépit de ce déficit d'information et de la méfiance que celui-ci induit, les jeunes sont aujourd'hui les utilisateurs les plus familiers d'Internet et des nouvelles technologies.

Une telle situation présente des risques pour le respect du droit à la vie privée. Comme le montrent les Professeurs Yves Poullet et Antoinette Rouvroy, prenant appui sur une décision de la Cour constitutionnelle fédérale allemande de 1983, l'opacité des systèmes et l'information déficiente procurée aux citoyens conduit ces derniers à s'imposer des restrictions et à s'autocensurer, par crainte d'adopter des comportements qui seraient considérés comme étranges par des tiers. En l'absence d'une sensibilisation suffisante au fonctionnement des nouvelles technologies, nous sommes conduits, dans le doute, à nous conformer au comportement majoritaire, au détriment de notre liberté à exercer nos propres choix[1].

Au terme des auditions auxquelles ils ont procédé, vos rapporteurs en sont ainsi parvenus à la conclusion que la mise en œuvre de la notion de respect de la vie privée ne peut être assurée sans l'implication pleine et entière des individus et qu'une sensibilisation de ces derniers à l'usage des nouvelles technologies constitue un préalable indispensable à la protection des données personnelles. Ce constat aboutit à préconiser, d'une part, un renforcement substantiel de l'éducation des citoyens, et en particulier des plus jeunes, aux enjeux de protection des données, et, d'autre part, une amélioration des conditions dans lesquelles les individus sont incités à faire valoir leurs droits.

---

[1] *Yves Poullet, Antoinette Rouvroy, Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie, en cours de publication.*

a) L'éducation des citoyens à la protection des données : un enjeu de génération

En matière de nouvelles technologies, les rapports entre générations sont inversés : non seulement, les plus jeunes sont les plus fréquents utilisateurs de nouvelles technologies, mais ce sont souvent eux qui initient leurs parents et grands-parents à l'usage de ces nouveaux outils de communication.

Certes, les parents ont un rôle essentiel en matière d'éducation au comportement de façon générale, et notamment au respect d'autrui. Mais les nouvelles technologies présentent en pratique un certain nombre de spécificités techniques face auxquelles une grande partie de nos compatriotes demeurent démunis.

Dans ces conditions, il a semblé évident à vos rapporteurs que la sensibilisation des plus jeunes à la question de la protection des données personnelles devait être assurée par l'école, car non seulement cette sensibilisation n'est peut-être pas toujours assurée à la maison, mais également car ces jeunes peuvent avoir à leur tour un rôle à jouer en termes d'information et de sensibilisation de leur entourage plus âgé.

(1) Une prise en compte par les programmes scolaires encore insuffisante

Les programmes de l'Education nationale intègrent depuis peu la sensibilisation à la question de la protection des données personnelles, au moyen du **brevet informatique et Internet (B2I)**.

Créé en 2001 et généralisé à l'ensemble de l'enseignement scolaire en 2006, le B2I constitue, depuis la session 2008, un préalable à la délivrance du diplôme national du brevet. Ses objectifs, tels qu'ils sont énoncés dans le Bulletin officiel du ministère de l'Education nationale du 16 novembre 2006, est de « *faire acquérir par chaque élève les compétences lui permettant d'utiliser de façon réfléchie et efficace [les technologies de l'information et de la communication] et de contribuer à former ainsi des citoyens autonomes, responsables, doués d'esprit critique* ».

Parmi les compétences que devront acquérir élèves, collégiens et lycéens figure un domaine n° 2 intitulé « adopter une attitude responsable », lequel intègre notamment une éducation aux règles élémentaires du droit de l'informatique et de l'Internet ainsi qu'une sensibilisation à la notion de respect de la vie privée de soi-même et d'autrui sur Internet.

Néanmoins, les modalités de mise en œuvre de ce B2I présentent un certain nombre de spécificités qui n'ont pas pleinement convaincu vos rapporteurs. En effet, aux termes du B.O. précité, « *tous les enseignants ont vocation à valider les items constitutifs des compétences qui figurent dans les feuilles de position du B2I* » : les compétences exigées du B2I ne font l'objet d'aucune heure d'enseignement spécifique, puisqu'elles ont vocation à être acquises à l'occasion de l'ensemble des enseignements par ailleurs dispensés (histoire-géographie, cours de langue, etc.). En outre, aucune formation

continue des enseignants n'est mise en place (alors que l'ensemble des enseignants ont vocation à faire valider ces compétences), si ce n'est en formation initiale, ce qui semble nettement insuffisant.

Au regard des enjeux que soulève aujourd'hui l'utilisation de plus en plus massive des nouvelles technologies par nos concitoyens, il semble indispensable à vos rapporteurs **qu'une sensibilisation à la question de la protection des données soit intégrée dans l'enseignement dispensé aux enfants comme une question à part entière.** Vos rapporteurs estiment en particulier qu'une telle question pourrait légitimement trouver sa place au sein des programmes d'**éducation civique**.

Recommandation n° 1 : Renforcer la place accordée à la sensibilisation aux questions de protection de la vie privée et des données personnelles dans les programmes scolaires.

(2) Une mobilisation de l'ensemble des acteurs

Vos rapporteurs se félicitent en revanche de l'effort substantiel accompli ces dernières années par les pouvoirs publics pour équiper les établissements scolaires en postes informatiques dotés d'une connexion à Internet. Cette question constitue en effet un préalable indispensable à l'éducation des plus jeunes à l'informatique, et tout particulièrement des plus défavorisés qui ne disposent pas d'un accès à Internet à domicile.

Ainsi, en mars 2009, le ministère de l'Education nationale a officiellement engagé, dans le cadre du « plan de relance », la mise en œuvre d'un programme consacré au développement du numérique dans les écoles rurales. Ce programme, doté d'un budget de 50 millions d'euros, prévoit l'équipement de 5.000 écoles situées dans des communes de moins de 2.000 habitants.

Ce programme associera au plus près les collectivités territoriales, qui jouent déjà un rôle essentiel en matière d'éducation des plus jeunes aux questions de protection des données personnelles.

L'attention de vos rapporteurs a en effet été appelée sur les actions de sensibilisation organisées par un certain nombre d'associations ou de sociétés en partenariat avec les établissements scolaires et les collectivités locales. Par exemple, l'agence Calysto, spécialisée dans l'accompagnement aux usages d'Internet[1], est à l'origine du « Tour de France des collèges et des écoles », une action d'information et de sensibilisation aux enjeux de l'Internet à destination des 9-18 ans, menée en partenariat avec le ministère de l'Education nationale et avec le ministère de la Culture. De son côté, l'association Action Innocence, engagée dans l'éducation des jeunes à l'utilisation responsable d'Internet, a effectué 135 interventions en 2007, à destination de près de

[1] *Cette société privée a signé avec le ministère de l'Education nationale le 13 septembre 2004 une convention de coopération pour l'accompagnement des élèves, des familles et du corps enseignant dans l'utilisation des nouvelles technologies.*

5.000 enfants et adolescents, 1.500 parents d'élèves et plus de 500 professionnels de l'enfance. Google a quant à lui participé au financement du « Tour de France des collèges et des écoles » ainsi qu'à l'élaboration du jeu pédagogique « Cherchenet ».

L'exemple d'une action de sensibilisation menée en partenariat avec le ministère de l'Education nationale : le jeu éducatif « Cherchenet »

Le 24 mars 2009, un jeu-concours baptisé « Cherchenet », destiné aux élèves des classes de 6ème et de 5ème, a été lancé par la société Google et l'agence Calysto, en partenariat avec le ministère de l'Education nationale et l'association La Voix de l'Enfant.

Il s'agit d'un jeu éducatif dont l'objectif est de former les collégiens de manière ludique aux bons usages d'Internet. Les enfants sont invités, à travers la résolution d'énigmes et la création d'un *blog* collectif, à adopter une attitude responsable sur Internet.

Le jeu a en effet pour but de leur permettre d'adopter les compétences suivantes :

- préparer un travail, une recherche sur Internet, en respectant les droits de propriété intellectuelle,

- rechercher efficacement en vérifiant les sources d'information,

- apprendre à protéger sa vie privée et celle des autres sur les réseaux sociaux ou les blogs,

- apprendre à s'appliquer, à rédiger, « même sur Internet » et mettre de côté le « langage SMS ».

Début mai 2009, soit six semaines après son lancement, 877 classes s'étaient portées candidates à ce jeu-concours dont les résultats seront connus au début du mois de juin.

En outre, vos rapporteurs se félicitent de la signature, en janvier 2009, d'une Convention de partenariat entre la CNIL et la Défenseure des enfants destinée à renforcer les actions de sensibilisation à la question de la protection des données sur Internet à destination des jeunes tout autant que de ceux qui en ont la responsabilité (parents, enseignants, éducateurs).

L'ensemble de ces actions s'inscrivent pleinement dans le plan de développement de l'économie numérique appelé « France numérique 2012 » présenté par M. Eric Besson, alors secrétaire d'Etat chargé du développement de l'économie numérique, en octobre 2008. En particulier, l'action n° 80 préconisée par ce plan invite la CNIL à mettre en place une campagne de sensibilisation « informatique et libertés » à destination du grand public, « *et en tout premier lieu des jeunes, pour bien faire comprendre les risques inhérents à la diffusion sur Internet des données sur leur vie privée, par exemple sur les réseaux sociaux, mieux faire connaître les règles de protection des données et ainsi leur permettre de protéger plus efficacement leur vie privée* ».

Vos rapporteurs ne peuvent que saluer et encourager ces initiatives destinées à mieux sensibiliser les enfants et les adolescents aux questions de droit au respect de la vie privée et à la protection des données personnelles.

b) L'information des citoyens, préalable nécessaire à la mise en œuvre du consentement

(1) Une information encore insuffisante

Vos rapporteurs ont été interpellés par la remarque faite par plusieurs des interlocuteurs américains qu'ils ont eu l'occasion de rencontrer dans le cadre de l'élaboration du présent rapport : ceux-ci ont certes convenu que la France disposait d'une législation très complète et protectrice en matière de protection des données, mais ont fait observer que, **dans les faits, il était très difficile aux individus de faire valoir les droits que cette loi leur reconnaît**, faute de disposer d'une information claire et complète sur l'exercice de ces droits. L'exemple le plus souvent cité à vos rapporteurs a été celui des hôtels qui procèdent à l'enregistrement de leurs clients : dans les faits et en règle générale, aucune information n'est donnée à ces derniers concernant la finalité d'une telle collecte, la durée pendant laquelle ces données sont conservées ou encore le nom du responsable de traitement auquel s'adresser pour pouvoir exercer son droit d'accès et de rectification.

Or, l'absence d'une telle information rend particulièrement difficile et coûteuse l'exercice de leurs droits par les citoyens, ce qui crée le risque de priver d'ineffectivité les dispositions de la loi « informatique et libertés ».

L'article 32 de la loi du 6 janvier 1978 modifiée oblige certes le responsable d'un traitement à mettre les personnes concernées par les informations qu'il a collectées et qu'il détient en mesure d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer son identité, la finalité du traitement (par exemple : gestion de clientèle, prospection commerciale, etc.), le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits ainsi que les transmissions envisagées.

Néanmoins, faute pour les citoyens de connaître leurs droits, les formules ainsi imprimées au verso des formulaires tendent à revêtir un caractère incantatoire.

C'est la raison pour laquelle **vos rapporteurs appellent de leurs vœux une grande campagne de sensibilisation destinée à informer les citoyens des droits qui leur sont reconnus par la loi « informatique et libertés »**. En effet, un sondage Eurobaromètre réalisé il y a quelques mois a montré que les deux tiers de nos compatriotes ne connaissaient pas cette loi ni les droits qu'elle reconnaît.

(2) Une implication encore timide de la société civile

Corrélativement, vos rapporteurs ne peuvent qu'encourager les associations de défense des citoyens à investir davantage le champ de la protection de la vie privée et des données à caractère personnel et, au-delà des seuls enjeux relatifs aux fichiers de police et aux bases de données publiques, à se saisir pleinement de l'ensemble de la problématique de la compatibilité entre développement technologique et respect de la vie privée.

A cet égard, vos rapporteurs ont été particulièrement intéressés par les échanges qu'ils ont pu avoir, à l'occasion de leur déplacement à Madrid, avec les membres de **la Comisión de Libertades e Informática (CLI)**, une association indépendante fédérant un grand nombre de structures diverses de la société civile (syndicats, associations d'internautes, etc.) autour des questions relatives à la protection de la vie privée et des droits des citoyens à l'heure du numérique. Il leur est apparu que cette association, indépendante des pouvoirs publics, s'était pleinement engagée sur un certain nombre de terrains pour faire avancer la question de la protection des données en Espagne : recours devant les tribunaux, rédaction de manuels (y compris en langues régionales) destinés à sensibiliser les enfants aux enjeux de la protection des données, prises de position publiques sur un grand nombre de sujets (RFID, dossier médical personnel, etc.), etc. Partant du constat que, selon un sondage qu'ils avaient fait réaliser, 90 % des personnes souhaitaient mieux connaître leurs droits face à la montée en puissance des nouvelles technologies, les membres de la CLI ont plaidé auprès de vos rapporteurs **en faveur d'une sensibilisation de l'ensemble des Européens à ces enjeux, organisée à l'échelle de l'Union européenne.**

(3) Un préalable à la mise en œuvre du consentement

A l'issue des auditions auxquelles ils ont procédé, vos rapporteurs ont acquis la conviction qu'un tel travail de sensibilisation et d'information constituait un préalable indispensable à la mise en œuvre de la notion de consentement, qui figure à de multiples reprises dans le texte de la loi.

Corrélativement, il leur a semblé qu'une telle question dépassait de loin la simple dichotomie « *opt in* » / « *opt out* », qui est fréquemment mise en avant dès que l'on aborde la question de la protection des données. Ces deux modalités de mise en œuvre du consentement présentent en effet chacune des avantages et des inconvénients :

- L' « *opt out* » désigne la possibilité offerte à un citoyen de ne pas participer à une collecte de données personnelles. Il s'agit *a priori* de l'option la moins protectrice de la vie privée, puisque, par défaut, l'individu est supposé consentir à la collecte de ses données.

▪ L' « *opt in* », plus protectrice en termes de respect de la vie privée, désigne la possibilité offerte au citoyen de participer, au cas par cas, à la collecte de ses données. En pratique, la mise en œuvre d'une telle option peut néanmoins s'avérer parfois contraignante.

Il a semblé à vos rapporteurs qu'il n'était pas possible de trancher *a priori* cette question, qui demeure avant tout une affaire d'espèce et de sensibilité de chacun aux données qu'il choisit de divulguer, en fonction des enjeux en présence. Ainsi, en matière de *spam* (courrier publicitaire non sollicité), le principe retenu par l'Union européenne est celui de l' « *opt in* », sauf en ce qui concerne les activités commerciales entre entreprises où l' « *opt out* » est autorisé. A l'inverse, les cookies fonctionnent sur le principe de l' « *opt out* », du fait des inconvénients qu'un système d' « *opt in* » entraînerait pour la navigation sur Internet (cf. *supra*).

Le choix de l'option mérite donc d'être examiné au cas par cas. Encore faut-il que chacun ait pleinement conscience des implications en termes de respect de la vie privée que sous-tend l'utilisation des nouvelles technologies : de ce point de vue, **la question de l'éducation des individus à la maîtrise de leurs propres données constitue aux yeux de vos rapporteurs la condition *sine qua non* de l'effectivité du droit au respect de la vie privée.**

Recommandation n° 2 : Promouvoir l'organisation et le lancement d'une campagne d'information à grande échelle destinée à sensibiliser les citoyens aux enjeux liés à la vie privée et à la protection des données à l'heure du numérique ainsi qu'à les informer des droits que leur reconnaît la loi « informatique et libertés ».

2. Renforcer la confiance du citoyen dans la société du numérique par la création de labels « protection des données »

Pour que le citoyen puisse devenir **acteur de sa propre protection**, il faut non seulement, comme il vient d'être indiqué, qu'il ait été sensibilisé aux enjeux du numérique au regard du droit à la vie privée, mais encore qu'il dispose de l'information pertinente pour identifier, parmi les innombrables produits ou procédures proposés sur le marché, ceux qui offrent **des garanties renforcées** en matière de protection des données.

Il s'agit là d'une condition essentielle pour préserver le **climat de confiance** entre les nouvelles technologies et les utilisateurs.

C’est pourquoi vos rapporteurs sont convaincus de la nécessité de créer et généraliser **des labels « protection des données personnelles »** qui, parce qu’ils répondent à une attente forte des citoyens, sont susceptibles de procurer aux entreprises un avantage concurrentiel significatif (a).

Aussi ne peuvent-ils que se féliciter de l’intervention récente du Sénat pour permettre le lancement effectif de la labellisation en France (b), tout en étant conscients qu’à l’heure de la mondialisation, il faut prioritairement agir au niveau européen voire international (c).

a) Une exigence pour les citoyens, un outil de compétitivité pour les entreprises

(1) Une exigence pour les citoyens

Au cours des auditions conduites par vos rapporteurs, de nombreuses personnes ont regretté **l’absence d’information relative au niveau de protection** offert par les différents produits ou procédures proposés sur le marché en matière de droit à la vie privée.

Cette lacune contraste avec l’information délivrée aux consommateurs dans de nombreux domaines tels que la restauration, l’automobile ou l’environnement. On sait ainsi qu’un hôtel 4 étoiles offre de bonnes prestations, qu’un véhicule 5 étoiles est très résistant et qu’un congélateur de classe A + consomme peu d’énergie. Ces informations sur la qualité des produits semblent donner entière satisfaction aux consommateurs et leur fournissent des repères très utiles pour orienter leurs achats.

Ce besoin d’information est peut-être encore plus fort dans le domaine du numérique compte tenu de l’abondance des produits existants, de leur technicité et de leur caractère relativement récent.

Il est ainsi probable qu’à prix et service égaux, un utilisateur privilégierait s’il a le choix un produit labellisé, et que même à prix plus élevé ou service moindre, il pourrait **refuser une technologie intrusive** au profit d’une technologie dont le label lui assure un niveau de protection supérieur.

Concrètement, un tel label pourrait récompenser des protocoles, standards et outils **limitant, voire supprimant, la collecte des données à caractère personnel**, ce que les Américains appellent les « *Privacy Enhancing Technologies* » (ou « PET »), c'est-à-dire les technologies renforçant le droit à la vie privée.

