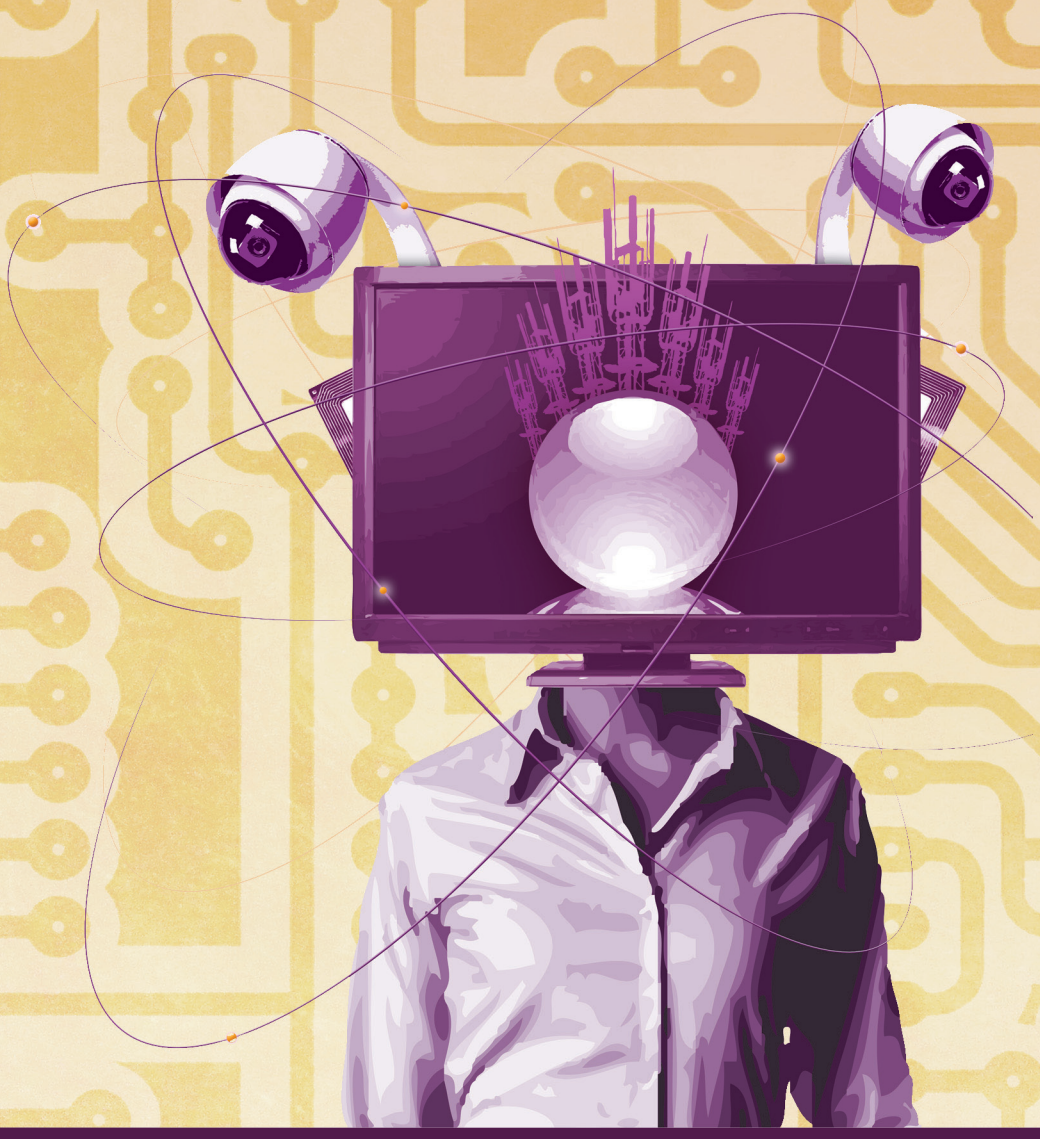
LES NOUVELLES TECHNOLOGIES AU SERVICE DU CITOYEN ?



Ligue des droits de l'Homme

îledeFrance

SOMMAIRE

INTRODUCTION

Une société de surveillance, c'est ainsi que la Ligue des droits de l'Homme intitulait son « Etat des droits de l'Homme en France » en 2009. Elle témoignait ainsi de l'importance de l'intrusion dans tout notre quotidien des « Nouvelles technologies de l'information et de la communication » (Ntic ou Tic), et de la menace pour les droits et les libertés.

