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*).

Aussi ne peut-on 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. »