A titre d’exemple, ce label pourrait être décerné à **un standard permettant l’anonymisation complète de l’adresse IP**. Rappelons, à cet égard, que s’il faut saluer les prises de position du G29 tendant à raccourcir les délais de conservation des données détenues par les moteurs de recherche, il semble illusoire de se focaliser sur la seule durée de conservation si la méthode d’anonymisation des données mise en œuvre n’est pas d’une grande

robustesse. Marc Rotenberg, responsable de l'EPIC[1], a ainsi condamné certaines méthodes d'anonymisation qui s'apparentent, selon lui, à celles qui consistent à dissimuler uniquement les derniers chiffres d'un numéro de téléphone.

De même, un tel label pourrait utilement aider les consommateurs à faire un choix éclairé en matière de technologie RFID. Il pourrait en effet **récompenser les puces qui sont automatiquement désactivées** (cf. *supra*) dès qu'elles ont rempli leur fonction, par exemple à la sortie d'un magasin où le produit était étiqueté, ou qui, à tout le moins, prévoient que, par défaut, leur contenu ne peut être lu que par leurs propriétaires, à charge pour eux de paramétrer éventuellement la puce s'ils souhaitent que d'autres personnes y aient accès. Il s'agit d'un enjeu important car les consommateurs détiennent, souvent à leur insu, de nombreuses puces RFID (badge d'accès à une voiture, un parking, étiquettes sur un produit alimentaire…) susceptibles de contenir des informations à caractère personnel qu'une personne malveillante située à proximité peut être capable de capter.

Enfin, un label « protection des données » pourrait être décerné **à des sites Internet proposant, par défaut, des paramètres basés sur un haut niveau de protection**, sachant qu'en pratique, ils sont rarement modifiés par les utilisateurs. Ainsi pourrait-il être attribué aux réseaux sociaux qui, par défaut, proposent un profil de consultation des données limité aux seuls amis du membre du réseau et non à tous les internautes.

(2) Un outil de valorisation et de compétitivité pour les entreprises

Compte tenu de l'attente des utilisateurs décrite plus haut, vos rapporteurs sont convaincus que les entreprises ont tout intérêt à faire de la protection des données personnelles de leurs clients un axe fort de leur développement et solliciter ainsi **l'octroi d'un label** marquant cette préoccupation. Ce label est en effet susceptible de leur procurer un **avantage concurrentiel** significatif dès lors qu'il devrait apparaître aux yeux des consommateurs comme un label de qualité de nature à orienter leurs achats.

Comme l'a proclamé la 30ème conférence mondiale des commissaires à la protection des données et de la vie privée, qui s'est tenue à Strasbourg en octobre 2008, « *la protection des données ne doit pas être considérée comme un obstacle au développement économique mais bien comme une valeur ajoutée dans les relations avec les consommateurs et les citoyens* ».

C'est ce que résume la formule, prononcée notamment par M. Arnaud Belleil, vice-président de l'Association Française des Correspondants aux Données Personnelles, lors de son audition : « ***Privacy is good for business*** » (littéralement : « le respect de la protection des données est bon pour les affaires »).

---

[1] *Comme il a déjà été indiqué, l'EPIC (Electronic Privacy Information Center) est une puissante association américaine qui défend le droit à la vie privée qu'elle estime menacée par le développement des nouvelles technologies.*

Faire de la protection des données personnelles un facteur de différenciation concurrentiel suppose toutefois que soit prise en compte cette exigence très en amont, **dès la conception des produits** (par exemple des logiciels ou des puces RFID), traduction de que les spécialistes appellent la « ***Privacy by design*** » (« protection des données dès la conception »).

A titre d'exemple, il semble que l'entreprise **Microsoft** ait décidé de faire protection de la vie privée **un outil de valorisation et de compétitivité**.

Lors de leur audition, les représentants de cette société ont ainsi fait valoir :

- que l'entreprise avait été l'une des premières à nommer, il y a près de dix ans, un Responsable de la Protection de la vie privée ;

- qu'elle a rendu publique, le 22 juillet 2007, une nouvelle politique de confidentialité, en matière de publicité en ligne et de recherche sur Internet[1]. Sur ce dernier point, les représentants de la société ont rappelé que, conformément à l'avis du G29 sur les moteurs de recherche, Microsoft ne conservait les données de requête que **six mois**, et militait pour que cette durée devienne le standard de l'ensemble du secteur, le moteur de recherche de Microsoft ne représentant toutefois que 2 % du marché européen. Ils ont ajouté que la société avait mis en place **une méthode d'anonymisation complète des données de connexion** à l'issue de cette période, fondée sur une « *Privacy Enhancing Technology* ».

b) L'intervention du Sénat pour permettre le lancement effectif de la labellisation en France

La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel a inséré un article 11 à la loi « informatique et liberté » afin de prévoir que la CNIL puisse, à la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements, « *délivrer un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la présente loi* ».

Or, après l'adoption de la loi, le ministère de la Justice a estimé que cette procédure devait être précisée par décret.

Inquiet du retard pris par le Gouvernement pour la publication de ce décret, notre collègue M. Alex Türk, président de la CNIL, a interrogé en 2008 Mme la garde des sceaux, ministre de la justice par une question écrite[2]. Celle-ci, prenant acte que la Commission avait « *estimé ne pas être en mesure de*

---

[1] Microsoft a développé un moteur de recherche au même titre que Google et Yahoo.

[2] Question écrite n° 06628 de M. Alex Türk publiée dans le JO Sénat du 11/12/2008 - page 2478 ; réponse du Ministère de la Justice publiée dans le JO Sénat du 01/01/2009 - page 38.
La question et la réponse sont disponibles sur Internet :
http://www.senat.fr/questions/base/2008/qSEQ081206628.html.

procéder elle-même aux expertises et évaluations nécessaires » et avait ainsi « *exprimé le vœu de recourir à des centres d'évaluation agréés* », a répondu qu'une telle externalisation des expertises ne pouvait être envisagée qu'en modifiant la loi « informatique et libertés ».

Aussi, le législateur, à l'initiative de la commission des lois du Sénat, a-t-il inscrit, à **l'article 105 de la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures**, une disposition modifiant la loi de 1978 afin :

- d'une part, d'ouvrir la possibilité pour le président de la CNIL de recourir aux services d'un expert indépendant, dont le rapport sera transmis à la commission qui décidera ou non de délivrer le label ;

- d'autre part, de prévoir que les modalités de mise en œuvre de la procédure de labellisation seront déterminées par le règlement intérieur de la CNIL, auquel il appartiendra, par exemple, de fixer la durée de validité du label, le mode de publicité des décisions prises, les conditions de retrait provisoire ou définitif des labels accordés, etc.

c) La nécessaire création de labels européens, voire mondiaux

S'il faut saluer cette intervention du législateur, qui devrait permettre le lancement effectif de la labellisation en France, il reste qu'à l'heure de la circulation des données et produits sur toute la planète, il faut prioritairement agir au niveau européen voire international.

Aussi, vos rapporteurs se réjouissent-ils que l'Union européenne, reprenant une initiative menée en Allemagne, ait conduit une expérimentation concluante dans ce domaine, expérimentation qu'ils jugent nécessaire de pérenniser et d'étendre.

Une démarche de labellisation de produits ou procédures offrant des garanties renforcées en matière de protection de la vie privée a été engagée en Allemagne, en 2005, dans le Land du Schleswig-Holstein, sous l'égide de l'autorité locale de protection des données, dénommée « ULD ».

A ce jour une quarantaine de labels ont été attribués.

Forte de cette expérience, l'ULD a été désignée par la Commission européenne responsable du projet dit « *Europrise* » (pour « *European privacy Seal* », littéralement « Label européen de protection de la vie privée »), conduit entre 2007 et 2008. Dans ce cadre, quarante-quatre experts, dont des représentants de la CNIL, ont été accrédités pour l'évaluation préalable des produits soumis à la certification, présentés par quelque trente sociétés.

Le premier label a été décerné à la société néerlandaise Ixquick, conceptrice d'un « métamoteur de recherche », c'est-à-dire d'un moteur de moteurs de recherche : son rôle consiste à agréger les réponses générées par les principaux moteurs (Google, Microsoft, Wikipedia…), sur une même requête et à les présenter de manière ordonnée à ses visiteurs. La société a été

récompensée car, d'une part, elle a décidé, en 2006, d'effacer de ses fichiers les adresses IP des utilisateurs au bout de seulement 48 heures, d'autre part, elle garantit qu'aucune donnée personnelle concernant ses utilisateurs n'est transmise à des tiers.

« *La remise de cette récompense à Ixquick montre qu'un équilibre est possible entre la nature ouverte de l'Internet, les intérêts des fournisseurs de services et la protection des données des utilisateurs* », avait déclaré Viviane Reding, commissaire européen en charge de la société de l'information.

Compte tenu du succès du programme expérimental « *Europrise* », vos rapporteurs jugent nécessaire de le pérenniser et de l'étendre. En effet, si la mise en place prochaine de la procédure de labellisation en France constitue indéniablement une avancée notable, elle devra nécessairement être suivie par une démarche plus ambitieuse au plan européen, voire international, eu égard à la mondialisation des échanges de produits et données.

Il conviendra donc de définir une autorité collégiale de délivrance des labels chargée :

- d'une part, d'élaborer des référentiels ou cahiers des charges définissant les critères à respecter pour l'obtention d'un label,

- d'autre part, d'accréditer une équipe multinationale composée d'experts-auditeurs mandatés pour évaluer les produits en fonction des référentiels susvisés et pour en contrôler le respect après l'obtention du label.

La recherche d'un accord mondial, qui pourrait trouver sa place dans la réflexion en cours relative à **la définition de standards internationaux** dans le domaine de la protection des données (cf. *supra*), pourrait être facilitée par l'existence, aux Etats-Unis, d'un label, connu sous le nom de « TRUSTe », qui récompense, d'une part, les sites Internet les plus protecteurs des données personnelles en matière de commerce électronique, d'autre part, depuis quelques années, les logiciels de messagerie.

D'après les informations obtenues par vos rapporteurs, ce label a été décerné depuis sa création en 1997 à près de 3.500 sites Internet, parmi lesquels ceux d'eBay, Apple, NFL et AT&T et à 71 logiciels de messagerie.

Recommandation n° 3 : Promouvoir rapidement la création de labels identifiant et valorisant des logiciels, applications et systèmes protecteurs de la vie privée.

B. RENFORCER LES MOYENS ET LA LÉGITIMITÉ DE LA CNIL

Comme il a été précédemment indiqué, la protection des données personnelles doit faire face à un triple défi :

- la recherche d'une sécurité collective toujours plus infaillible ;

- l'accélération des progrès technologiques et leur diffusion dans toutes les entreprises et sur tout le territoire ;

- la tendance croissante à l'exposition de soi et d'autrui sur Internet.

A ces risques nouveaux, il ressort que, dans l'Union européenne, le cadre juridique sur la protection des données personnelles apporte, dans une très large mesure, des réponses adaptées et pérennes, peut-être, paradoxalement, parce qu'il les a précédées.

Le droit au respect de la vie privée est en effet bien garanti au niveau national et international et les données personnelles, déclinaison du droit à la vie privée, fait l'objet d'un cadre juridique dont la souplesse apparaît comme un gage de protection : en se gardant d'adopter des dispositions spécifiques pour certaines technologies ou applications, l'Europe a opportunément décidé, dès 1995, d'adopter une directive neutre sur le plan technologique en fixant des principes intemporels (finalité, proportionnalité, droit d'information, durée de conservation limitée, sécurité des données…).

Toutefois, **l'application effective de ces principes est éminemment fonction des moyens dévolus aux autorités indépendantes de protection des données.** Or, les évolutions majeures rappelées ci-dessus ont conduit ces dernières à **une augmentation sensible de leur activité**, non seulement parce qu'elles sont chargées d'interpréter les principes « informatique et liberté » à l'aune des nouvelles technologies et des nouveaux usages, en progression constante, mais également parce qu'elles ont pour mission d'en contrôler le respect par des responsables de traitement toujours plus nombreux.

Vos rapporteurs préconisent donc un renforcement des moyens et de la légitimité de la CNIL.

1. Renforcer les moyens de la CNIL par la mise en place d'« un financement à l'anglaise »

a) Des moyens encore insuffisants

Les nombreux auditions et déplacements ont permis de constater **l'insuffisance des moyens alloués à la CNIL**, tant au regard de l'importance grandissante de ses missions que de ceux accordés à certains de ses homologues.

(1) Au regard de l'importance grandissante de ses missions

De nombreuses personnes entendues par vos rapporteurs ont mis en avant le décalage entre la progression de la charge de travail de la CNIL depuis la loi de 2004 et l'évolution de ses moyens humains et budgétaires.

Le tableau ci-dessous, réalisé à partir des rapports d'activité de la CNIL, souligne qu'alors que **le nombre de délibérations et celui des contrôles de la CNIL ont respectivement progressé, entre 2004 et 2008, de 458 % et 384 %**, les moyens sont loin d'avoir suivi cette montée en puissance spectaculaire : ainsi les effectifs n'ont-ils progressé, sur cette même période, que de 50 % et les crédits de 65 %.

Évolution des moyens de la CNIL
au regard de la progression de son activité entre 2004 et 2008

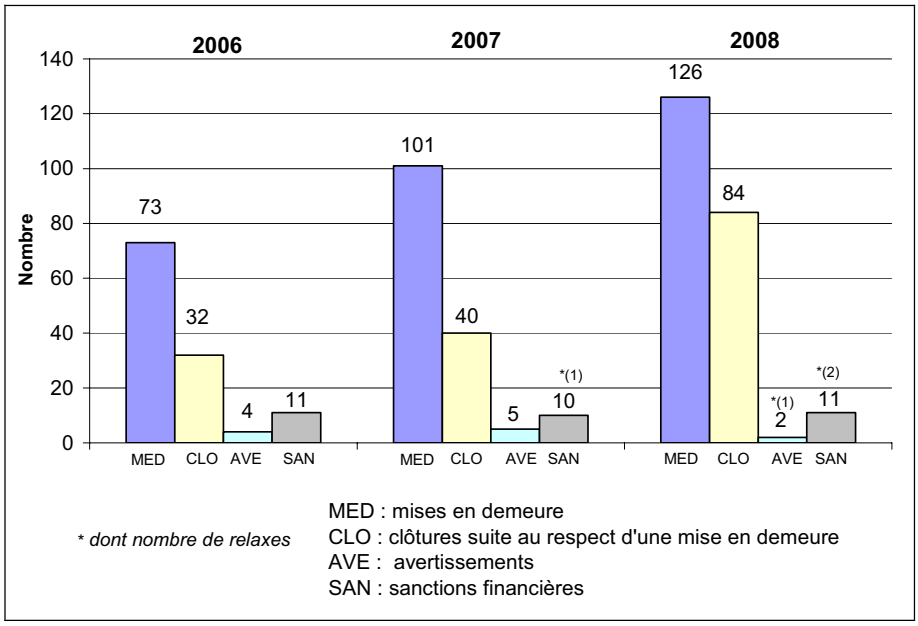
	2004	**2008**	**Evolution 2004-2008** (en %)
Postes	80	120	**+ 50 %**
Crédits (en M€)	6,9	11,4	**+ 65 %**
- dont personnel	4,6	7,2	
- dont fonctionnement	2,3	4,2	
Nombre de plaintes reçues	3591	4244	**+ 18 %**
Nombre de délibérations	105	586	**+ 458 %**
Nombre de contrôles effectués	45	218	**+ 384 %**

Cette progression globale de l'activité de la CNIL ne s'explique pas tant par l'augmentation du nombre des plaintes qui n'ont, elles, progressé « que » de 18 % de 2004 à 2009, que par la nécessité de répondre au **triple défi** décrit plus haut.

En effet, de nombreuses délibérations ont porté, depuis 2004, sur des **préconisations** concernant des technologies ou des usages nouveaux (déplacements urbains, vote électronique, puces RFID, panneaux publicitaires, géolocalisation, fichiers de police, réseaux sociaux…) et l'augmentation des contrôles est la conséquence directe de la multiplication et de la diversification des traitements de données en France.

En ce qui concerne l'activité de la formation restreinte, on peut noter que depuis 2006, année de l'entrée en vigueur effective de la nouvelle compétence contentieuse de la CNIL, le nombre d'affaires a quasiment doublé, comme l'illustre le schéma ci-après.

Sanctions prononcées par la CNIL entre 2006 et 2008



Source : CNIL

Là encore, cette progression illustre la volonté de la CNIL de faire un usage actif de ses nouveaux pouvoirs, dans un contexte marqué par **l'émergence de nouveaux risques d'atteinte à la vie privée**.

(2) Au regard de ceux accordés à certains de ses homologues

L'insuffisance des moyens accordés à la CNIL apparaît également au travers de comparaisons internationales.

Le tableau ci-après illustre que le ratio nombre d'agents par million d'habitants est particulièrement faible s'agissant de la CNIL (2,1) au regard de celui d'autorités d'autres pays tels que la République tchèque, le Canada, la Bulgarie, l'Irlande, l'Allemagne, les Pays-Bas, la Suède, le Royaume-Uni, l'Espagne ou encore la Roumanie.

En termes d'effectifs globaux, notons que l'autorité espagnole comprend 160 agents, l'autorité britannique 270, l'autorité canadienne 300 et l'autorité allemande 400.

EFFECTIFS DES AUTORITES DE PROTECTION DES DONNEES			
Autorités de Protection des Données	**Nombre d'employés**	**Population totale (en millions d'habitants)**	**Ratio nombre d'employés/million d'habitants**
France	**132**	**62**	**2,1**
République tchèque	100	10	10
Canada	300	33,3	9
Bulgarie	60	7,7	7,8
Irlande	22	4	5,5
Allemagne	400	82,4	4,9
Pays-Bas	75	16	4,7
Suède	42	9	4,7
Royaume-Uni	270	60	4,5
Espagne	160	45	3,6
Roumanie	52	22	2,4

Source : CNIL

On constate ainsi que confrontées, comme la CNIL, à de nouvelles menaces au regard du droit à la vie privée, de nombreuses autorités de protection des données sont dotées **de moyens humains supérieurs** à ceux de la France, si on les rapporte à la population du pays.

b) La mise en place d'un nouveau mode de financement

(1) Présentation de la réforme

Confrontée à la faiblesse de ses moyens, la CNIL s'interroge depuis 2008 sur la pertinence de son mode de financement actuel, exclusivement fondé sur une dotation fournie par l'Etat, alors qu'au Royaume-Uni, **une contribution versée par chaque société ou collectivité publique** qui déclare un traitement de données couvre la totalité des charges de la commission.

Le président de la CNIL a ainsi présenté l'an passé **un projet de diversification des sources de financement de la Commission**, qui suppose une modification de la loi de 1978 afin de faire de la CNIL une personne morale dotée de l'autonomie financière.

Ce projet, qui, d'après la CNIL, a rencontré de la part du Premier ministre un certain intérêt, propose de passer progressivement, au plus tôt à partir de 2010, du financement actuel à un financement qui reposerait majoritairement **sur des ressources propres** provenant d'une contribution due à la CNIL par chaque acteur du développement informatique qui génère des traitements de données à caractère personnel (entreprises, État, collectivités locales, établissements publics, etc.).