Les Tic sont, pour le meilleur : communiquer, s'informer, agir à distance, permettre les mobilisations, et pour le pire : tout savoir, tout voir, tout contrôler.

Mettant au cœur de son action ces thématiques, la LDH a notamment :

• adopté une résolution « Société de surveillance, vie privée et libertés », lors de son congrès 2009 ;

• mis en place un groupe de travail « Libertés et technologies de l'information et de la communication » ;

• mené plusieurs campagnes contre les fichiers (Fnaeg, Base-élèves, Edvige…) et contre la vidéosurveillance ;

• organisé des réunions publiques ;

• déposé des recours au Conseil d'Etat (passeport biométrique, fichier Oscar…) ;

• mis à disposition des outils de réflexion et d'analyse ;

• s'est impliquée dans plusieurs programmes européens, dont le programme « Données personnelles, des droits ? Informer et sensibiliser les jeunes citoyens européens ».

Cet investissement a été naturellement prolongé par la mise en œuvre d'un programme de travail sur trois ans en Ile-de-France, « Nouvelles technologies au service du citoyen », soutenu par le conseil régional (soutien en faveur de la vie citoyenne et démocratique en Ile-de-France).

Sensibiliser plus particulièrement les jeunes à l'impact des Tic sur les libertés publiques et à leur importance grandissante dans leur relation à l'exercice de la citoyenneté a été l'objectif de ce programme. Il a comporté deux axes de travail, l'un autour des questions du fichage, de la vidéosurveillance et du contrôle social, l'autre sur la question de l'information et de sa libre circulation, des médias, de la liberté d'expression et de la censure, avec un ensemble de réunions publiques.

Le présent document, à travers une synthèse des débats, résume les enjeux, met l'accent sur les questionnements et les inquiétudes, et retrace les orientations et les propositions formulées.

Les éléments techniques, juridiques et le détail des analyses sont disponibles dans les outils et documents publiés tout au long de ces trois années : deux numéros *d'Hommes & Libertés*, le hors-série « Tous surveillés, tous surveillants », et le n°157 « Médias, atouts technologiques, défis démocratiques », et deux guides juridiques, *La protection des données personnelles*, et *La vidéosurveillance*. Certains de ces apports sont repris dans cette synthèse.

Les Tic *versus* les libertés et le contrôle social

Les libertés face aux moyens de surveillance offerts par les technologies (fichiers, vidéo-surveillance, géolocalisation, téléphone, Internet, etc.).

L'utilisation des technologies de l'information et de la communication dans notre quotidien est devenue tout à fait naturelle pour la plupart des citoyens. Hormis quelques « réfractaires » qui ont choisi de les rejeter, ou des fractions de la population parmi les plus âgées ou les plus défavorisées qui ne peuvent se les approprier ou y accéder, une majorité de nos concitoyens utilise l'Internet et les réseaux sociaux, le téléphone portable et le GPS. Mais si ces utilisations des Tic sont choisies, en même temps les citoyens sont fichés, « vidéosurveillés ». Ils laissent des traces involontaires de leur passage, que ce soit dans leur entreprise, la cantine, les lieux de loisirs ou les transports en commun.

Les facilités que procure l'utilisation des Tic fait oublier à la plupart les risques qu'elle comporte, et nombreux sont ceux qui ne perçoivent pas ou veulent ignorer toutes ces possibilités d'atteintes à leur vie privée et aux libertés publiques.

Les technologies de l'information et de la communication portent en elles les possibilités du contrôle social. L'informatique permet le fichage et le profilage. On peut citer :

• le développement de l'informatique et la miniaturisation de ses outils (ordinateurs portables, tablettes, « smartphones », caméras et appareils photo numériques, etc.), les capacités de numérisation massive des données, les transmissions ultra-rapides par des réseaux physiques mais aussi virtuels, les capacités de stockage sur des supports de plus en plus réduits (clés USB, cartes-mémoire, etc.), les algorithmes de tri et de recherche de plus en plus performants dans des fichiers possiblement interconnectés ou dans des bases de données, les accès à distance et les protocoles d'échanges de données et d'interconnexion permettent la constitution de mégabases de données et leur interrogation par des moteurs de plus en plus rapides et puissants, qui donnent la possibilité aux sociétés commerciales de tracer les internautes, et à la police d'en surveiller certains ;

• les sociétés commerciales se livrent au suivi de nos traces sur Internet. De plus, les autorités ont légalisé les contrôles sur les communications téléphoniques et électroniques en obligeant les opérateurs et fournisseurs d'accès à enregistrer les interlocuteurs, la date et l'heure de connexion, ainsi que les contenus, aux prétextes de sécurité, de lutte contre le terrorisme, la cybercriminalité et la pédophilie ;

