

La vie privée à l'heure des mémoires numériques

Commission des lois du Sénat

Rapport d'information

de M. Yves Détraigne, sénateur de la Marne (U.C.)
et de Mme Anne-Marie Escoffier, sénateur de l'Aveyron (R.D.S.E)

➤ *La vie privée, une valeur fondamentale des sociétés modernes*

Apparu au XIX^{ème} siècle, sous l'impulsion, en particulier, des tenants du libéralisme politique, tels que Benjamin Constant et Alexis de Tocqueville, violemment contesté par les régimes totalitaires du XX^{ème} siècle, le droit à la vie privée, parce qu'il est indissociable de l'existence de l'individu et de l'exercice de ses libertés, est une **valeur fondamentale des sociétés modernes**. La notion de vie privée recouvre 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**, c'est-à-dire 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.

Le droit à la vie privée comme la protection des données personnelles, qui en est une déclinaison, sont **largement consacrés dans les textes**, qu'il s'agisse de la déclaration universelle des droits de l'homme de 1948, de la Convention européenne des droits de l'homme de 1950, du Pacte international relatif aux droits civils et politiques du 16 novembre 1966, de la « Convention 108 » du Conseil de l'Europe de 1981 et de la Charte européenne des droits fondamentaux du 7 décembre 2000. En France, le droit à la vie privée est inscrit à l'article 9 du code civil et consacré par la jurisprudence du Conseil constitutionnel.

➤ *La vie privée : un droit menacé ?*

Valeur fondamentale de nos sociétés, la vie privée n'en est pas moins confrontée, depuis quelques années, à l'apparition de « **nouvelles mémoires numériques** », conséquence de nombreuses évolutions technologiques ayant pour effet principal ou incident de collecter des données permettant de suivre un individu dans le **temps et l'espace**.

- La recherche d'une sécurité collective toujours plus infaillible

Le droit à la vie privée est né historiquement de la volonté de préserver les droits de l'individu et de sa sphère privée face aux immixtions de la puissance publique. Pourtant, 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, ce qui s'est traduit 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* ». Ce déplacement du point d'équilibre entre sécurité et liberté explique certains glissements sémantiques : ainsi, par exemple, le terme de « *vidéosurveillance* » tend à être remplacé par celui de « *vidéoprotection* ».

Cette tendance à l'acceptation d'une « surveillance institutionnelle » est complétée par deux nouvelles tendances qui ont en commun d'exposer la vie privée à une nouvelle menace : la **surveillance par les acteurs privés**. Ces tendances sont l'accélération des progrès technologiques et l'exposition de soi et d'autrui sur Internet.

- L'accélération des progrès technologiques

On assiste depuis quelques années à des développements technologiques spectaculaires, tels que la géolocalisation, le Bluetooth, les RFID, les nanotechnologies, etc., qui donnent naissance à des **usages toujours plus nombreux** et dans des **domaines les plus variés** : transport, ergonomie, publicité, etc. Si tous visent à apporter de nouvelles facilités aux utilisateurs, ils sont également **porteurs de risques nouveaux au regard du droit à la vie privée**. A titre d'exemple, si chacun comprend l'intérêt du GPS pour trouver plus facilement son chemin, ce système permet aussi de suivre les déplacements des individus et doit être encadré pour éviter toute dérive. De même, si la technologie « sans contact » RFID peut apporter certains progrès en permettant, par exemple, d'améliorer la ponctualité des vols dans l'hypothèse où les cartes d'embarquement, dotés de cette technologie, permettent de localiser rapidement les passagers en retard, elles constituent **un défi nouveau au regard du droit à la vie privée et de la liberté d'aller et venir**. Enfin, si les puces RFID offrent des fonctionnalités nouvelles et intéressantes pour les utilisateurs (badge d'accès à une voiture, un parking, étiquettes sur un produit alimentaire permettant, demain, à un réfrigérateur de lire les dates de péremption...), il convient d'interdire à des tiers non autorisés l'accès à ces informations qui, dans certains cas, « *racontent une portion de vie d'un individu* ». Le danger est d'autant plus grand à l'heure des nanotechnologies, qui permettent de fabriquer des puces à l'échelle du nanomètre, c'est-à-dire du milliardième de mètre, ce qui les rend **invisibles**.