Pour la CNIL, l'intérêt d'une telle réforme serait double : d'une part, accroître ses ressources dans une proportion probablement importante, d'autre part, faire peser le financement de l'organe chargé du contrôle de la protection des données personnelles non plus sur les seuls contribuables mais également sur les acteurs du monde informatique, qui assurent la promotion des nouveaux usages technologiques.

Vos rapporteurs soutiennent pleinement ce nouveau mode de financement dès lors, comme la CNIL semble l'envisager, d'une part, qu'il exclura du périmètre des contributeurs les particuliers et les organismes de petite taille, d'autre part, que la redevance acquittée par les autres soit fixée à un niveau raisonnable.

Recommandation n° 4 : Renforcer les moyens de la CNIL par la création d'une redevance, de faible montant, acquittée par les grands organismes, publics et privés, qui traitent des données à caractère personnel.

(2) Les effets attendus : la création d'antennes interrégionales et le renforcement des capacités d'expertise et de contrôle de la CNIL

Selon vos rapporteurs, les ressources nouvelles générées par la mise en place du nouveau mode de financement décrit plus haut devraient être majoritairement mobilisées, d'une part, pour créer des antennes interrégionales de la CNIL, d'autre part, pour renforcer les capacités d'expertise et de contrôle de cette dernière.

En premier lieu, il apparaît nécessaire que la CNIL, à l'instar d'autres autorités administratives indépendantes telles que le Médiateur de la République, la Haute autorité de lutte contre les discriminations (HALDE) ou le Défenseur des enfants[1], engage **une déconcentration de ses services**.

En effet, l'un des défis nouveaux que doit relever la CNIL depuis quelques années est l'accélération des progrès technologiques et leur diffusion **dans toutes les structures, publiques et privées,** y compris les plus petites, et **sur tout le territoire**.

Or, ces structures ont besoin d'être **conseillées et accompagnées** dans la création ou le développement de leurs traitements de données personnelles, comme l'atteste le succès rencontré par les « Rencontres régionales » au cours

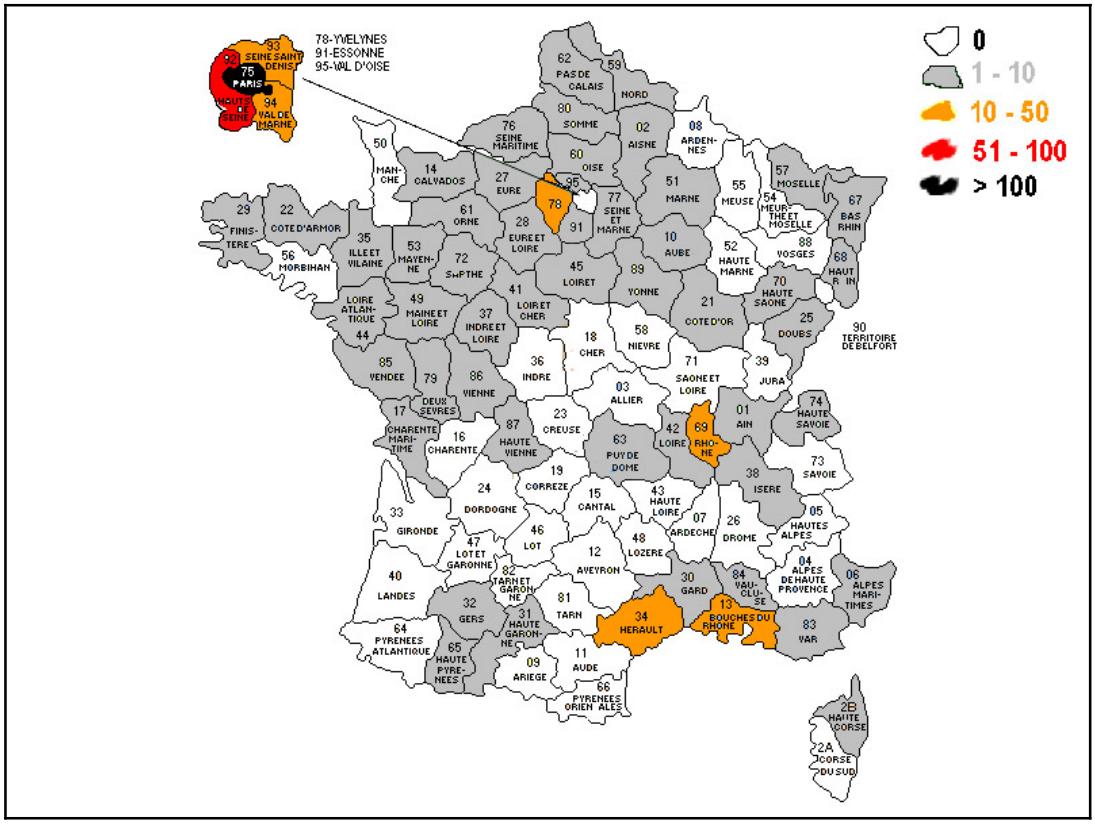
[1] *Voir le rapport budgétaire du 20 novembre 2008 de M. Jean-Claude Peyronnet sur le programme « Protection des droits et libertés » : http://www.senat.fr/rap/a08-104-8/a08-104-8.html.*

desquelles une délégation de la CNIL dialogue, pendant deux jours, avec l'ensemble des responsables des entreprises, des administrations préfectorales, des avocats, des personnels de santé, etc. Depuis 2007, la CNIL a organisé seize rencontres de ce type dans toute la France, rencontres qui ont toutes révélé de fortes demandes de la part des responsables économiques et administratifs.

Si, en 1978, la commission des lois du Sénat s'était prononcée contre la création de délégations régionales de la CNIL, jugeant l'intérêt d'une telle mesure limitée –la plupart des banques de données étant localisées à Paris– au regard des risques de « *bureaucratie* » et « *d'apparition de contrariété de jurisprudence* » , il semble que la généralisation du recours aux fichiers et leur dissémination sur l'ensemble du territoire, dans la quasi-totalité des structures, tant publiques que privées, **rendent désormais obsolète le modèle initial de la CNIL de 1978, installée seulement à Paris**.

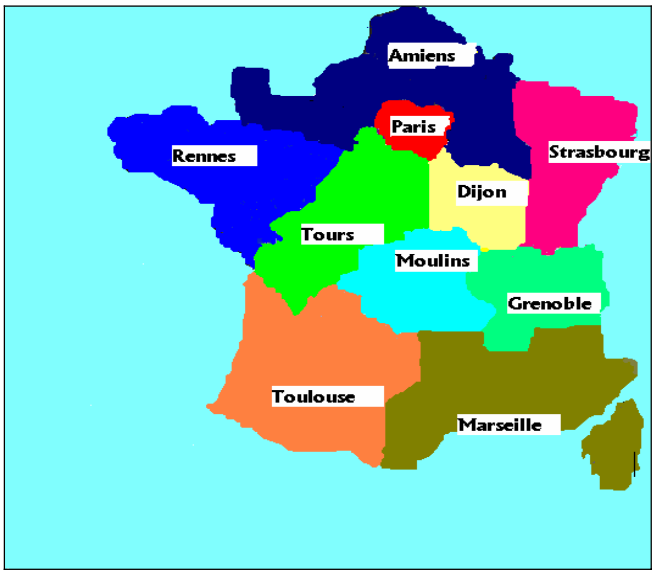
Comme le reconnaît la CNIL dans son dernier rapport d'activité, « *les effectifs encore insuffisants de la Commission ne permettent pas d'exercer une présence effective sur tout le territoire, et cela peut impliquer une certaine inégalité de traitement des droits des citoyens* ».

Nombre de contrôles effectués par la CNIL en 2008
sur l'ensemble de la France



Source : CNIL

D'après les informations obtenues par vos rapporteurs, la CNIL souhaiterait ouvrir **neuf antennes en province**, dotées chacune d'une équipe d'environ quinze agents, d'un budget de 400.000 euros et investies de missions de contrôle, de conseil, de traitement des plaintes les plus simples et d'information.



Source : CNIL

Recommandation n° 5 : Déconcentrer les moyens d'actions de la CNIL par la création d'antennes interrégionales.

En second lieu, de nouveaux moyens accordés à la CNIL lui permettraient de **renforcer ses capacités d'expertise et de contrôle**. Ce renforcement est rendu nécessaire par la multiplication et la diversification des traitements de données personnelles depuis quelques années, évolutions qui génèrent de **nouveaux risques** au regard du droit à la vie privée.

Certes, vos rapporteurs se réjouissent que la CNIL se soit dotée **d'un service de l'expertise**, composé de quatre ingénieurs de haut niveau qui sont à même d'accompagner les entreprises dans leurs projets, d'identifier, voire d'anticiper les tendances technologiques en cours et de contrôler plus efficacement les systèmes informatiques en matière de sécurité des données.

Toutefois, les auditions ont montré que la CNIL, comme l'ensemble des autorités de protection des données, souffraient **d'une image trop juridique qui affecte leur crédibilité**. Il est donc indispensable que ces autorités développent leur capacité d'expertise, de prospective et d'intervention dans le domaine technologique. Il paraîtrait ainsi opportun que chacune des antennes interrégionales évoquées plus haut comprenne au moins un expert.

Le renforcement de la capacité d'expertise de la CNIL pourrait utilement accompagner le développement de son **activité de contrôle, trop faible à l'heure actuelle**. La CNIL n'a ainsi effectué que 280 contrôles en 2008 contre environ 1.250 pour son homologue espagnol, qui affecte la moitié de ses effectifs au service de l'inspection.

En particulier, comme il a été indiqué précédemment, la CNIL est chargée de veiller au respect de l'article 34 de la loi du 6 février 1978 modifiée qui impose à tout responsable d'un traitement de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

Or, si en France aucun scandale n'a révélé des failles de sécurité graves, il semble que notre pays ne soit pas à l'abri d'une perte ou d'un vol de centaines de milliers de données, comme cela s'est produit à l'étranger ces dernières années. Ces risques nouveaux résultent à la fois de la multiplication des bases de données numériques et de leur **insuffisante sécurisation**, comme le constate régulièrement la CNIL, alors même que les pirates disposent d'outils toujours plus perfectionnés pour violer les systèmes de sécurité informatique.

Le développement de l'activité de contrôle de la CNIL, sur ce point, permettrait sans doute de **responsabiliser les responsables de traitements à ces enjeux de sécurité,** en particulier ceux qui traitent des données sensibles (cf. également *infra*).

Recommandation n° 6 : Renforcer la capacité d'expertise et de contrôle de la CNIL.

2. Renforcer la légitimité et la crédibilité de la CNIL

Si vos rapporteurs jugent prioritaires de renforcer les moyens de la CNIL, pour lui permettre de faire face à certaines évolutions majeures susceptibles de mettre à mal le droit à la vie privée, ils jugent également nécessaires, pour les mêmes raisons, de renforcer sa **légitimité et sa crédibilité** à la fois par le maintien de son autonomie, la généralisation des « Correspondants informatique et libertés », la publicité systématique des audiences et des décisions de la formation restreinte et, enfin, le renforcement éventuel de ses pouvoirs de sanction.

a) Par le maintien de l'autonomie de la CNIL

Il apparaît tout d'abord nécessaire de **maintenir l'autonomie de la CNIL**, que d'aucuns estiment menacée par la création du Défenseur des droits, prévue par la loi constitutionnelle n° 2008-724 du 23 juillet 2008 mais dont l'entrée en fonction est conditionnée par l'adoption d'une loi organique qui

devrait être soumise au Parlement au cours du second semestre 2009. Cette nouvelle autorité a vocation à reprendre les attributions de certaines autorités administratives indépendantes.

Pour vos rapporteurs, quatre raisons militent en faveur du maintien de l'autonomie de la CNIL par rapport au futur Défenseur des droits :

- en premier lieu, l'existence d'une instance indépendante chargée spécifiquement d'assurer la protection des données est **une exigence communautaire**, qui résulte de la directive de 1995 précitée. A cet égard, les vingt-sept autorités indépendantes que compte l'Union européenne sont exclusivement dédiées à la protection des données, à l'exception des CNIL allemandes et britanniques qui exercent également la mission dévolue, en France, à la Commission d'accès aux documents administratifs (CADA), et aucune d'entre elles n'est placée sous la tutelle, ni absorbée, par l'autorité de médiation lorsqu'elle existe (Défenseur du peuple espagnol ou ombudsman suédois) ;

- en second lieu, l'intégration de la CNIL au sein du futur Défenseur des droits mettrait à mal **sa visibilité et sa notoriété** acquises auprès de ses partenaires francophones et européens, étant rappelé que la CNIL est membre de l'organisation des « CNIL européennes » (dite aussi « G29 », voir supra, dont M. Alex Türk est le Président depuis avril 2008) et de l'association francophone des autorités de protection des données ;

- par ailleurs, la CNIL consacre aujourd'hui **80 à 90 % de son activité à des actions de régulation dans le secteur privé**, alors que le futur Défenseur des droits devrait surtout avoir vocation à intervenir dans la sphère publique ;

- enfin, comme il a été précédemment indiqué, la CNIL est dotée depuis la loi du 6 août 2004, **d'un rôle quasi-juridictionnel** dans le cadre de sa formation restreinte, tandis que le Défenseur des droits serait appelé à jouer essentiellement un rôle de médiation.

b) Par la généralisation des « Correspondants informatique et libertés »

Comme l'ont indiqué à vos rapporteurs les représentants de l'Association Française des Correspondants aux Données Personnelles, qui regroupe environ 10 % des correspondants informatique et libertés, le bilan de leur action apparaît pleinement satisfaisant. Ils ont ainsi permis, selon eux, « *la diffusion de la culture informatique et libertés au sein des entreprises et des administrations publiques* ». La CNIL partage cette analyse.

De même, les représentants de la chambre de commerce américaine à Paris ont salué le rôle joué, dans l'administration fédérale, des *Chief Privacy Officers* (CPO), équivalents des correspondants aux pouvoirs plus étendus (voir *supra*), et se sont réjouis du caractère obligatoire des correspondants en Allemagne, présentés comme des « facilitateurs » pour la bonne marche de l'entreprise.

Vos rapporteurs, regrettant en particulier la faible implantation des correspondants dans les collectivités territoriales[1], proposent donc de **généraliser les « Correspondants informatique et libertés » en France dans les structures, publiques et privées, d'une certaine taille**, par exemple de plus de cinquante salariés. Cette dernière condition paraît doublement essentielle : d'une part, elle permet de ne pas créer une contrainte supplémentaire pour les petites structures ; d'autre part, elle offre davantage de possibilités pour trouver, au sein de l'entreprise ou de l'administration, une personne dont **l'expérience** et **la compétence** garantiront **l'indépendance** indispensable au bon accomplissement de ses missions[2].

Vos rapporteurs insistent sur la nécessité pour la CNIL d'assurer une solide formation régulière à ces correspondants.

Recommandation n° 7 : Rendre obligatoires les correspondants informatique et libertés pour les structures publiques et privées de plus de cinquante salariés.

c) Par la publicité systématique des audiences et des décisions de la formation restreinte

Si, conformément aux règles du procès équitable issues de la jurisprudence du Conseil d'Etat et de la Convention européenne des droits de l'homme, la procédure suivie devant la formation restreinte est **contradictoire** et **le rapporteur ne participe pas au délibéré qui est secret**, il reste que le caractère juridictionnel de cette formation, reconnu par le Conseil d'Etat, par une ordonnance de référé le 19 février 2008, impose de **rendre publiques**, d'une part, **les audiences** (elles ne le sont aujourd'hui qu'à la demande des parties), d'autre part, **les décisions** qu'elle rend (mises en demeure, avertissements et sanctions financières), alors que cette publicité est aujourd'hui une simple faculté à la discrétion de la CNIL (article 46 de la loi « informatique et libertés ») .

Vos rapporteurs estiment en particulier que la publicité systématique des décisions de la formation restreinte de la CNIL constituerait une mesure efficace et dissuasive tant pour les personnes publiques que pour les entreprises privées.

Recommandation n° 8 : Rendre publiques les audiences et les décisions de la formation restreinte de la CNIL.

---

[1] *Comme l'a souligné M. Alex Türk, président de la CNIL, lors de son audition par la commission des lois le 5 novembre 2008.*

[2] *L'indépendance des correspondants informatique et liberté est une exigence posée par la loi de 1978 (article 22).*

d) Par le renforcement éventuel de ses pouvoirs de sanction

Vos rapporteurs préconisent également de **réfléchir à l'opportunité de renforcer les pouvoirs de sanction de la CNIL.**

En effet, l'article 47 de la loi de 1978 limite la sanction financière à **150.000 euros**, ou 300.000 euros en cas de manquement réitéré dans les cinq années, à condition de ne pas excéder 5 % du chiffre d'affaires hors taxes du dernier exercice clos.

A ce plafonnement légal s'ajoute **une pratique empreinte d'une certaine timidité.** Il semble que la première sanction, 45.000 euros contre le Crédit lyonnais en juillet 2006, somme à l'évidence modeste pour une entreprise de cette importance, ait servi de jurisprudence. En 2008, la CNIL a ainsi prononcé onze sanctions pour un montant total de 137.100 euros. Rappelons que le montant total des sanctions prononcées par la formation restreinte de la CNIL depuis sa création s'élève à 520.400 euros.

A titre de comparaison, on notera :

- que le Conseil de la Concurrence a le pouvoir d'infliger une amende qui peut aller jusqu'à 10 % du chiffre d'affaires mondial de l'entreprise (article L. 464-2 du Code de commerce), sans plafonnement en valeur absolue ; elle a ainsi prononcé une amende de 534 millions d'euros en 2005 dans le domaine de la téléphonie mobile et de 174 millions d'euros en 2000 dans une affaire de crédit immobilier ;

- que l'agence espagnole de protection des données, dont la sanction ne peut excéder 600.000 euros, est particulièrement sévère, en pratique, à l'encontre des entreprises qui contreviennent au droit applicable aux données personnelles. Ainsi, sur la seule année 2008, pas moins de 630 sanctions ont été prononcées pour un total de 22,6 millions d'euros.

Compte tenu de ces éléments, vos rapporteurs estiment nécessaire d'ouvrir un débat sur l'opportunité de relever le plafond des sanctions pécuniaires susceptibles d'être prononcées par la CNIL.

C. COMPLÉTER LE CADRE JURIDIQUE ACTUEL

S'il apparaît souhaitable de conserver le cadre juridique actuel, un certain nombre de compléments et d'améliorations à la marge pourraient y être utilement ajoutés.