• les puces RFID (identification à distance par radiofréquence), qui peuvent contenir de façon plus ou moins sécurisée, en fonction de la qualité et donc du coût de la puce, de nombreuses données personnelles et les restituer à des lecteurs sans contact, facilitent les accès à différents services (transports, piscines, bibliothèques, entreprises, cantines, etc.), mais elles permettent aussi de « tracer » ces divers porteurs qui parfois peuvent voir leurs données piratées ;

• certaines technologies, qui vont plus loin encore, par une utilisation croissante de la biométrie : empreintes palmaires pour accéder aux cantines scolaires, empreintes digitales, photos numérisées ou encore empreintes ADN alimentent de plus en plus de fichiers, notamment ceux mis en place par les services de police, ou ceux utilisés pour les documents d'identité et les fichiers associés.

Dans les villes et parfois dans les plus petites communes[1], la vidéosurveillance, désormais promue par les pouvoirs publics, est utilisée par les élus locaux comme recours « providentiel » pour lutter contre la délinquance. Cette utilisation constitue un risque pour la vie privée et les libertés.

En effet les caméras déployées dans l'espace public, reliées à des postes d'observation ou des espaces de stockage, permettent de surveiller les citoyens sans que ceux-ci ne voient leurs surveillants. Les images de qualité de plus en plus précises peuvent être regardées en temps réel par des opérateurs, ou traitées par des logiciels de sélection automatique sur certains critères de tri, d'analyse comportementale et, bientôt, comparées aux images numériques des fichiers d'analyses sérielles, elles permettront de repérer des personnes recherchées par la reconnaissance faciale.

Le traitement des données issues de ces systèmes constitue une menace pour la vie privée. En effet, les policiers et les gendarmes peuvent avoir accès aux images collectées sans le contrôle d'un juge. Ce traitement induit aussi une tendance à la discrimination. Parmi les trop grandes quantités d'images que les opérateurs ont à surveiller, leurs choix se portent plus facilement sur les jeunes, et surtout ceux dont l'allure leur semble suspecte.

1 Beaudinard-sur-Vernon, 12 caméras pour 146 habitants, Rennes-les-Bains, 10 caméras pour 170 habitants, source : http://owni.fr

Les Tic et l'enjeu démocratique

L'enjeu démocratique au travers des possibilités offertes par les technologies de l'Internet

Si la démocratie est avant tout une forme de gouvernement (du peuple, par le peuple, pour le peuple), pour la LDH, elle implique aussi et surtout l'exercice de la citoyenneté. S'il est entendu que tous les citoyens doivent pouvoir exercer leur droit de vote, ils doivent aussi pouvoir s'informer librement (liberté d'accès à l'information), avoir le droit de s'exprimer (liberté d'expression), et jouir du droit de contester certaines décisions de leur gouvernement (liberté de manifester, etc.). Par l'accès à la connaissance qu'il permet, Internet peut être considéré comme un moyen favorisant ces différents droits. Mais sans doute cela doit-il être nuancé et précisé. L'accès à l'Internet doit être considéré comme un droit fondamental (accès à l'information). Or cet accès dépend d'opérateurs privés qui ont d'abord des objectifs commerciaux. Il existe une « fracture numérique », liée au niveau d'éducation ou aux coûts d'abonnements, qui concerne encore de nombreux citoyens, et l'accès aux réseaux haut débit (nécessaires pour une utilisation confortable des différents services) est encore inégal sur le territoire français, créant aussi une fracture territoriale s'ajoutant à la fracture sociale.

Droit à l'information

L'accès à l'information offert par l'Internet peut sembler sans limites au regard des milliards de données (textes, images, etc.) disponibles et partageables quasi instantanément. La question de la pertinence de ces informations, de leur véracité devrait inciter à la même vigilance que celle développée vis-à-vis des médias classiques. Les informations sur les sites de médias dits alternatifs sont soumises à des réalités commerciales identiques à celles de la presse classique. Les manipulations d'informations, d'images sont tout aussi présentes sur Internet que les célèbres disparitions de personnages sur les photos de l'ère soviétique.

Liberté d'expression

L'Internet a grandement favorisé les possibilités pour les individus de s'exprimer. C'est depuis plus de deux décennies, par les messageries et les listes de diffusion puis, grâce au web 2.0, par les blogs, les réseaux sociaux, les forums, sondages et consultations en ligne que les individus peuvent s'exprimer sur la nouvelle agora que constitue l'Internet.