*Les rapporteurs en déplacement au Minatec
(centre spécialisé dans les nanotechnologies)
de Grenoble le 6 avril 2009*

- La tendance à l'exposition de soi et d'autrui

L'apparition de nouvelles formes de sociabilité sur Internet s'exprimant par le biais de *blogs* ou de réseaux sociaux (tels que Facebook, MySpace, etc.) a fait naître une nouvelle tendance sociologique forte : l'exposition volontaire de soi et d'autrui. Or, cette tendance, mue par certains facteurs tels que le mimétisme social, mais aussi par l'adhésion aux nouvelles valeurs d'échange et de partage, sur un mode largement informel et « décontracté », n'est pas sans risques au regard du droit à la vie privée.

En effet, considérer que livrer des informations personnelles sur Internet – sur soi ou sur autrui – est comparable à entretenir des conversations privées au milieu d'une foule bruyante, et qu'en conséquence, la probabilité qu'un tiers non autorisé prenne connaissance de nos propos est infime revient à faire fi des spécificités d'Internet : une fois mises en ligne, les données acquièrent **une universalité dans l'espace et le temps**, d'autant que, même diffusées sur des sites très variés et sur des périodes très étendues, elles peuvent aisément resurgir au moyen des moteurs de recherche, tels que Google, qui permettent en un seul clic d'agréger des sources d'information qu'il aurait été quasi-impossible de réunir auparavant.

➤ **Un cadre juridique protecteur**

Si ces trois nouvelles tendances constituent de nouveaux défis au regard du droit à la vie privée, notre cadre juridique sur la protection des données personnelles y apporte dans une très large mesure des **réponses adaptées et pérennes**, peut-être, paradoxalement, **parce qu'il les a précédées**.

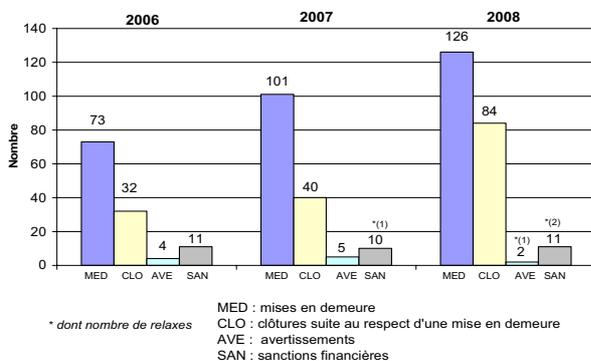
La France a été ainsi l'un des premiers pays au monde à se doter d'une loi de protection des données personnelles, au travers de la loi de 1978 « informatique et libertés ».

Par ailleurs, l'Union européenne a adopté, dès 1995, une directive sur la protection des données personnelles. Le choix a alors été fait de ne pas adopter de dispositions spécifiques pour certaines technologies ou applications et de fixer des principes intemporels (« neutralité techno-logique ») dont la **souplesse** apparaît comme un **gage de protection**. Ces principes, transposés en France par la loi 6 août 2004, sont les suivants : finalité, proportionnalité, sécurité des données, accès et rectification, droit à l'information, droit d'opposition et droit au consentement préalable. Si le choix avait été fait de s'engager sur la voie de législations spécifiques pour certaines technologies ou applications, il aurait nécessairement conduit à des vides juridiques, le temps technologique étant plus rapide que le temps démocratique d'élaboration des normes.

En outre, l'Europe a opportunément décidé de renforcer les pouvoirs des autorités nationales de protection des données, notamment en les dotant d'un **pouvoir de sanction**, et de créer deux nouveaux gardiens de cette protection : le G29, groupe de travail européen rassemblant les représentants de vingt-sept autorités indépendantes de protection des données nationales et le contrôleur européen des données dont la principale mission est de contrôler les traitements de données à caractère personnel effectués par l'administration de l'Union européenne.