1. Ne pas toucher aux grands principes…

a) Conserver un haut niveau de protection : le débat sur la révision de la directive du 24 octobre 1995

Vos rapporteurs se sont interrogés sur l'opportunité de recommander la révision de la directive du 24 octobre 1995, qui, comme il a été précédemment indiqué, sert de cadre juridique à la protection de la vie privée en Europe et a été transposée en France par la loi du 6 août 2004.

Après avoir analysé les positions, d'une part, du Royaume-Uni et de l'Irlande, d'autre part, de la Commission européenne, ils sont arrivés à la conclusion que le *statu quo* était préférable.

(1) La position du Royaume-Uni et de l'Irlande : réviser la directive de 1995 pour la rendre « plus efficace et moins lourde pour les entreprises »

Jugeant la directive de 1995 trop contraignante pour les entreprises et, de surcroît, inadaptée aux technologies du XXI^{ème} siècle, l'autorité britannique de protection des données (« *Information Commissioners Office* » ou « ICO ») a clairement pris position pour sa révision, par communiqué de presse du 7 juillet 2008.

M. Richard Thomas, son Président, a ainsi mis en avant la nécessité de « *mener un débat international sur la future orientation de la législation européenne relative à la protection des données* ». Il a cependant indiqué qu'il s'agissait d'un objectif qui ne pourrait être atteint avant cinq ou six ans.

D'après les informations recueillies par vos rapporteurs auprès de la CNIL et de la commission européenne, il semble que l'Irlande soit également sur cette même ligne.

La CNIL comme l'Agence espagnole de protection des données ont fait part à vos rapporteurs de leurs **craintes que ces positions,** si elles devaient emporter l'adhésion des autres Etats membres, **n'aboutissent à abaisser le niveau de protection des données en Europe.**

(2) La position de la Commission européenne : répondre aux nouveaux défis technologiques sans réduire le niveau de protection de la directive

La Commission européenne affiche, elle, une position différente sur la question de la révision de la directive de 1995.

Si, comme le Royaume-Uni et l'Irlande, elle juge nécessaire de réfléchir à la révision de la directive, en particulier pour « *répondre aux nouveaux défis dont on parle aujourd'hui, que nous ne pouvons plus ignorer et que nous devons absolument relever* »[1], elle souligne également qu'il convient de ne pas réduire le niveau de protection que la directive a institué, garant du respect de la vie privée dans l'Union européenne.

Il est donc clair que la Commission européenne n'a pas, en l'état, l'intention de promouvoir une révision de la directive qui aurait pour effet d'alléger les contraintes pesant sur les entreprises qui gèrent des traitements de données, et il semble *a priori* peu probable que la future Commission, qui entrera en fonctions à l'automne 2009, adopte une position différente.

---

[1] *Extrait du discours prononcé par M. Jacques Barrot, commissaire en charge de la protection des données, le 28 janvier 2009 lors la troisième journée européenne de la protection des données. Mme Viviane Reding, commissaire chargée des nouvelles technologies, est sur la même ligne : dans un communiqué publié le 14 avril 2009, elle a en effet souligné que la directive datait de 1995, « époque où internet était beaucoup moins développé qu'aujourd'hui » et que sa mise à jour était rendue nécessaire par « la rapidité du développement technologique ».*

(3) La position de vos rapporteurs : « ne pas ouvrir la boite de Pandore »

Compte tenu de ces positions, manifestement incompatibles, vos rapporteurs considèrent comme *a priori* peu opportun d'engager un processus de révision de la directive de 1995 qui exposerait l'Europe, et donc notre pays, à **un double risque** :

- d'une part, **revenir sur la plasticité des concepts** forgés par la directive de 1995 en matière de protection des données, concepts dont, rappelons le, la neutralité technologique garantit la pérennité ;

- d'autre part, **aboutir à un cadre juridique moins protecteur** pour les personnes alors que la directive offre déjà un haut niveau de protection des données. A cet égard, vos rapporteurs notent que les Etats-Unis pourraient saisir l'opportunité de l'engagement d'un processus de révision de la directive pour convaincre les Européens d'adopter leur système en matière de données personnelles, globalement moins protecteur pour les données gérées par les entreprises, même si nous verrons plus loin que les approches sont, de fait, moins éloignées que ce qu'on a coutume de dire.

Une récente polémique illustre parfaitement ce risque.

Le 20 juin 2008, la commission européenne a publié un « *appel à manifestation d'intérêts* », afin de constituer **un groupe d'experts** chargé de réfléchir au cadre juridique applicable à la protection des données personnelles en Europe.

Vingt dossiers, émanant d'Américains comme d'Européens, ont été présentés à l'expiration du délai limite de réception des candidatures, fixé au 20 août 2008.

Le comité de sélection de la commission a retenu un Européen et quatre Américains ou représentants de sociétés ayant leurs principaux intérêts aux Etats-Unis, apparemment au regard de leurs compétences techniques mais visiblement sans prendre en compte la dimension politique d'un tel choix.

Grâce, d'une part, à la vigilance de la CNIL, bien relayée par la commission des affaires européennes du Sénat[1], d'autre part, à la diligence du gouvernement français, la commission européenne a décidé de dissoudre ce groupe d'experts et de le remplacer par une nouvelle instance de réflexion composée de manière équilibrée et pluraliste afin d'assurer la représentation de toutes les approches en matière de protection des données[2].

Au total, il apparaît plus sage, dans le contexte d'une négociation nécessairement plus difficile et plus incertaine à 27 qu'elle ne le fut à 12, puis à 15, en 1995, et compte tenu des positions de certains Etats membres et de la possible influence du système américain, **de ne pas engager de processus de révision de la directive de 1995.**

---

[1] *Le 3 février 2009, la commission des affaires européennes du Sénat, suite à une audition de M. Alex Türk, président de la CNIL, a décidé, à l'initiative de son Président, M. Hubert Haenel, d'adopter une proposition de résolution européenne pour protester contre la composition de ce groupe d'experts.*

[2] *Cette instance s'est réunie à Bruxelles les 19 et 20 mai 2009.*

b) Promouvoir, au plan international, la définition de standards internationaux dans le domaine de la protection des données

Un des enjeux essentiels à l'avenir sera de trouver, au plan international, **une approche commune en matière de protection des données** qui, en plus de représenter un objectif essentiel sur le plan économique, permettrait de relativiser l'importance du problème juridique de l'extra-territorialité.

Le fait, d'une part, que la protection des données personnelles aux Etats-Unis soit en réalité **plus forte** qu'il n'est coutume de le dire, d'autre part, qu'Européens et Américains aient prouvé, dans un passé récent, leur capacité à surmonter leurs différends en matière de protection des données, invite à un certain **optimisme** quant à la possibilité d'aboutir à des standards internationaux dans ce domaine, objectif actuellement poursuivi par un groupe de travail international.

(1) un objectif essentiel sur le plan économique

En premier lieu, la recherche, au plan mondial, d'une approche commune de protection des données personnelles est rendue indispensable par l'intensification des flux transfrontaliers de données personnelles, phénomène irréversible au cœur **d'enjeux économiques** considérables.

Deux exemples ont régulièrement été cités lors des auditions :

- tout d'abord, d'innombrables données circulent au sein des multinationales, qui disposent généralement d'une **base de données centralisée,** gérée par les services centraux de la direction des ressources humaines de l'entreprise. Cette base comporte des renseignements de tous ordres sur le personnel : formations, qualifications, postes précédemment occupés, souhaits d'affectation, notations, loisirs…, renseignements collectés à partir de **multiples sources** (formulaires remplis lors des entretiens d'embauche, appréciations par les supérieurs hiérarchiques, participation à des cycles de formation…) et envoyés à partir de lieux divers (centres de formation, directions du personnel des différentes entités locales…) ;

- par ailleurs, la **délocalisation d'activités** dans des pays en développement génère également d'importants flux de données transfrontaliers. A titre d'illustration, de nombreuses entreprises européennes décident de sous-traiter l'ensemble de leurs relations-clients auprès de centres d'appel situés en Afrique du Nord ou en Inde, ce qui implique le transfert des fichiers de la clientèle, et donc de données à caractère personnel.

(2) un moyen de relativiser le problème de l'extraterritorialité

La question de savoir quel est le droit applicable à certains traitements de données personnelles, par exemple dans le cas des moteurs de recherche (cf. infra), se pose aujourd'hui avec d'autant plus d'acuité que tous les systèmes nationaux n'assurent pas un niveau de protection équivalent. Avec des standards internationaux permettant une harmonisation mondiale des conditions de protection des données, ce problème s'en trouverait clairement relativisé.

(3) des raisons d'y croire

(a) Des affaires qui prouvent qu'Européens et Américains sont capables de rapprocher leurs points de vue

Si l'Europe et les Etats-Unis n'ont toujours pas complètement aplani leur différend au sujet de l'affaire des dossiers passagers dite PNR, d'autres dossiers ont récemment prouvé qu'Européens et Américains étaient capables de rapprocher leurs points de vue en matière de protection des données. Citons en particulier les principes du « Safe Harbor », le dossier des moteurs de recherche et l'opération dite « Swift ».

- « Les principes du Safe Harbor »[1]

Afin de permettre aux entreprises américaines **de recevoir des flux de données personnelles** des pays membres de l'Union européenne, des principes ont été élaborés, à partir de 1999-2000, par le Département du commerce américain en coopération avec la Commission européenne. Ils portent en particulier sur le droit d'accès, la finalité du traitement et l'effectivité de la protection. Leur respect est contrôlé par la Commission fédérale du commerce.

Ces principes s'inscrivent dans la démarche de l'Union européenne qui, en liaison avec le G29, a élaboré, en 2001 et 2005, des **clauses contractuelles types**, qui permettent de sécuriser les transferts de données vers des pays extra-communautaires qui ne disposent pas d'un niveau de protection adéquat[2].

- L'affaire des moteurs de recherche

Même si, comme il a été indiqué dans la deuxième partie du présent rapport, certains moteurs de recherche américains ont contesté l'applicabilité du droit communautaire aux traitements de données auxquels ils procèdent en Europe, force est de reconnaître qu'ils ont fait preuve d'une certaine **bonne volonté**, que la CNIL a d'ailleurs saluée dans un communiqué le 17 décembre 2008, puisque la société Google a réduit la durée de conservation des données de dix-huit à **neuf mois**, que Microsoft a accepté de ne conserver les données que **six mois** et qu'enfin Yahoo a annoncé son intention de passer à **trois mois**, sauf exceptions concernant les impératifs de sécurité, de lutte contre de la fraude et de respect des obligations légales.

---

[1] *Littéralement « principes du port sûr », généralement traduits en français par « principes de la sphère de sécurité relatifs à la protection de la vie privée ».*

[2] *L'article 25 paragraphe 1 de la directive de 1995 sur la protection des données fait obligation aux Etats-membres de veiller à ce que les transferts de données à caractère personnel vers un pays tiers n'aient lieu que si le pays en question assure un niveau de protection adéquat. Ce dernier s'apprécie en fonction notamment des dispositions en vigueur dans le pays tiers, des mesures de sécurité qui y sont appliquées mais aussi des caractéristiques propres du traitement, telles que ses finalités et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées.*

▪ L'affaire « Swift »

Enfin l'affaire « Swift » démontre la capacité d'aboutir à un **accord transatlantique** en matière de protection des données.

Cette affaire est née de la révélation en juin 2006, par la presse américaine, de l'existence d'un **programme de surveillance des transactions bancaires internationales**, mis en place par la CIA peu après les attentats du 11 septembre 2001. Ces révélations ont indiqué que la CIA et le département du Trésor américain bénéficiaient d'un accès, depuis des années, à des millions de données transitant par la société de droit belge Swift, principal réseau international de messagerie utilisé dans le domaine bancaire.

Cet accès, mis en place au titre de la lutte contre le financement du terrorisme, permettait de surveiller non seulement les transferts financiers vers les Etats-Unis mais également tous les autres types de transactions réalisés par Swift, y compris à l'intérieur de l'Union européenne. Etaient ainsi communiqués le montant de la transaction, la devise, la date valeur, le nom du bénéficiaire, le client qui a demandé la transaction financière et son institution financière.

Le G29, dans un avis rendu en novembre 2006, a jugé que la société Swift n'avait pas respecté les règles européennes de protection des données, notamment en prêtant son concours à la mise en œuvre du programme de surveillance des données bancaires et financières par les autorités américaines.

Cette intervention a permis d'aboutir à un **accord en l'espace de quelques mois**. Au printemps 2007, la Commission européenne et le Conseil ont en effet négocié avec le gouvernement américain un certain nombre de **garanties**, parmi lesquelles la limitation des usages à la lutte contre le terrorisme, l'échange des données intra-européennes au moyen d'un serveur situé en Europe[1], le respect du principe de nécessité, la limitation à cinq ans de la durée de conservation des données et la nomination d'une « personnalité européenne éminente » ayant compétence pour vérifier le bon fonctionnement du programme de surveillance (M. Jean-Louis Bruguière). Cet accord politique a fait l'objet d'un échange de lettres qui ont été publiées par la Commission européenne.

(b) Une protection aux Etats-Unis plus forte qu'on ne le croit

- des principes similaires à ceux existant en Europe pour les bases de données gérées par l'administration fédérale

Si, comme il l'a été précédemment indiqué, les Etats-Unis protègent moins les bases de données privées qu'en Europe, en dehors de quelques lois sectorielles, **il n'en est pas de même des données gérées par les pouvoirs publics.**

---

[1] *En Suisse exactement, pays considéré comme offrant un niveau adéquat de protection des données.*

Comme l'a exposé, lors de son audition, Mme Lauren Saadat, directrice chargée de la politique internationale en matière de protection des données au ministère de la Sécurité des Etats-Unis (Department of Homeland Security), une « Privacy Act », adoptée en 1974, **s'applique à toute l'administration fédérale.** Elle énonce les principes de transparence, de droit d'accès et de rectification, de limitation de collecte des données, de leur usage et de leur divulgation, de la sécurité des données et de responsabilité des gestionnaires de traitement. Ces principes sont très proches de ceux figurant dans la directive de 1995 et transposés en France en 2004. Cet encadrement juridique traduit, selon Mme Saadat, une certaine **défiance historique** vis-à-vis des pouvoirs publics puisque les Etats-Unis ont été créés en réaction contre le pouvoir de la couronne britannique et que tant la mise en place du fédéralisme que la stricte application de la séparation des pouvoirs au niveau fédéral traduisent la volonté de prévenir l'apparition d'un pouvoir central fort.

On peut ajouter que cette protection des bases de données publiques est parfois complétée au niveau des Etats puisqu'environ un quart d'entre eux ont des législations générales de protection des données applicables aux fichiers de l'État.

- une position plus avancée que l'Europe à certains égards

Les auditions ont révélé que, contrairement à certaines idées reçues, les Etats-Unis sont, à certains égards, **plus en pointe que l'Europe en matière de protection des données.**

En premier lieu, certaines Constitutions d'États fédérés américains reconnaissent expressément la protection des données personnelles comme un droit fondamental. La plus forte protection par une Constitution est ainsi assurée en Californie où en 1974, un référendum a fait de la protection des données un **droit inaliénable** et où, en 1994, la Cour suprême de l'Etat a décidé que la protection constitutionnelle s'appliquait aussi bien au secteur public que privé.

En second lieu, toutes les administrations fédérales **comprennent obligatoirement un « Chief Privacy Officer » (CPO)**[1], garant du respect du « Privacy Act » et placés sous l'autorité et le contrôle d'un organe de la Maison blanche dénommé « Office of Management and Budget » (OMB) ; même s'il semble que ces CPO disposent de peu de moyens et que l'OMB mobilise peu de ressources pour les contrôler, cette organisation mérite d'être signalée et traduit une préoccupation certaine des Etats-Unis en matière de protection des données personnelles gérées par les personnes publiques.

---

[1] *Le CPO est comparable à un correspondant informatique et libertés mais aux pouvoirs plus étendus. En effet, il dirige tout un service, à la différence du correspondant qui est seul. En outre, il est obligatoirement associé, très en amont, aux projets informatiques de l'administration à laquelle il appartient. C'est pourquoi les représentants américains ont estimé que le CPO « pourrait presque se comparer à une autorité de protection de données personnelles interne à l'administration, une sorte de "mini-CNIL". »*

Par ailleurs, il apparaît que les Etats-Unis sont en avance sur l'Europe en matière de **transparence quant aux éventuelles failles de sécurité**, qu'il s'agisse de perte, vol ou altération de données. Alors que l'Europe devrait prochainement réviser la directive « vie privée et communications électroniques » de 2002, en particulier pour introduire une obligation d'information quand des données personnelles ont été compromises à la suite d'une violation de la sécurité d'un réseau, 45 Etats américains sur 50 disposent déjà d'une législation contraignante dans ce domaine.

Enfin – et ce point est capital – il ressort des auditions que si les Etats-Unis protègent peut-être un peu moins *de jure* les données personnelles privées, les quelques lois en vigueur **sont** *de facto* **rigoureusement appliquées**. Les associations de consommateurs, tout comme certaines associations spécialisées dans la protection des données[1], sont particulièrement puissantes[2] et leur action bien relayée par les médias.

De surcroît, la Commission fédérale du commerce américaine semble résolue, depuis quelques années, à **sanctionner sévèrement** les atteintes aux lois sur la protection des données. Elle a ainsi, en septembre 2006, infligé une amende d'**un million de dollars**, pour une infraction, commise par le réseau social Xanga.com, à la loi précitée portant protection de la vie privée des enfants sur Internet. Plus récemment, en décembre 2008, la société Sony BMG Music Entertainment a accepté de régler une amende, également d'un montant d'un million de dollars, pour mettre fin aux poursuites engagées contre elle par cette même commission et sur ce même fondement légal. Il était reproché à l'entreprise d'avoir collecté et diffusé, via des sites musicaux, des données personnelles sur des enfants de moins de treize ans sans recueillir l'autorisation préalable des parents.

Ces montants **contrastent singulièrement** avec ceux pratiqués en Europe, notamment en France, comme il a été précédemment indiqué. Ainsi, à titre d'exemples, la société Neuf-Club Internet a été condamnée par la CNIL, en juin 2008, à une amende de 7.000 euros pour violation du droit d'accès aux données personnelles et en mars 2009, un centre commercial Leclerc a fait l'objet d'une sanction de 30.000 euros à la suite de nombreuses infractions à la loi « informatique et libertés ».

On observe ainsi que si les Etats-Unis disposent d'un **arsenal juridique moins contraignant** que l'Europe pour les bases de données privées, cette faiblesse est contrebalancée par une **effectivité du droit**[3] **incontestablement meilleure**.

---

[1] Citons en particulier l'EPIC (Electronic Privacy Information Center) dirigé par l'universitaire Marc Rotenberg.

[2] Elles peuvent notamment s'appuyer sur l'existence d'actions de groupe (ou « class actions ») qui n'existent pas en droit français.

[3] C'est ce que traduit le concept anglais de « compliance » souvent prononcé par les représentants américains entendus par vos rapporteurs.

(c) La dynamique en cours du groupe de travail international sur la protection des données personnelles

Lors de la dernière conférence internationale de protection des données qui s'est tenue en octobre 2008 à Strasbourg, une résolution visant à établir des **standards internationaux** a été adoptée. Un groupe de travail international s'est déjà réuni en janvier 2009 à Barcelone dans le cadre de la préparation de la prochaine conférence mondiale de protection des données qui se tiendra en octobre 2009 en Espagne.

Vos rapporteurs soutiennent pleinement cette **démarche ambitieuse** et souhaitent qu'elle permette**, sans abaisser le niveau de protection garanti par la directive de 1995**, d'examiner sans tabou l'ensemble des questions relatives à la protection des données personnelles, telles que la définition d'un référentiel destiné à permettre la labellisation, au plan mondial, des produits offrant des garanties renforcées dans le domaine de la protection de la vie privée, ainsi que l'opportunité de créer, sur le modèle de l'organisation mondiale de la propriété intellectuelle, une agence internationale de régulation compétente dans le domaine de la protection des données.

Ce groupe de travail international peut s'appuyer :

- d'une part, sur l'adoption par l'OCDE[1], dès le 23 septembre 1980, de *« lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel »*, lignes directrices qui traduisent un **consensus international ancien** sur les orientations générales régissant le recueil et la gestion d'informations de caractère personnel ;

- d'autre part, sur l'existence de normes internationales « ISO » dans certains domaines de la protection des données personnelles, telles que l'archivage électronique[2].

Une fois élaborés, ces standards internationaux pourraient aboutir à la signature d'une **convention internationale**.

Recommandation n° 9 : soutenir la dynamique en cours tendant à la définition de standards internationaux dans le domaine de la protection des données personnelles.

2. ... sans s'interdire des précisions et un renforcement de l'effectivité de ces principes

Si les grands principes de la protection des données demeurent la bonne réponse aux développements des technologies numériques, cette conclusion n'interdit pas une amélioration à la marge de ces principes et de leur déclinaison.

---

[1] Organisation de coopération et de développement économiques, l'OCDE est une organisation internationale, créée en 1961, qui offre aux Etats-membres un cadre leur permettant de comparer leurs expériences en matière d'action publique, de chercher des réponses à des problèmes communs, d'identifier les bonnes pratiques et de coordonner leurs politiques nationales et internationales.

[2] Normes ISO n°s 14721 et 15489.

S'agissant des principes de proportionnalité et de finalité, il semble délicat d'apporter des précisions, l'appréciation du respect de ces principes demeurant une affaire d'espèces.

En revanche, le droit à l'information ou le droit d'accès sont des principes plus objectifs. Leur mise en œuvre pourrait être précisée.

Ainsi, à l'article 39 de la loi du 6 janvier 1978 modifiée, l'exercice du droit d'accès pourrait ne plus donner lieu à aucune facturation, fût-elle le coût de la reproduction.

En matière d'information, la loi pourrait préciser qu'elle doit être claire, complète « *et adaptée aux différents publics visés par le traitement* ».

De manière plus fondamentale, vos rapporteurs ont identifié quatre domaines dans lesquels des améliorations pourraient être utilement apportées : le statut des données de connexion, les dispositions relatives à la sécurité des données, le cadre juridique de la vidéosurveillance, et, enfin, l'encadrement des fichiers de police.

a) Clarifier le statut de l'adresse IP

Alors que le statut juridique de l'adresse IP en France demeure flou (cf. *infra*), **vos rapporteurs ont pour leur part acquis la conviction que l'adresse IP constituait un moyen d'identifier un internaute,** au même titre qu'une adresse postale ou un numéro de téléphone par exemple : l'adresse IP répond de ce point de vue aux critères fixés par la directive 95/46/CE, repris à l'article 2 de la loi du 6 janvier 1978 modifiée et selon lesquels une donnée à caractère personnel est une information « *relative à une personne identifiée **ou identifiable*** ».

Leur attention a en outre été attirée sur le fait que, contrairement à la juridiction judiciaire, la juridiction administrative ne contestait pas le caractère de donnée personnelle de l'adresse IP[1].

Compte-tenu du rôle essentiel qu'Internet est appelé à jouer dans la vie d'une partie sans cesse croissante de nos concitoyens, il leur semble indispensable que les garanties concernant la collecte de données à caractère personnel s'appliquent également sans ambiguïté aux données de connexion des internautes. **Une rapide clarification en ce sens de l'article 2 de la loi du 6 janvier 1978 leur paraîtrait de ce point de vue tout à fait opportune.**

Recommandation n° 10 : Affirmer sans ambiguïté que l'adresse IP constitue une donnée à caractère personnel.

b) Améliorer les dispositions relatives à la sécurité des données

Le principe de la sécurité des données est probablement celui qui mériterait les aménagements les plus importants.

---

[1] *Voir notamment CE, 23 mai 2007, SACEM et autres.*

L'article 34 de la loi du 6 février 1978 modifiée impose à tout responsable d'un traitement de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

Principe fondamental, la sécurité des données est **en pratique difficile à vérifier**, à moins de contrôler chaque système de sécurité par des attaques-tests. En outre, l'évolution de l'état de l'art en cette matière rend rapidement obsolète un système de sécurité qui était hier encore inviolable. L'actualisation des anti-virus illustre cette course constante entre le bouclier et le glaive.

Difficile à contrôler en amont, la sécurité des données est aussi **délicate à définir par la réglementation** en raison de l'évolution rapide des techniques[1]. En outre, il n'existe pas une réponse unique, mais autant que de systèmes à protéger. L'exposition à une attaque extérieure n'est pas égale.

Dans ces conditions, la CNIL intervient surtout lorsque la faille de sécurité est flagrante : perte de données, accès libre à certaines données, etc. L'absence de mesures destinées à assurer la sécurité et la confidentialité des données expose alors le responsable du traitement à des sanctions lourdes (5 ans d'emprisonnement et 300.000 euros d'amende). La CNIL peut également prononcer une série de sanctions (avertissement, amende, injonction de cesser le traitement, retrait de l'autorisation, interruption du traitement) prévue à l'article 45 de la loi du 6 janvier 1978.

Néanmoins, si, en France, assez peu de scandales ont révélé des failles de sécurité graves, à l'étranger les exemples sont nombreux. A chaque fois, ce sont des centaines de milliers de personnes, voire plusieurs millions, dont les données sont perdues ou, ce qui est plus dangereux, volées.

Quelques exemples de faille de sécurité

Novembre 2007 : des cédéroms contenant les données bancaires de 25 millions de contribuables sont égarés par les services fiscaux britanniques.

Avril 2008 : la première banque britannique perd un cédérom contenant des informations sur 370.000 de ses clients.

Août 2008 : un ordinateur contenant les données bancaires d'un million de clients britanniques est vendu pour 44 euros sur le site d'enchères eBay.

Dans le même temps, le ministère des Finances britannique égare un fichier comportant les noms des 84.000 prisonniers, dont ceux de 10.000 personnes « à surveiller en priorité pour leur comportement délictueux prolifique ».

En août 2008, la presse allemande révèle qu'il est possible d'acheter sur Internet des fichiers de 6 millions de données confidentielles pour 850 euros.

Source : CNIL

[1] *L'article 34 de la loi du 6 janvier 1978 permet l'élaboration de prescriptions techniques pour les traitements les plus sensibles.*

La CNIL estime qu'en France, même si aucune faille importante de sécurité n'a été révélée, **le niveau de protection des données ne peut être jugé satisfaisant**, comme en témoignent ses contrôles, tant auprès des entreprises que des administrations. La sécurité des données ne constitue malheureusement pas encore une préoccupation majeure.

Selon des responsables de Thalès, si les administrations et les entreprises sensibles sont bien protégées en France, des progrès très importants restent à accomplir pour sécuriser les données du secteur marchand.

Il serait absurde d'appliquer à tous les traitements les normes de sécurité mises en œuvre pour protéger le secret de la Défense nationale. Mais il semble à tout le moins que tout organisme possédant de grandes bases de données incluant des informations telles que des numéros de compte bancaire ou de carte de crédit devrait mettre en œuvre des sécurités renforcées. Selon Thalès, la précaution consistant à crypter la base de données elle-même est peu répandue.

Lors de leur audition, les représentants de la chambre américaine de commerce en France ont expliqué que **la règle selon laquelle les failles de sécurité** –vols et pertes de données– **doivent être notifiées occupait une place très importante dans le dispositif américain de protection des données.**

La grande majorité des Etats américains (42 sur 50) dispose de lois imposant de telles notifications. L'Etat de Californie a été pionnier en ce domaine dès 2002. L'objectif recherché est **d'inciter les entreprises à renforcer leurs mesures de sécurité interne**, car les notifications sont coûteuses et préjudiciables à leur image de marque.

Les dispositifs mis en place varient beaucoup d'un Etat à l'autre. Les délais des notifications, leur contenu, les moyens employés et les destinataires ne sont pas identiques. Ainsi, la notification peut se faire selon les cas par voie de presse, par écrit ou par voie électronique. Les délais varient aussi considérablement : soit immédiatement après la découverte de la faille, soit dans un délai raisonnable. Dans 25 Etats environ, la notification peut être reportée si une autorité policière décide que la notification risque d'empêcher ou de menacer une enquête criminelle.

Une conséquence de ces obligations de notification est une meilleure connaissance statistique de l'ampleur des failles de sécurité aux Etats-Unis. Ainsi, selon l'organisme *Internet Identity Theft Resource Center* (IRTC), en 2008, plus de 35 millions de données personnelles auraient été perdues, soit une hausse de 47 % par rapport à 2007.

En France, une telle obligation n'existe pas. L'article 4 de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des

communications électroniques[1] (ci-après dénommée directive « vie privée et communications électroniques ») contraint seulement les opérateurs de télécommunications à informer leurs abonnés en cas de risque particulier de violation de la sécurité des réseaux. Cette disposition doit notamment permettre aux abonnés de prendre leurs propres mesures de précaution.

Toutefois, dans le cadre de la réforme du « paquet télécom », la Commission européenne a présenté, le 13 novembre 2007, trois propositions de texte dont une proposition de directive modifiant la directive 2002/58/CE[2]. Le (3) de l'article 2 de cette proposition tend à obliger les responsables de traitement, « *en cas de violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés à des données personnelles* », d'avertir l'autorité administrative compétente et l'abonné concerné.

Compte tenu du champ de la directive « vie privée et communications électroniques », seuls les fournisseurs de services de communications électroniques accessibles au public (opérateurs mobiles, FAI, etc.) seraient concernés.

Le Contrôleur européen de la protection des données et le G 29[3] se sont déclarés très favorables à cette proposition. Allant plus loin, ils préconisent d'étendre cette obligation à « tous les prestataires de services en ligne » sur Internet[4]. Ils proposent également de permettre, dans certaines circonstances, à l'autorité administrative compétente[5] de divulguer l'information au public.

Le Sénat s'est également prononcé sur cette question en adoptant une résolution européenne en mai 2008[6] sur le rapport de la commission des affaires économiques. Dans son rapport[7], notre collègue Pierre Hérisson exprime plusieurs réserves : « *la proposition de la Commission d'obliger tout opérateur à notifier aux abonnés toute atteinte à leurs données personnelles, si elle peut contribuer à une meilleure transparence au profit des consommateurs, pourrait se révéler contre-productive en nourrissant l'inquiétude des consommateurs voire en provoquant des attaques pour tester la sécurité des réseaux. Sans doute serait-il donc préférable de prévoir l'accord préalable du régulateur national avant tout type de communication en matière de sécurité ou [...] de limiter l'information du consommateur aux seules atteintes à ses données personnelles qui seraient susceptibles de lui porter préjudice* ».

---

[1] Transposé à l'article D. 98-5 du code des postes et des communications électroniques.
[2] Document COM (2007) 698 final.
[3] Avis WP 150 du 15 mai 2008.
[4] Le Parlement européen a adopté des amendements en ce sens.
[5] En France, cette autorité ne serait pas la CNIL mais l'Autorité de régulation des communications électroniques et des postes (ARCEP). Toutefois, les négociations ont fait évoluer la proposition. Les autorités chargées de la protection des données seraient également associées.
[6] Résolution n° 96 (2007-2008).
[7] Rapport n° 349 (2007-2008).

Vos rapporteurs partagent ces réserves, notamment quant au risque que la notification d'une faille au public n'attise de nouvelles attaques.

Toutefois, l'éventail des solutions en vigueur aux Etats-Unis montre que le choix n'est pas entre tout ou rien.

Il faut d'ailleurs souligner que la loi du 6 janvier 1978 ouvre une fenêtre pour la publicité des failles de sécurité constatées par la CNIL à l'occasion de ses contrôles. En effet, son article 46 autorise la CNIL à « *rendre publics les avertissements qu'elle prononce. Elle peut également, en cas de mauvaise foi du responsable du traitement, ordonner l'insertion des autres sanctions qu'elle prononce dans des publications, journaux et supports qu'elle désigne. Les frais sont supportés par les personnes sanctionnées* ». A cet égard, vos rapporteurs estiment que **la publicité de ces sanctions devrait être désormais la règle** (cf. *supra*).

Il semble possible d'aller un peu plus loin en créant *a minima* **une obligation de notification des failles de sécurité à la CNIL**, des critères et des seuils devant être définis pour ne pas la submerger. Cette obligation pèserait sur tous les responsables de traitement.

Bien maîtrisée et encadrée, l'obligation de notification des failles de sécurité peut être **une incitation forte au renforcement de la sécurité des données.**

Recommandation n° 11 : Créer *a minima* une obligation de notification des failles de sécurité auprès de la CNIL.

c) Transférer à la CNIL l'autorisation et le contrôle des dispositifs de vidéosurveillance

Le groupe de travail de la commission des lois sur la vidéosurveillance a proposé dans son rapport de décembre 2008 de **rapatrier la vidéosurveillance dans le champ de la loi du 6 janvier 1978 et de la CNIL**.

Vos rapporteurs partagent ces conclusions à l'heure de la convergence numérique. En outre, les technologies étant de moins en moins utilisées isolément mais au contraire combinées entre elles –par exemple la biométrie avec la vidéosurveillance–, l'existence d'une législation unique reposant sur quelques principes est un facteur important de simplicité et de clarté de la loi.

Recommandation n° 12 : Réunir sous une seule autorité, la CNIL, les compétences d'autorisation et de contrôle en matière de vidéosurveillance.

d) Réserver au législateur la compétence exclusive en matière de fichiers de police

Les articles 26 et 27 de la loi du 6 janvier 1978 modifiée disposent que les fichiers intéressant la sûreté de l'Etat, la défense ou la sécurité publique, ou qui ont pour objet la répression des infractions pénales, **sont**

créés par arrêté du ministre compétent. En cas de recours à la biométrie, un décret en Conseil d'Etat est nécessaire. La CNIL rend un avis simple (voir *supra*).

Toutefois, en pratique, la création des fichiers de police est laissée au choix à la loi –le FNAEG par exemple– ou au pouvoir réglementaire[1].

Certains cas sont hybrides. La loi arrête le principe d'un fichier, parfois ses grandes lignes, et le décret précise les caractéristiques.

Cette confusion apparaît regrettable. Il semble légitime, compte tenu de l'importance de ces fichiers et des précautions qu'ils requièrent, **qu'ils ne puissent plus être autorisés que par la loi**. La loi du 6 janvier 1978 devrait être modifiée en conséquence.

Ils rejoignent très exactement sur ce point les conclusions des travaux de la mission d'information de la commission des lois de l'Assemblée nationale sur les fichiers de police[2].

Cette disposition règlerait les débats sur la perte d'influence de la CNIL. Qui, plus que le Parlement, est légitime à débattre de ces questions primordiales pour la protection de la vie privée ?

La CNIL ne serait pas absente pour autant. D'ores et déjà, elle rend un avis sur les projets de loi. Ceux-ci sont désormais publics depuis l'adoption de la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures. La publicité des avis de la CNIL sur les projets de loi a été introduite par le Sénat.

Recommandation n° 13 : Réserver au législateur la compétence exclusive pour créer un fichier de police.

Il reviendra alors à la représentation nationale de fixer l'équilibre entre les besoins de sécurité et le respect nécessaire de la vie privée.

Enfin, vos rapporteurs observent que le perfectionnement de certains fichiers ne signifie pas uniquement un accroissement des capacités de contrôle et de traçage des individus.

A cet égard, le projet ARIANE, qui se substituera aux deux fichiers STIC et JUDEX, se doit d'être exemplaire. Il faut attendre de la modernisation de ces deux fichiers un renforcement du traçage de leurs utilisateurs.

Comme il a été vu, ces fichiers sont insuffisamment mis à jour et se prêtent à des consultations qui ne correspondent pas aux finalités légales.

La modernisation des fichiers doit donc aussi permettre :

- des actualisations en temps réel et automatiques ;

---

[1] La mission d'information de la commission des lois de l'Assemblée nationale précitée a relevé que certains fichiers de police avaient été créés en dehors de tout texte.

[2] A la suite de cette mission, les deux rapporteurs ont déposé le 7 mai 2009 la proposition de loi n° 1659, dont l'article 5 tend à réserver à la loi la création de fichiers de police.

- une sécurisation des données ;

- une identification précise et certaine des personnes qui les consultent et de leurs motifs.

En effet, si nous le souhaitons collectivement, les progrès technologiques ne sont pas antinomiques d'un meilleur respect de la protection des données à caractère personnel.

3. Compléter les grands principes de la reconnaissance d'un droit à l'oubli

L'expansion de la sphère de la vie publique, l'immédiateté avec laquelle elle peut être portée à la connaissance de tous à tout moment et en tout point du globe grâce à Internet ne sont-ils pas autant d'éléments nouveaux qui finissent par en changer la nature et justifierait de lui appliquer des règles habituellement réservées à la protection de la vie privée ?

Le droit **à l'oubli** ou **au remord** a été évoqué de nombreuses fois lors des auditions. Pour Maître Alain Bensoussan, cette perte de mémoire a vocation à protéger l'individu par rapport à son passé : « *il devient le seul archiviste de son histoire personnelle* ».

Battu en brèche par la révolution numérique, le droit à l'oubli n'est pas absent de la loi « informatique et libertés ». L'obligation pour les responsables de traitements de ne pas conserver les données au-delà de la durée nécessaire aux finalités est la principale protection. Le droit à l'oubli est alors mis en œuvre par **la destruction des données** ou **une anonymisation irréversible**.