Depuis 2006, année de l'entrée en vigueur effective de la nouvelle compétence de la CNIL en matière de sanctions, le nombre d'affaires a quasiment doublé, comme l'illustre le tableau ci-dessous.

Sanctions prononcées par la CNIL
entre 2006 et 2008



➤ **Un cadre néanmoins partiellement inadapté aux enjeux de la globalisation et aux spécificités d'Internet**

Le cadre juridique ainsi défini n'apporte pas toujours des réponses satisfaisantes aux bouleversements qui viennent défier le droit à la vie privée.

En premier lieu, 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. La directive de 1995 sur la protection des données prévoit en particulier que lorsque 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, c'est le droit de ce dernier qui s'applique.

Ces dispositions soulèvent 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 G29 soutenait que les moteurs de recherche, pour établir des profils d'utilisateurs détaillés, utilisaient des « cookies » qui devaient 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.

Ces divergences prennent un relief particulier compte tenu du fait qu'Européens et Américains n'ont pas les mêmes approches en matière de protection des données personnelles. Toutefois, elles ne doivent pas être caricaturées. La protection des données personnelles est aussi une préoccupation forte des autorités et des citoyens américains. Ceci invite à un certain optimisme quant à la possibilité de trouver au plan international une approche commune en matière de protection des données.

En second lieu, Internet pose des **questions nouvelles** au regard du droit à la vie privée. D'une part, le principe du droit à l'effacement et à l'anonymisation des données de connexion, garant du respect de la vie privée, doit être tempéré par la nécessité de garantir d'autres droits fondamentaux tels que le droit à la protection de la propriété intellectuelle, qui justifie une certaine forme de traçage que la loi s'efforce d'encadrer. D'autre part, le modèle économique d'un grand nombre de sociétés de l'Internet repose sur l'offre de services dits « gratuits », financés par une publicité ciblée de plus en plus élaborée. En particulier, les « cookies », installés sur les disques durs des internautes sans que, souvent, ceux-ci en aient conscience, permettent de mémoriser les habitudes de navigation des individus dans le but d'établir des profils de consommation auxquels seront adressés des messages publicitaires adaptés.

Or Internet se révèle être un terrain mal adapté à l'exercice des droits reconnus par la loi « informatique et libertés » : comment peut-on refuser les cookies sans être pénalisé pour la navigation ? Comme exiger du responsable d'un site implanté en-dehors du territoire communautaire qu'il rectifie ou supprime des informations touchant à notre vie privée ? Comment envisager qu'un individu fasse valoir ses droits de rectification et d'opposition sur des données le concernant qu'aurait rendues publiques, via un réseau social, un ami, un collègue ou un parent.

➤ **15 recommandations**

Le rapport d'information formule **15 recommandations** pour mieux **garantir le droit à la vie privée à l'heure des nouvelles mémoires numériques** et renforcer **ainsi la confiance des citoyens à l'égard de la société de l'information**.

→ Faire du citoyen un « homo numericus » libre et éclairé, protecteur de ses propres données

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

- Créer une redevance, de faible montant, acquittée par les grands organismes, publics et privés, qui traitent des données à caractère personnel
- Déconcentrer les moyens d'actions de la CNIL par la création d'antennes interrégionales
- Renforcer la capacité d'expertise et de contrôle de la CNIL
- Rendre obligatoires les correspondants informatique et libertés pour les structures publiques et privées de plus de cinquante salariés
- Rendre publiques les audiences et les décisions de la formation restreinte de la CNIL

→ Compléter le cadre juridique actuel

- Soutenir la dynamique en cours tendant à la définition de standards internationaux dans le domaine de la protection des données personnelles
- Affirmer sans ambiguïté que l'adresse IP constitue une donnée à caractère personnel
- Créer *a minima* une obligation de notification des failles de sécurité auprès de la CNIL
- Réunir sous une seule autorité, la CNIL, les compétences d'autorisation et de contrôle en matière de vidéosurveillance
- Réserver au législateur la compétence exclusive pour créer un fichier de police
- Réfléchir à la création d'un droit à « l'hétéronymat » et d'un droit à l'oubli
- Inscrire dans notre texte constitutionnel la notion de droit au respect de la vie privée