Toutefois, la législation relative à la protection des données personnelles devient **largement inopérante pour répondre aux défis posés par Internet et les moteurs de recherche** (cf. *supra*). Les questions en jeu sont moins celles de la protection des données personnelles que de l'équilibre entre le respect de la vie privée, du droit à l'oubli et la protection de la liberté d'expression et d'information. En outre, la défense d'un droit à l'oubli ne doit pas non plus aboutir à une déresponsabilisation des individus. Le droit à l'oubli ne signifie pas que chacun pourrait réécrire à sa guise son histoire personnelle.

Vos rapporteurs souhaitent donc réaffirmer ici que la première réponse consiste toujours à bien peser les avantages et les risques consécutifs à la mise en ligne d'une information, privée ou publique. Cela passe par l'éducation et la sensibilisation aux risques comme cela a été développé précédemment.

Il ne faut d'ailleurs pas exclure une évolution naturelle des comportements dans un sens qui permette de préserver les nouvelles opportunités d'expression et d'information sur Internet, notamment celles offertes par les réseaux sociaux, et une utilisation responsable et respectueuse d'autrui.

L'apparition des réseaux sociaux est encore très récente. Comme pour tout nouvel outil, il existe **un temps d'apprentissage**. Depuis plusieurs mois, les exemples de mésaventures se multiplient. Les travaux de Dominique Cardon montrent que « *les usagers des plateformes relationnelles, même s'ils ont une vue imparfaite de l'ensemble des conséquences possibles de leurs actes, mesurent en revanche constamment, par un processus d'essais/erreurs, les gênes, troubles, audaces, amusements ou frottements que peut faire naître la visibilité particulière que leur donne les réseaux sociaux* ». **On peut donc parier que les comportements et stratégies vont encore beaucoup évoluer**.

En février dernier, les réactions consécutives à l'annonce par Facebook de sa décision de modifier ses conditions générales d'utilisation afin de se rendre propriétaire à vie des données figurant sur ses pages montrent que les utilisateurs sont très sensibles au respect de la vie privée, même si leur comportement pourrait laisser penser le contraire.

Il n'est pas impossible aussi que la jurisprudence de la Cour de cassation précise certaines ambiguïtés des réseaux sociaux. Est-ce un espace public ou privé ? Rigoureusement, les réseaux sociaux ne sont pas publics, puisqu'il faut, dans la plupart des cas, être membre pour y accéder[1]. C'est un espace en clair-obscur comme cela a été dit, plastique et paramétrable. Toutefois, lorsqu'un réseau social possède plusieurs dizaines de millions de membres et que par un jeu de contagion, le cercle de ses « Amis » et « Amis d'Amis » s'accroît considérablement, est-on encore dans un cercle privé ? Certaines personnalités détournent ainsi les réseaux sociaux de leur usage premier à des fins de communication publique affichée. Lors de la campagne présidentielle américaine en 2008, le président Barack Obama avait développé une stratégie de communication et de dialogue autour de son profil sur Facebook.

La Cour de cassation n'a pas encore eu à se prononcer. Mais elle sera probablement conduite à préciser dans quelle mesure les échanges sur les réseaux sociaux sont assimilables à une correspondance privée ou à une communication.

Une communication peut se définir comme la mise à disposition au public d'un message. Elle s'oppose à la correspondance privée, dont la violation du secret est sanctionnée pénalement. La distinction se fonde sur l'intention de la personne qui émet le message : le met-elle à la disposition du public ou le destine-t-elle à une ou plusieurs personnes nommément désignées ? Pour déterminer le caractère public ou non, le juge vérifie si la diffusion est circonscrite à un groupement de personnes « *liées par une communauté d'intérêts* »[2].

Appliquée aux réseaux sociaux, cette notion peut être interprétée de diverses façons. Un message pourrait être considéré comme une correspondance privée à plusieurs conditions : ne pas avoir trop d'« amis »,

---

[1] *Sur Facebook, il est possible d'autoriser l'accès libre à son profil.*
[2] *Voir par exemple Cass. crim. 27 mai 1999. n° 98-82461.*

activer les options limitant l'accès des « amis d'amis » à ce message. En tout état de cause, si le régime protecteur du secret de la correspondance s'appliquait à une partie des réseaux sociaux, cela constituerait une garantie importante et permettrait à chacun d'arbitrer entre son désir d'exposition et son besoin de confidentialité.

Toutefois, il convient de ne pas se leurrer. Les réseaux sociaux ne sont qu'une infime partie de la question et on voit mal comment le secret de la correspondance pourrait être applicable à d'autres domaines de « la toile ».

D'autres stratégies et concepts doivent être mis en place pour reconstituer une maîtrise de chacun sur son histoire numérique.

a) La notion de droit de propriété sur ses données personnelles : une fausse bonne idée

A plusieurs reprises, la reconnaissance d'un droit de propriété sur ses données personnelles a été avancée. L'idée, séduisante, serait de faire de chaque individu le véritable maître de son identité numérique. Chacun pourrait gérer ses données en les louant, prêtant, récupérant, etc.

Toutefois, **le concept de propriété n'apporte pas de réponses adéquates** et pourrait poser plus de problèmes encore.

Notre conception de la vie privée place sa protection sur le terrain de la dignité humaine. En se référant au concept de propriété, **le risque de marchandisation** de ses données personnelles est évident. La propriété comprend aussi le droit de céder la chose. Or, comment pourrait-on céder une donnée qui peut aussi être un attribut de sa personnalité ? Faut-il imaginer des droits d'exclusivité ?

Il pourrait être objecté que le droit à l'image est d'ores et déjà un droit patrimonial et peut donner lieu à l'établissement de contrats.

Mais ce régime juridique est inadapté aux enjeux d'Internet. Comment y faire valoir ses droits de propriété quand on a soi-même diffusé une donnée personnelle ? Quant aux informations relatives à sa vie publique, il ne peut être question d'un droit de propriété à moins de remettre en cause fondamentalement la liberté d'expression.

Enfin, lorsque le rapport de force entre des contractants est inégal, quelle valeur donner au consentement à contracter ?

b) Brouiller les pistes

A une époque où les risques d'usurpation d'identité sont souvent pointés du doigt et où les Etats renforcent les moyens d'identification des personnes (avec la biométrie par exemple), les réflexions ci-dessous peuvent surprendre.

Mais, face aux nouveaux défis posés au droit à la vie privée ou à une « vie publique discrète », les solutions traditionnelles ne semblent pas à la hauteur pour rendre aux individus des marges de manœuvre.

Sans se prononcer pour ou contre à ce stade, vos rapporteurs jugent intéressantes **les réflexions autour d'un droit à l'« hétéronymat ».**

Chaque individu pourrait se forger de véritables personnalités alternatives, distinctes de la personnalité civile qui les exploite. Afin d'éviter que ce droit ne serve à commettre des infractions, ces identités alternatives pourraient être déposées auprès d'un organisme chargé de les gérer. En cas d'infractions par exemple, la justice pourrait demander l'identité civile de la personne.

Mis en avant notamment par M. Daniel Kaplan, délégué général de la Fondation pour l'Internet Nouvelle génération (FING)[1], ce droit s'inspire de stratégies déjà utilisées par de nombreux internautes. Mais ayant une forme de reconnaissance légale, ce droit permettrait de faire beaucoup plus de choses anonymement, comme des achats en ligne, sans que cela puisse être reproché à la personne.

Peuvent être rattachés à cette stratégie de brouillage des pistes tous les dispositifs tendant à permettre l'anonymat sur Internet ou à réduire la liste des données communiquées. C'est le cas notamment des « payweb card » proposés par les banques. Ce service consiste à délivrer un numéro de carte virtuel différent pour chaque paiement en ligne. De cette façon, le numéro de carte bancaire n'est pas communiqué.

c) Vers un droit à l'oubli…

Vos rapporteurs sont conscients que ces solutions sont imparfaites et partielles. Se pose donc la question de **la reconnaissance d'un droit à l'oubli qui permettrait à une personne de retirer de « la toile » des informations publiques la concernant** et dont elle souhaite ne plus permettre la consultation.

Comme il a été dit, la difficulté est de trouver un équilibre entre le droit à l'oubli et la liberté d'expression et d'information.

---

[1] Créée en 2000 par une équipe d'entrepreneurs et d'experts, la Fing a pour objet de repérer, stimuler et valoriser l'innovation dans les services et les usages du numérique. La Fing compte aujourd'hui plus de 160 membres, parmi lesquels on compte des grandes entreprises, des start-ups, des laboratoires de recherche, des universités, des collectivités territoriales, des administrations, des associations….
Dans un article récent, Daniel Kaplan propose d'autres droits comme le droit à l'anonymat, le droit au mensonge légitime ou le droit à récupérer ses données. Ces propositions relèvent plutôt du débat sur la protection des données personnelles au sens de la loi du 6 janvier 1978. Cet article intitulé « Le nouveau paysage des données personnelles : quelles conséquences sur les droits des individus » est consultable à l'adresse suivante : http://www.internetactu.net.

(1) … des atteintes diffamatoires et injurieuses

Les diffamations publiques, les injures et les provocations envers des particuliers se prescrivent par trois mois. Ce délai expiré, aucune action n'est possible.

Or, une diffamation publique proférée envers un particulier peut avoir été publiée sur un support écrit (un journal ou un livre) tout en passant inaperçue de l'intéressé. Le temps, à l'égard du papier, fait son office. Mais par le biais d'Internet, le vieux journal ou le livre oublié demeurent mondialement accessibles pendant des années.

En l'état actuel du droit, il paraît impossible d'obtenir la suppression d'une très ancienne diffamation qui bénéficie de la prescription de trois mois depuis bien longtemps.

Il en va de même pour les diffamations diffusées directement sur Internet. On notera toutefois que le Sénat a adopté en novembre 2008 une proposition de loi de notre collègue Marcel-Pierre Cléach tendant à porter le délai de prescription à un an lorsque la diffamation, l'injure ou la provocation a été commise par l'intermédiaire d'Internet, sauf s'il s'agit de la reproduction du contenu d'une publication de presse ou d'une émission audiovisuelle[1]. Cette proposition de loi n'a pas encore été examinée par l'Assemblée nationale.

Afin de permettre la suppression de faits diffamatoires sur Internet, sans remettre en cause les délais de prescription traditionnellement courts de cette infraction, Maître Christian Charrière-Bournazel, bâtonnier de Paris, a exposé à vos rapporteurs une solution intéressante.

Il serait créé **une action en suppression d'une imputation diffamatoire**, ouverte à toute personne concernée, sans limitation dans le temps. Cette action n'aurait pour effet ni de faire revivre le droit, désormais prescrit, à solliciter une réparation, ni de permettre une condamnation pour diffamation, ni de mettre en échec la liberté d'expression.

Une diffamation poursuivie dans le délai de prescription peut être justifiée ou excusée si le diffamateur, dans les conditions prévues par la loi du 29 juillet 1881, rapporte la preuve de la vérité des propos diffamatoires ou réussit à prouver qu'il était de bonne foi.

L'action en suppression répondrait aux mêmes exigences que l'action intentée dans le délai de la prescription et bénéficierait des mêmes moyens de défense. La suppression ne serait pas acquise si la diffamation n'est pas constituée. En revanche, si elle l'est, la suppression serait de droit tout en constituant la seule mesure que le juge aurait le droit d'ordonner.

---

[1] *Voir le rapport n° 60 (2008-2009) de notre collègue Marie-Hélène Des Egaulx au nom de la commission des lois.*

(2) … général, y compris des faits portés à la connaissance du public par l'intéressé ?

Ne devrait-il pas exister un « droit à l'oubli » pour les internautes, quand bien même ceux-ci auraient souhaité, à un moment donné de leur vie, se « mettre à nu » sur le web ?

La prise en compte des différences d'accessibilité d'un message dans le temps, selon qu'il est publié sur support papier ou disponible sur un support numérique, pour reprendre les mots du Conseil constitutionnel dans sa décision du 10 juin 2004 relative à la loi pour la confiance dans l'économie numérique, plaiderait en faveur d'une telle solution. **Ce droit à l'oubli pourrait s'exercer devant le juge à tout moment.** Le demandeur démontrerait par exemple que les faits ou les propos rapportés ne correspondent plus à son mode de vie ou à ses opinions et qu'ils lui causent un préjudice dans sa vie familiale ou professionnelle.

Il appartiendrait au juge d'apprécier si la demande de retrait porte atteinte à la liberté d'expression. L'intérêt de l'information pour le public, son ancienneté et la notoriété de la personne seraient des critères.

A propos de la mise en œuvre d'une telle décision, deux voies concurrentes doivent être envisagées.

La première consisterait à demander le retrait de l'information du site proprement dit. Toutefois, plusieurs obstacles se dressent. La page peut être hébergée à l'étranger et l'information étant duplicable, elle est susceptible de resurgir.

La seconde pourrait consister à empêcher les moteurs de recherche d'indexer les pages contenant l'information non désirée.

Cette solution a pour avantage d'être plus respectueuse de la liberté d'expression. L'information n'est pas retirée, mais les conditions pour y accéder sont rendues plus difficiles. Elles se rapprochent de celles du monde physique.

Elle est aussi plus aisée à mettre en œuvre. Certes, il existe plusieurs moteurs ou méta-moteurs de recherche, mais les principaux ne sont pas si nombreux. En outre, par le biais des moteurs de recherche, en cas de résurgence de l'information, quelle que soit la page, celle-ci ne sera pas indexée.

Enfin, on pourrait même imaginer que l'intervention du juge ne soit pas nécessaire, puisqu'il n'y aurait pas d'atteinte à la publication elle-même.

Les moteurs de recherche pourraient mettre à disposition des utilisateurs identifiés des outils qui leur permettraient, même d'une manière imparfaite, de « nettoyer leur passé » en coupant certains liens issus du référencement.

Recommandation n° 14 : Réfléchir à la création d'un droit à « l'hétéronymat » et d'un droit à l'oubli.

4. Une mesure symbolique forte : l'inscription du droit au respect de la vie privée dans la Constitution

Compte tenu des risques et des enjeux précédemment identifiés, il pourrait être intéressant de revenir sur une idée écartée par le comité présidé par Mme Simone Veil : l'inscription du droit au respect de la vie privée dans notre Constitution.

Par lettre datée du 9 avril 2008, le Président de la République a confié à Mme Simone Veil la présidence d'un comité de réflexion chargé de s'interroger sur l'opportunité de compléter les droits fondamentaux reconnus par la Constitution de principes nouveaux, et, le cas échéant, de proposer un texte correspondant à ses préconisations. Dans leur rapport, remis le 17 décembre 2008 au chef de l'Etat, les membres du comité, après avoir entendu un grand nombre de personnalités, se sont déclarés défavorables à une révision du Préambule de notre Constitution.

En ce qui concerne plus particulièrement la question de la reconnaissance du respect de la vie privée et de la protection des données personnelles, le comité a choisi de ne pas recommander l'inscription de ces deux notions dans le Préambule :

- D'une part, **le comité a observé que le droit au respect de la vie privée comme celui à la protection des données à caractère personnel étaient déjà consacrés**, non par le texte même de la Constitution ou de son Préambule, mais **par deux sources de droit qui s'imposent au législateur : la jurisprudence du Conseil constitutionnel d'une part, les engagements internationaux auxquels la France est partie d'autre part** (voir *supra*). Le comité est ici resté fidèle à la doctrine de l'effet utile qu'il s'était donnée comme principe et selon laquelle l'inscription d'un principe dans le Préambule ne doit être recommandée que pour autant qu'elle constitue une véritable innovation ou apporte une garantie des droits sensiblement supérieure.

- D'autre part, le comité a fait valoir que les contraintes propres au processus de révision de la Constitution et de son Préambule pouvaient se révéler inadaptées à certains domaines ou à certaines matières, particulièrement sensibles **à une exigence d'adaptabilité de la règle de droit :** de ce point de vue, le comité a considéré que **la loi était mieux adaptée pour suivre, avec une réactivité suffisante, l'évolution des techniques.**

Le comité en a conclu que, considérant l'environnement constitutionnel et international préexistant, la voie législative et jurisprudentielle demeurait la plus efficiente pour assurer le *réglage fin* de la protection de la vie privée et des données à caractère personnel, et qu'il était préférable de confier au législateur la tâche d'épouser l'évolution des sciences et des techniques et d'assurer, sous le contrôle du juge, la conciliation nécessaire des intérêts et des droits en présence.

Ce faisant, le comité a choisi de ne pas retenir les propositions formulées par M. Alex Türk, président de la CNIL, lors de son audition par les membres du comité le 25 mai 2008[1]. Ce dernier avait alors fait valoir que notre sphère privée était aujourd'hui exposée à des risques sans précédents, causés par l'accélération des progrès technologiques et leur diffusion dans un cadre globalisé ainsi que par la recherche d'une sécurité collective toujours plus infaillible. Dans ce contexte, **M. Türk avait estimé qu'il serait à la fois logique et pertinent de reconnaître de manière explicite dans notre Constitution le droit au respect de la vie privée et à la protection des données**, dont le Conseil constitutionnel avait fait un principe de référence de sa jurisprudence et dont un nombre croissant d'Etats européens reconnaissaient aujourd'hui la valeur constitutionnelle.

Vos rapporteurs ont suivi avec beaucoup d'attention ce débat et souhaitent faire valoir les arguments suivants :

- D'une part, comme ils l'ont exprimé précédemment, **ils ont acquis la conviction qu'en ce qui concerne la conciliation entre développement technologique et droits au respect de la vie privée et à la protection des données, ni la loi, ni *a fortiori* la Constitution ne devraient contenir de dispositions trop rigides, qui risqueraient de se retrouver rapidement dépassées par le développement technologique et d'entraver ce dernier, sinon de rester inappliquées.**

- D'autre part, il leur a semblé évident qu'à l'heure où le développement technologique suscite, à juste titre, des craintes de voir se multiplier et s'amplifier les risques d'atteintes à la vie privée, **l'inscription de cette notion dans le cœur de notre texte constitutionnel aurait valeur de symbole fort.**

A cet égard, vos rapporteurs ne considèrent pas pour leur part qu'il serait utile d'inscrire dans notre Constitution à la fois le principe de respect de la vie privée et le droit à la protection des données à caractère personnel : **pour vos rapporteurs, le droit à la protection des données à caractère personnel doit être regardé comme une déclinaison du principe de respect de la vie privée**, et non comme un droit autonome et spécifique dont la reconnaissance devrait être élevée au niveau constitutionnel.

Ce faisant, ils rejoignent les arguments développés par les professeurs Yves Poullet et Antoinette Rouvroy dans un article consacré à « l'auto-détermination en tant que concept-clé »[2], lesquels font valoir les éléments suivants : « *en plaçant le droit à la protection des données au même niveau que le droit au respect de la vie privée, ne risque-t-on pas d'atténuer l'intelligibilité des fondements des régimes de protection des données – la*

---

[1] *Son intervention est reproduite en annexe du rapport du comité, lequel est disponible en accès libre sur le site Internet de la Documentation française.*

[2] *En cours de publication.*

dignité et l'autonomie individuelle – et de rendre de ce fait plus difficile la tâche du législateur lorsqu'il aura à évaluer et, éventuellement, à revoir les instruments de protection des données au vu des évolutions socio-politiques et technologiques de la société de l'information ? [...] Faire du « droit à la protection des données » un droit fondamental distinct entraîne un autre inconvénient. En effet, cela risque d'atténuer le lien essentiel existant entre le respect de la vie privée et la protection des données et de détacher ainsi la protection des données des valeurs fondamentales de dignité humaine et d'autonomie individuelle, valeurs fondatrices du concept de respect de la vie privée, dans lesquelles les régimes de protection des données trouvent leurs racines ».

En revanche, vos rapporteurs ont acquis la conviction qu'**une reconnaissance de la notion de respect de la vie privée par notre Constitution,** au même titre que la liberté, l'égalité ou la laïcité, **complèterait de façon pertinente notre Loi fondamentale dans un sens conforme aux principes fondateurs de notre ordre politique.**

A cet égard, vos rapporteurs tiennent à rappeler que **la reconnaissance de la notion de respect de la vie privée figurait dans le projet de loi constitutionnelle portant révision de la Constitution du 4 octobre 1958 et relatif à l'organisation des pouvoirs publics adopté en Conseil des ministres le 10 mars 1993.** Ce projet avait été déposé sur le Bureau du Sénat mais n'avait jamais été inscrit à l'ordre du jour par le Gouvernement issu des élections de mars 1993. Or, ce projet de loi constitutionnelle prévoyait **d'inscrire expressément la notion de respect de la vie privée dans le texte de l'article 1er de notre Constitution[1].**

A l'heure où le développement des nouvelles technologies soumet la notion de respect de la vie privée à un certain nombre de défis, vos rapporteurs considèrent que la reprise d'une telle disposition parait essentielle.

Recommandation n° 15 : Inscrire dans notre texte constitutionnel la notion de droit au respect de la vie privée.

*

* *

[1] *Le projet de loi constitutionnelle prévoyait de compléter l'article 1er de la Constitution par la phrase suivante : « Elle [la France] assure le respect de la vie privée et de la dignité de la personne ».*

Au cours de leur réflexion, probablement parce qu'ils étaient chaque jour plus avertis des évolutions technologiques et de leur impact sur la vie privée des consommateurs et utilisateurs d'Internet, vos rapporteurs ont mesuré l'absolue nécessité d'encadrer plus strictement l'utilisation des outils numériques.

Sans nier ni rejeter en aucune façon ces outils dont l'existence et le développement sont incontournables et, au demeurant, porteurs de progrès, ils se sont attachés à relever l'extrême vigilance qui doit accompagner leur évolution dans un contexte non seulement national mais international.

La mondialisation actuelle des flux d'informations emporte l'obligation d'une harmonisation des politiques et des procédures en la matière, dans le respect absolu des principes fondateurs de la protection des données personnelles.

L'enjeu primordial de ce nouveau siècle est bien celui du respect de la dignité humaine.

Réunie le mercredi 27 mai 2009, la commission a autorisé la publication du présent rapport.

EXAMEN EN COMMISSION
MERCREDI 27 MAI 2009

_____

Mme Anne-Marie Escoffier et M. Yves Détraigne ont tout d'abord présenté les grandes orientations de leur rapport d'information. Ils ont précisé que les travaux du groupe de travail les avaient conduits à préférer à la notion de traçage électronique celle de mémoires numériques. En conséquence, ils ont proposé de dénommer le groupe de travail, créé le 22 octobre 2008, relatif au traçage électronique et à la protection de la vie privée « *groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques* ». La commission en a ainsi décidé.

Un débat s'est engagé à l'issue de cette présentation.

M. Alex Türk s'est félicité de la constitution de ce groupe de travail, illustrant une nouvelle fois la prise de conscience, par le Parlement, des enjeux « informatique et libertés » depuis quelques années.

Il a souligné :

- que la loi du 6 août 2004 avait profondément transformé les missions de la CNIL, relevant que 90 % de son activité était désormais tournée vers le secteur privé ;

- qu'il était particulièrement difficile de sensibiliser les jeunes à la nécessité de préserver leur intimité même si, comme ils le disent, « ils n'ont rien à cacher » ;

- que le ministère de l'éducation nationale n'avait pas encore pris la mesure des nouveaux risques d'atteinte à la vie privée et, en conséquence, n'avait pas intégré cette dimension dans l'enseignement ;

- que la CNIL, à la différence de son homologue britannique, n'avait pas les moyens budgétaires de lancer de vastes campagnes d'information pour sensibiliser la population aux nouveaux enjeux « informatique et libertés » ;

- que les membres des réseaux sociaux devaient en être regardés comme des consommateurs, ce afin de leur garantir une plus grande protection ;

- que le législateur avait opportunément permis, dans la dernière loi de simplification du droit, le lancement effectif de la labellisation des produits ou procédures offrant des garanties renforcées en matière de protection des données personnelles, démarche attendue depuis la loi du 6 août 2004 ;

- que le Gouvernement était aujourd'hui réservé quant à l'idée d'asseoir le financement de la CNIL sur une redevance, craignant qu'elle ne

soit perçue comme un impôt supplémentaire, alors même qu'elle ne viendrait que se substituer à la dotation prévue dans le budget de l'Etat ;

- qu'il était nécessaire de déconcentrer les moyens de la CNIL par la création d'antennes interrégionales qui permettraient notamment de mieux répartir ses contrôles sur l'ensemble du territoire ;

- qu'il était important de ne pas céder à la pression du Royaume-Uni concernant la révision de la directive de 1995, qui ne devait pas, selon lui, être envisagée à court terme ;

- qu'il était essentiel de travailler à l'élaboration de normes internationales dans le domaine de la protection des données, soulignant que les Etats-Unis d'Amérique et l'Asie étaient nettement en dessous du niveau de protection garanti en Europe par la directive de 1995, ajoutant que la France, forte de ses collectivités outre-mer dans le Pacifique, pouvait jouer un rôle d'influence important au sein de la Coopération économique pour l'Asie-Pacifique (APEC) ;

- qu'il était en effet opportun de clarifier le statut de l'adresse IP ;

- qu'il regrettait que le Gouvernement ait considéré que la CNIL n'était pas compétente pour se prononcer sur le volet « vidéosurveillance » du projet de loi d'orientation et de programmation pour la sécurité intérieure, qui sera prochainement soumis au Parlement ;

- qu'il était favorable à la constitutionnalisation de la protection de la vie privée et des données personnelles, afin d'inscrire dans la loi fondamentale des principes généraux qui s'imposent au législateur ;

- que la recommandation des rapporteurs concernant la compétence législative en matière de fichiers de police, inscrite dans la proposition de loi des députés, Mme Delphine Batho et M. Jacques Alain Benisti, posait une question importante et complexe.

M. Patrice Gélard a souligné que le Comité Veil chargé de réfléchir à l'opportunité de compléter le préambule de la Constitution par des principes nouveaux comité dont il était membre avait décidé, après une longue réflexion, de ne pas consacrer dans le préambule le droit à la vie privée, considérant, d'une part, que ce droit, reconnu par le Conseil constitutionnel et garanti par les engagements internationaux de la France, avait déjà valeur supra-législative, d'autre part, qu'il était préférable de laisser au législateur le soin de définir cette notion aux contours imprécis et évolutifs.

M. Simon Sutour a approuvé les conclusions des rapporteurs, en particulier celle tendant à constitutionnaliser le droit à la vie privée, gage selon lui d'une plus grande protection et celle réservant au législateur la compétence pour les fichiers de police, dont il a dénoncé au passage la médiocre actualisation, illustrée par certaines affaires récentes. Il a enfin regretté que la France ait été, en 2004, un des derniers pays à transposer la directive de 1995 sur la protection des données personnelles.

Après avoir salué la grande qualité du travail des rapporteurs, M. Jean-Pierre Sueur s'est demandé si la réunion sous une seule autorité, la CNIL, des compétences d'autorisation et de contrôle en matière de vidéosurveillance, proposée par les rapporteurs, permettrait de mieux garantir en pratique le droit de consultation des images aujourd'hui non effectif. Par ailleurs, il a jugé étonnant que la directive de 1995 ait admis, dans certaines conditions, l'applicabilité du droit du pays où se trouve la société, quand bien même celle-ci proposerait des services à des utilisateurs situés en Europe, relevant qu'il suffisait alors que les sociétés s'installent dans un pays dépourvu de réglementation en matière de protection des données pour échapper à toute contrainte en la matière. Enfin, il s'est demandé si la recommandation concernant l'« hétéronymat » n'était pas contraire aux principes de clarté et de transparence des débats sur Internet, principes en vertu desquels, par exemple, les auteurs de propos injurieux ou diffamatoires doivent assumer nominativement leurs actes pour pouvoir en répondre le cas échéant.

Après avoir rappelé que le Sénat avait adopté, en novembre 2008, une proposition de loi de M. Marcel-Pierre Cléach tendant à porter le délai de prescription à un an lorsque la diffamation, l'injure ou la provocation ont été commises par l'intermédiaire d'Internet et avoir déploré que cette proposition reste en instance à l'Assemblée nationale, M. Jean-Jacques Hyest, président, a souligné que l'emploi de pseudonymes n'empêchait pas les services de police ou de gendarmerie de retrouver les auteurs véritables de ces infractions.

M. Richard Yung s'est étonné que le Royaume-Uni, patrie de la démocratie, développe autant certaines technologies intrusives, telles que la vidéosurveillance et que, de même, les Etats-Unis, historiquement attachés à la protection des libertés, acceptent aussi facilement, depuis les attentats du 11 septembre 2001, de sacrifier celles-ci sur l'autel de la lutte contre le terrorisme. Il a approuvé les recommandations des rapporteurs, notamment celles qui concernent le renforcement général des pouvoirs de la CNIL, la compétence de cette dernière en matière de vidéosurveillance et la constitutionnalisation du droit à la vie privée, soulignant que cette dernière recommandation avait au moins le mérite de souligner la nécessité, pour le Parlement, d'engager un débat sur les conclusions du Comité Veil relatives à cette question essentielle.

M. Jean-Jacques Hyest, président, a souligné que certaines recommandations des rapporteurs pourraient être traduites en amendements à certains textes de loi, citant le projet de loi d'orientation et de programmation pour la sécurité intérieure.

M. Alain Anziani s'est déclaré sceptique sur la possibilité de parvenir un jour à l'élaboration d'un cadre juridique international en matière de protection des données. Il s'est par ailleurs demandé pourquoi la directive de 1995 n'avait pas fait le choix de prévoir, conformément aux règles du droit commun, l'application du droit communautaire aux services accessibles en Europe, quelle que soit leur provenance. Il a mis en avant la nécessité

d'informer la population des différents moyens permettant de se protéger des techniques intrusives, citant la suppression des « cookies » par l'utilisateur lui-même pour éviter la publicité ciblée.

Après avoir salué la qualité du travail des rapporteurs, M. Jacques Mézard a jugé insuffisante l'information délivrée par certains acteurs d'Internet concernant les caractéristiques du traitement des données effectué, telles que sa finalité ou encore la durée de conservation des données.

M. Yves Détraigne, co-rapporteur, a souligné la nécessité pour l'école de sensibiliser les jeunes générations aux risques présentés par les nouvelles technologies au regard du droit à la vie privée. Il a relevé que cette démarche d'information ne devait pas être menée exclusivement par l'école, saluant, à titre d'exemple, l'action de l'association espagnole dénommée Comisión de Libertades e Informática (commission des libertés et de l'informatique).

En réponse à M. Patrice Gélard, Mme Anne-Marie Escoffier, co-rapporteur a souligné que le rapport ne préconisait pas la constitutionnalisation de la protection des données personnelles, comme M. Alex Türk, entendu en qualité de président de la CNIL, l'avait souhaité lors son audition par le Comité Veil, mais celle du droit à la vie privée, notion plus large. En outre, elle a indiqué que de nombreux pays européens avaient élevé au niveau constitutionnel une telle protection. Elle a enfin estimé que la reconnaissance d'un droit à l'oubli, qui permettrait à une personne de retirer d'Internet des informations publiées la concernant et dont elle souhaite ne plus permettre la consultation, pouvait, au regard des nouveaux enjeux liés à Internet, constituer une réponse plus intéressante que la consécration d'un droit de propriété sur ses données personnelles voire d'un droit à « l'hétéronymat ».

M. Alex Türk a relayé le souhait de nombreux enseignants de disposer d'outils pédagogiques adéquats pour présenter à leurs élèves les nouveaux risques d'atteinte à la vie privée.

M. Pierre-Yves Collombat s'est inquiété de l'alourdissement régulier des tâches supportées par les enseignants.

M. Jean-Jacques Hyest, président, a exprimé certaines réserves concernant la recommandation relative à la compétence du législateur en matière de fichiers de police.

A l'issue de ce débat, M. Jean-Pierre Sueur ayant particulièrement marqué l'intérêt d'une large diffusion des travaux menés par les co-rapporteurs, la commission a autorisé la publication du rapport d'information.

ANNEXES

_____

ANNEXE 1

GLOSSAIRE

_____

Adresse IP (Internet Protocol)

Adresse, formée de plusieurs chiffres, qui permet aux ordinateurs connectés au réseau Internet d'être identifiés.

Bluetooth

Norme de communication qui permet de relier deux appareils par une connexion radio dans un rayon de 10 à 100 m.

Collecte déloyale de données personnelles

Collecte effectuée à l'insu des personnes.

Cookie

Petit fichier envoyé par un gestionnaire de site Internet sur le disque dur de l'utilisateur permettant d'identifier celui-ci lors de sa connexion au site et de mémoriser celle-ci.

Correspondants informatique et libertés

Institués en 2004, les correspondants informatique et libertés sont des personnes nommées au sein des entreprises et des administrations pour agir comme relais de la CNIL et se porter garants du respect de la loi « informatique et liberté » de 1978. En contrepartie, les structures qui désignent un tel correspondant ne sont pas tenues d'adresser leurs déclarations à la CNIL car le correspondant recense ces fichiers. Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à autorisation et continuent de faire l'objet de formalités**.**

Cryptage

Technique qui assure la confidentialité des données en les traduisant sous une forme codée et qui ne devient intelligible qu'avec la connaissance de la méthode de codage utilisée. On parle de chiffrement lorsque les données sont converties par un algorithme en une suite de caractères incompréhensibles.

Donnée biométrique

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

Donnée personnelle

Information identifiant directement ou indirectement une personne physique (par exemple, nom, numéro d'immatriculation, numéro de téléphone, photographie, date de naissance, empreinte digitale, etc.).

Donnée sensible

Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. Les traitements sur de telles données ne peuvent être mis en œuvre qu'après une autorisation de la CNIL et ne peuvent, en principe, être recueillis qu'après le consentement explicite des personnes.

Droit d'accès

Droit pour toute personne de prendre connaissance de l'intégralité des données la concernant dans un fichier, soit en s'adressant directement à ceux qui le détiennent (droit d'accès direct) soit en demandant que la CNIL vérifie les renseignements dans les fichiers intéressants la sûreté de l'Etat et la Défense (droit d'accès indirect).

Droit à l'information

Droit pour toute personne d'être informée de la mise en œuvre d'un traitement de données à caractère personnel, de l'identité du responsable de traitement, 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 ainsi que des éventuels transferts de données vers un pays hors de l'Union Européenne.

Droit d'opposition

Droit pour toute personne de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et de refuser, sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale.

Droit de rectification

Droit pour toute personne de 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.

Finalité d'un traitement

Objectif principal d'une application informatique de données personnelles, par exemple : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux…

Forum de discussion

Service permettant l'échange et la discussion sur un sujet donné, l'ensemble des contributions étant accessibles à tous et chacun pouvant apporter son commentaire. Il existe la plupart du temps un modérateur chargé d'éviter les débordements et notamment que ce lieu virtuel de discussion ne serve à la diffamation.

Fournisseur d'accès à Internet (FAI)

Intermédiaire entre l'internaute et le réseau Internet. Les principaux fournisseurs d'accès à Internet en France sont Orange, Neuf-Cegetel, Free et Numericable. Il attribue l'adresse IP et est soumis à des obligations en matière de conservation des données de connexion.

Géolocalisation

Technologies permettant la localisation précise d'un individu, en particulier à partir des téléphones portables et des systèmes de navigation GPS.

G29

Groupe de travail européen, créé par l'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation, rassemblant les représentants de vingt-sept autorités indépendantes de protection des données nationales.

Moteurs de recherche

Service proposé aux internautes leur permettant de trouver les sites correspondant aux mots clés qu'ils ont sélectionnés (sorte d'annuaire). Les plus connus sont Google, Yahoo et Microsoft. Ces services archivent les références des pages web et « indexent » les pages des différents sites, c'est-à-dire qu'ils leur associent des mots clés afin de permettre aux internautes de les localiser plus facilement.

Nanotechnologie

Technologie fondée sur l'étude, la fabrication et la manipulation de structures, de dispositifs et de systèmes matériels à l'échelle du nanomètre, c'est-à-dire du milliardième de mètre (ou du millionième de millimètre).

Opt in / Opt out

Désigne deux modalités de mise en œuvre du consentement.

- L'« *opt out* » désigne la possibilité offerte à l'utilisateur d'un logiciel ou d'un service sur Internet de ne pas participer à une collecte de données personnelles. Il s'agit *a priori* de l'option la moins protectrice de la vie privée, puisque, par défaut, l'individu est supposé consentir à la collecte de ses données.

- L'« *opt in* », plus protectrice en termes de respect de la vie privée, désigne la possibilité offerte à ce même utilisateur de participer, au cas par cas, à la collecte de ses données. En pratique, la mise en œuvre d'une telle option peut néanmoins s'avérer parfois contraignante.

Réseaux sociaux

Communauté d'individus en relation directe ou indirecte sur Internet. Les plus connus en France sont Facebook, My Space, Copains d'avant et LinkedIn.

Responsable du fichier

Personne physique ou morale qui détermine les finalités et les moyens de toute opération (collecte, enregistrement, modification ...), appliquée à des données à caractère personnel.

RFID (Radio Frequency Identification)

Technologie qui permet d'identifier et de localiser sans contact des objets ou des personnes grâce à une micropuce (également dénommée étiquette ou tag) qui dialogue par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à une dizaine de mètres.

Serveur

Ordinateur qui héberge des informations consultables à distance quand d'autres ordinateurs se connectent à lui.

Traitement de données

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

ANNEXE 2

LISTE DES PERSONNES ENTENDUES PAR LES RAPPORTEURS

_____

INSTITUTIONNELS

● **CNIL**

- M. Alex Türk, *président*

● **Ministère de l'Education nationale**

- Mme Catherine Gabay, *conseiller technique*

- M. Jean-Yves Capul, *sous-directeur des technologies de l'information et de la communication pour l'éducation*

- M. Emmanuel Meyer, *sous-directeur des affaires juridiques de l'enseignement scolaire à la direction des affaires juridiques*

- Mme Véronique Fouquat, *chef du bureau des programmes d'enseignement à la direction générale de l'enseignement scolaire*

● **Ministère de l'intérieur**

- **M. Guillaume Schlumberger**, *délégué à la prospective et à la stratégie*

- M. Régis Reboul, *chargé de mission auprès du délégué*

● **Représentants des Etats-Unis**

- Mme Florence Radovic, *spécialiste économique à l'Ambassade des Etats-Unis à Paris*

- Mme Lauren Saadat, *directrice chargée de la politique internationale en matière de protection des données au ministère de la Sécurité des Etats-Unis (Department of Homeland Security)*

- M. Hugh Stevenson, *directeur adjoint de la Commission fédérale du commerce (Federal Trade Commission), bureau des affaires internationales*

● **Chambre de commerce américaine**

- **M. Winston Maxwell,** *avocat associé, Hogan et Hartson*
- **Mme Denise Lebeau Marianna**, *avocat, Baker & McKenzie*
- **Mme Carol Umhoefer**, *avocat, DLA-Piper*
- **Mme Florence Chafiol-Chaumont**, *avocat, August & Debouzy*
- **M. Anthony Paronneau**, *avocat, Dechert*
- **Mme Pauline Le Bousse**, *avocat, Hogan & Hartson*

● **TGI de Paris**

- **M. Nicolas Bonnal**, *vice-président de la 17ème chambre (presse)*

ENTREPRISES

● **Facebook France**

- **M. Damien Vincent**, *directeur commercial France*
- **M. Chris Kelly**, *directeur de la sécurité et des données personnelles*
- **M. Mozelle Thompson**, *consultant*

● **Google France**

- **M. Olivier Esper**, *directeur chargé des relations institutionnelles*
- **M. Peter Fleischer**, *directeur de la protection de la vie privée*

● **Honeywell**

- **M. Jérôme Maironi**, *vice-président*

● **JC Decaux - Vélib**

- **M. Pierre Foulon**, *responsable des relations contractuelles pour vélos en libre service*
- **M. Marc Merlini**, *directeur application grand public*

● **Majority Report**

- **M. Laurent Collot**, *directeur*
- **M. François Mariet**, *directeur marketing*

● **Microsoft France**

- **M. Jean Gonié,** *responsable des affaires institutionnelles*

- M. Marc Mossé, *directeur des affaires publiques et juridiques*

● **My Space France**

- M. David Fares, *directeur des relations institutionnelles chez NewsCorp*

- M. Lionel Thoumyre, *directeur de la prévention et de la sécurité*

● **RATP**

- **M. Dominique Chaumet**, *correspondant informatique et libertés*

● **Sagem**

- Mme Carole Pellegrino, *responsables des relations institutionnelles*

- M. Bernard Didier, *directeur général adjoint, directeur recherche et technologies, business développement*

● **Thalès**

- M. Jacques Delphis, *directeur des relations extérieures et institutionnelles du groupe Thales*

- M. Franck Greverie, *directeur général de la sécurité des systèmes d'information de la division D3S*

- M. Kamal Boussadia, *responsable des solutions innovantes au sein de la division sécurité*

ASSOCIATIONS

● **Association Française des Correspondants aux Données**

- M. Arnaud Belleil, *vice-président et directeur associé de Cecurity.com*

- M. Paul-Olivier Gibert, *président et directeur de la sécurité et de la déontologie AG2R Prévoyance*

● **Association Iris**

- Mme Meryem Marzouki, *présidente*

● **Forum des droits sur Internet**

- Mme Isabelle Falque-Pierrotin, *présidente du conseil d'orientation*

- **M. Stéphane Grégoire**, *juriste*

● **Ligue des droits de l'homme**

- M. Jean-Claude Vitran, *responsable du groupe de travail Liberté et TIC*

PERSONNALITES QUALIFIEES

● **GIE avocats**

- M. Paul-Albert Iweins, *président du Conseil national des Barreaux*

- M. Pascal Eydoux, *président de la conférence des Bâtonniers*

- M. le Bâtonnier Christian Charrière-Bournazel, *Bâtonnier de Paris*

● **Avocats**

- Maître Alain Bensoussan

- **Mme Corinne Lepage**

- Maître Olivier Proust

● **M. Dominique Cardon,** *sociologue*

● **Mme Nathalie Mallet-Poujol**, *professeur à l'Université Montpellier 1*

● **M. Yves Poullet**, *directeur du centre de recherche informatique et de droit à l'Université de Namur*

ANNEXE 3

DÉPLACEMENTS DU GROUPE DE TRAVAIL

(avec M. Yves Détraigne et Mme Anne-Marie Escoffier, co-rapporteurs)

Déplacement à Madrid
12 et 13 mars 2009

Jeudi 12 mars

• Entretien avec **M. Antonio Troncoso,** *directeur de l'agence de protection des données de la Communauté de Madrid*

• Déjeuner de travail avec :

- **Mme María Rosa Vindel Lopez**, *sénateur de la Communauté de Madrid, membre du conseil consultatif de l'Agence espagnole de protection des données personnelles (AEPD),*

- **M. Juan Luis Rascon**, *député de Cordoue, membre de la commission constitutionnelle du Congrès des députés,*

- **M. Alejandro Perales**, *président de l'association des usagers de la communication et représentant du conseil des consommateurs et usagers auprès du conseil consultatif de l'Agence espagnole de protection des données (AEPD),*

- **Mme Belén Veleiro**, *directrice du département juridique du conseil supérieur des chambres de commerce, d'industrie et de navigation de l''Espagne, membre du conseil consultatif de l'AEPD*

• Entretiens avec :

- **M. José Antonio Martin**, *magistrat du Tribunal Suprême*

- **M. Juan Cesareo Ortiz Urculo**, *procureur en chef du Tribunal constitutionnel* et **M. Vicente Conde Martin De Hijas**, *magistrat au sein de cette juridiction*

- **M. Antoni Farriols**, *président de la Comisión de Libertades e Informática (commission des libertés et de l'informatique)*

Vendredi 13 mars

• Entretien avec des membres de l'agence espagnole de protection des données :

- **M. Jesús Rubi**, *directeur adjoint de l'agence*

- **M. José Lopez**, *sous-directeur chargé de l'Inspection*

- **Mme Marta Aguirre**, *conseillère du service international*

Déplacement à Bruxelles
31 mars 2009

Mardi 31 mars

• Entretien avec :

- **M. Alain Brun**, *chef d'unité chargé de la protection des données -direction générale « Justice, Liberté et sécurité » de la Commission européenne*

- **MM. Laurent Beslay** et **Hielke Hijman**, *conseillers scientifiques, bureau du contrôleur européen de la protection des données*

• Déjeuner de travail avec :

- **M. Jean-Philippe Mochon,** *conseiller juridique à la représentation permanente de la France auprès de l'Union européenne*

• Entretien avec :

- **M. Manuel Mateo Goyet**, *conseiller scientifique, unité D4 (entreprises de réseaux, RFID) à la Direction Générale « société de l'information » de la Commission européenne*

- **M. Achim Klabunde**, *responsable « vie privée » à la Direction Générale « société de l'information » de la Commission européenne*

Déplacement à l'aéroport de Paris Charles de Gaulle
2 avril 2009

Jeudi 2 avril

Accueil par M. Patrick Espagnol, sous-préfet chargé de mission auprès du préfet de la Seine-Saint-Denis pour la sécurité et la sûreté des plates-formes aéroportuaires de Roissy-Charles de Gaulle et du Bourget

- Présentation globale des applications utilisées sur la plate-forme
- Présentation du dispositif de vidéo-protection par Aéroports de Paris
- Présentation du « tracing » au Terminal 2 F1 par Aéroports de Paris

- Présentation des applications utilisées par Air-France au Terminal 2F1 :
  Application « Gaetan »
  Dématérialisation de la Carte d'Embarquement sur téléphone mobile « Smartboarding »

- Présentation par la Police aux frontières (PAF) de leur système de contrôle biométrique interne ainsi que des visas biométriques

Déplacement à Grenoble
31 mars 2009

Lundi 6 avril

- Entretien avec **M. Jean-Charles Guibert**, *directeur de la valorisation au CEA et Directeur de Minatec*
- Visite des laboratoires de biotechnologie : présentation des systèmes intégrés pour l'analyse biologique « laboratoire sur puce »
- Visite du show room des objets communicants : présentation des systèmes innovants « carte à puce sans contact » et « capture de mouvement »
- Visite du plateau d'innovation pluridisciplinaire MINATEC IDEAs Laboratory® : présentation des initiatives visant à favoriser l'innovation tout en anticipant les usages des utilisateurs et l'acceptabilité des objets communicants innovants en termes d'enjeux sociétaux et d'éthique

ANNEXE 4

LOI N° 78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS (EXTRAITS)

(Version consolidée au 14 mai 2009)

Chapitre Ier : Principes et définitions

Article 1

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Article 2

La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

Article 5

I. - Sont soumis à la présente loi les traitements de données à caractère personnel :

1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;

2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne.

II. - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.

Chapitre II : Conditions de licéité des traitements de données à caractère personnel

Section 1 : Dispositions générales

Article 6

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

1° Les données sont collectées et traitées de manière loyale et licite ;

2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au

regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Article 7

Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée ;

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Section 2 : Dispositions propres à certaines catégories de données

Article 8

I.-Il est interdit de collecter ou de traiter des 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.

II.-Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :

1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;

2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;

3° Les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :

- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ;

- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;

- et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;

4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;

5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;

6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;

7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ;

8° Les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX.

III.-Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables.

IV.-De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26.

Article 9

Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par :

1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;

2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;

3° [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004 ;]

4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits.

Chapitre III : La Commission nationale de l'informatique et des libertés

Article 11

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes :

1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;

2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi.

A ce titre :

a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements ;

b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ;

c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;

d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en œuvre ou

envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel ;

e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ;

f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou des agents de ses services, dans les conditions prévues à l'article 44, de procéder à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;

g) Elle peut, dans les conditions définies au chapitre VII, prononcer à l'égard d'un responsable de traitement l'une des mesures prévues à l'article 45 ;

h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ;

3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements :

a) Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ;

b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ;

c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission, le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ;

4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ;

A ce titre :

a) Elle est consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés. A la demande du président de l'une

des commissions permanentes prévue à l'article 43 de la Constitution, l'avis de la commission sur tout projet de loi est rendu public ;

b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ;

c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ;

d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine.

Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.

La commission présente chaque année au Président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission.

Article 13

I. - La Commission nationale de l'informatique et des libertés est composée de dix-sept membres :

1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat ;

2° Deux membres du Conseil économique et social, élus par cette assemblée ;

3° Deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'Etat ;

4° Deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ;

5° Deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ;

6° Trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ;

7° Deux personnalités qualifiées pour leur connaissance de l'informatique, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat.

La commission élit en son sein un président et deux vice-présidents, dont un vice-président délégué. Ils composent le bureau.

La formation restreinte de la commission est composée du président, des vice-présidents et de trois membres élus par la commission en son sein pour la durée de leur mandat.

En cas de partage égal des voix, celle du président est prépondérante.

II. - Le mandat des membres de la commission mentionnés aux 3°, 4°, 5°, 6° et 7° du I est de cinq ans ; il est renouvelable une fois. Les membres mentionnés aux 1° et 2° siègent pour la durée du mandat à l'origine de leur désignation ; leurs mandats de membre de la Commission nationale de l'informatique et des libertés ne peuvent excéder une durée de dix ans.

Le membre de la commission qui cesse d'exercer ses fonctions en cours de mandat est remplacé, dans les mêmes conditions, pour la durée de son mandat restant à courir.

Sauf démission, il ne peut être mis fin aux fonctions d'un membre qu'en cas d'empêchement constaté par la commission dans les conditions qu'elle définit.

La commission établit un règlement intérieur. Ce règlement fixe les règles relatives à l'organisation et au fonctionnement de la commission. Il précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission, ainsi que les modalités de mise en œuvre de la procédure de labellisation prévue au c du 3° de l'article 11.

Article 17

La formation restreinte de la commission prononce les mesures prévues au I et au 1° du II de l'article 45.

Chapitre IV : Formalités préalables à la mise en œuvre des traitements

Article 22

I. - A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.

II. - Toutefois, ne sont soumis à aucune des formalités préalables prévues au présent chapitre :

1° Les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

2° Les traitements mentionnés au 3° du II de l'article 8.

III. - Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé.

La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel.

Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.

En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.

IV. - Le responsable d'un traitement de données à caractère personnel qui n'est soumis à aucune des formalités prévues au présent chapitre communique à toute personne qui en fait la demande les informations relatives à ce traitement mentionnées aux 2° à 6° du I de l'article 31.

Section 1 : Déclaration.

Article 23

I. - La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

Elle peut être adressée à la Commission nationale de l'informatique et des libertés par voie électronique.

La commission délivre sans délai un récépissé, le cas échéant par voie électronique. Le demandeur peut mettre en œuvre le traitement dès réception de ce récépissé ; il n'est exonéré d'aucune de ses responsabilités.

II. - Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Dans ce cas, les informations requises en application de l'article 30 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

Article 24

I. - Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes publics et privés représentatifs, des normes destinées à simplifier l'obligation de déclaration.

Ces normes précisent :

1° Les finalités des traitements faisant l'objet d'une déclaration simplifiée ;

2° Les données à caractère personnel ou catégories de données à caractère personnel traitées ;

3° La ou les catégories de personnes concernées ;

4° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées ;

5° La durée de conservation des données à caractère personnel.

Les traitements qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité envoyée à la commission, le cas échéant par voie électronique.

II. - La commission peut définir, parmi les catégories de traitements mentionnés au I, celles qui, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées, sont dispensées de déclaration.

Dans les mêmes conditions, la commission peut autoriser les responsables de certaines catégories de traitements à procéder à une déclaration unique selon les dispositions du II de l'article 23.

Section 2 : Autorisation

Article 25

I. - Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :

1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ;

2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;

3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;

4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;

5° Les traitements automatisés ayant pour objet :

- l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;

- l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;

6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ;

7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;

8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

II. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes

destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

III. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.

Article 26

I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :

1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

L'avis de la commission est publié avec l'arrêté autorisant le traitement.

II. - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement.

III. - Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.

IV. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

Article 27

I. - Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :

1° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ;

2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

II. - Sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :

1° Les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le numéro d'inscription à ce répertoire ;

2° Ceux des traitements mentionnés au I :

- qui ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ;

- qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ;

- et qui sont mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques ;

3° Les traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer ;

4° Les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I aux fins de mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques.

III. - Les dispositions du IV de l'article 26 sont applicables aux traitements relevant du présent article.

Chapitre V : Obligations incombant aux responsables de traitements et droits des personnes

Section 1 : Obligations incombant aux responsables de traitements.

Article 32

I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

2° De la finalité poursuivie par le traitement auquel les données sont destinées ;

3° Du caractère obligatoire ou facultatif des réponses ;

4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;

5° Des destinataires ou catégories de destinataires des données ;

6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;

7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

II.- Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :

- de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;

- des moyens dont elle dispose pour s'y opposer.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

III.- Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.

Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ou à la réutilisation de ces données à des fins statistiques dans les conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

IV.- Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I.

V.- Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en oeuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement.

VI.-Les dispositions du présent article ne s'appliquent pas aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Article 34

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour

préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

Section 2 : Droits des personnes à l'égard des traitements de données à caractère personnel

Article 38

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement.

Article 39

I.-Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit

d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.

Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition.

II.- Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées.

Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés.

Article 40

Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39.

Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.

Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

Article 41

Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient.

La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi.

Chapitre VI : Le contrôle de la mise en œuvre des traitements

Article 44

I.-Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Le procureur de la République territorialement compétent en est préalablement informé.

II.- En cas d'opposition du responsable des lieux, la visite ne peut se dérouler qu'avec l'autorisation du président du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter ou du juge délégué par lui.

Ce magistrat est saisi à la requête du président de la commission. Il statue par une ordonnance motivée, conformément aux dispositions prévues aux articles 493 à 498 du code de procédure civile. La procédure est sans représentation obligatoire.

La visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée. Celui-ci peut se rendre dans les locaux durant l'intervention. A tout moment, il peut décider l'arrêt ou la suspension de la visite.

III.- Les membres de la commission et les agents mentionnés au premier alinéa du I peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles ; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Ils peuvent, à la demande du président de la commission, être assistés par des experts désignés par l'autorité dont ceux-ci dépendent.

Seul un médecin peut requérir la communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en œuvre par un membre d'une profession de santé.

Il est dressé contradictoirement procès-verbal des vérifications et visites menées en application du présent article.

IV.- Pour les traitements intéressant la sûreté de l'Etat et qui sont dispensés de la publication de l'acte réglementaire qui les autorise en application du III de l'article 26, le décret en Conseil d'Etat qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article.

Chapitre VII : Sanctions prononcées par la Commission nationale de l'informatique et des libertés

Article 45

I. - La Commission nationale de l'informatique et des libertés peut prononcer un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la présente loi. Elle peut également mettre en demeure ce responsable de faire cesser le manquement constaté dans un délai qu'elle fixe.

Si le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée, la commission peut prononcer à son encontre, après une procédure contradictoire, les sanctions suivantes :

1° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;

2° Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.

II. - En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la commission peut, après une procédure contradictoire :

1° Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26, ou de ceux mentionnés à l'article 27 mis en œuvre par l'Etat ;

2° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ;

3° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ; le Premier ministre fait alors connaître à la commission les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

III. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.

Article 46

Les sanctions prévues au I et au 1° du II de l'article 45 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la commission mais ne prend pas part à ses délibérations. La commission peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information.

La commission peut rendre publics les avertissements qu'elle prononce. Elle peut également, en cas de mauvaise foi du responsable du traitement, ordonner

l'insertion des autres sanctions qu'elle prononce dans des publications, journaux et supports qu'elle désigne. Les frais sont supportés par les personnes sanctionnées.

Les décisions prises par la commission au titre de l'article 45 sont motivées et notifiées au responsable du traitement. Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat.

Article 47

Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.

Lors du premier manquement, il ne peut excéder 150 000 Euros. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 euros ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros.

Lorsque la Commission nationale de l'informatique et des libertés a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.

Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.

Chapitre VIII : Dispositions pénales

Article 50

Les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

Article 51

Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :

1° Soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 ;

2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;

3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.