Au-delà de « l'exposition de soi » qui constitue l'essentiel des contenus des réseaux sociaux (et sans grand intérêt pour la démocratie…), le « web citoyen » permet à des militants de traiter certains sujets en profondeur, avec un ancrage dans la réalité des citoyens. Cette expression militante constitue une nouvelle forme de contre-pouvoir. Que l'on songe aux contestations relayées par les réseaux sociaux, qui ont pris une part non négligeable dans les révolutions arabes, ou aux pétitions et courriers aux élus, aux envois massifs de courriers à certains préfets pour libérer des sans-papiers (notamment à la demande de RESF), dans bien des cas le « web citoyen » a souvent permis d'obtenir des résultats positifs : pétition contre le projet de fichier Edvige ou Base-élèves, au niveau européen contre le projet de traité international Acta. L'Internet instaure de nouvelles conditions du débat démocratique, et les récentes élections présidentielles en France ou aux Etats-Unis montrent que les pratiques politiques évoluent. L'Internet peut même susciter la création de partis politiques, tels que le Parti pirate qui a eu des élus en Suède, en Suisse et en Allemagne. La démocratie, c'est aussi l'égal accès aux services publics. L'Internet permet de mettre en œuvre des services d'une administra-

tion électronique (e-administration), c'est-à-dire l'accès à des guichets virtuels qui permettent à l'usager d'accomplir certaines démarches depuis un ordinateur ou même un « smartphone ». On peut ainsi demander des pièces d'état civil, s'inscrire sur les listes électorales, inscrire ses enfants aux services scolaires et périscolaires et payer en ligne cantine et autres services.

Par ailleurs, sous l'impulsion d'une directive européenne, de plus en plus d'administrations ou de villes ouvrent l'accès aux données publiques. Si l'accès à ces informations peut inciter à une plus forte participation à la décision publique et renforcer les liens entre citoyens et gouvernement, des questions se posent sur l'utilisation qui pourrait être faite de ces données par les citoyens (ont-ils les connaissances et les moyens de les analyser et interpréter) et sur l'utilisation par des sociétés commerciales, qui peuvent en faire des usages qu'elles commercialiseront (recherches généalogiques, etc.). La question de la protection des données personnelles est-elle suffisamment prise en compte dans ces mises en ligne ? On peut en effet craindre que ces données ouvertes ne puissent révéler, par divers recoupements et croisements de fichiers, des données personnelles, ce qui représenterait un danger pour les droits et pour la démocratie elle-même.

La surveillance et les libertés

La volonté de surveillance des citoyens par l'Etat, au nom de l'ordre public, n'est pas nouvelle, mais de nos jours elle est, d'une part, exacerbée par l'obsession sécuritaire, l'idéologie du « risque zéro » et, d'autre part, favorisée par les progrès des Tic. Celles-ci permettent souvent d'utiliser les données personnelles des citoyens pour exercer cette surveillance. Pourtant, la loi Informatique et libertés, du 6 janvier 1978, interdisait à l'administration et aux sociétés commerciales d'utiliser les données personnelles à des fins autres que celles pour lesquelles elles ont été collectées.

Les fichiers

Une preuve que la volonté de surveillance ne se relâche pas et que les Tic la favorisent, est sans doute l'inflation des fichiers de police : il y en avait trente-six en 2006, on en compte plus de quatre-vingts en 2012 (et plus de quarante-deux lois sécuritaires en dix ans). Les dangers du fichage sont principalement liés à la quantité de données enregistrées, à la durée excessive de conservation des données, aux détournements de finalité par l'interconnexion des fichiers, ou par l'élargissement de la finalité première, ou encore par les catégories de populations concernées par ce fichage. Ainsi plusieurs fichiers sont particulièrement susceptibles de présenter des dangers pour la vie privée :

- Le Fichier national automatisé des empreintes génétiques (Fnaeg), créé à l'origine pour enregistrer l'ADN des auteurs de crimes sexuels, est utilisé maintenant pour ficher le moindre manifestant ou auteur d'infraction au Code de la route (toute infraction passible d'un an de prison). Outre le fait que ces relevés d'empreintes ADN soient disproportionnés par rapport à la finalité première du fichier, les progrès de la recherche scientifique démontrent que cet ADN pourrait révéler des informations importantes sur la santé des individus fichés, atteinte grave à la vie privée.

- Le Système de traitement des infractions constatées (Stic) répertorie tous les délits portés à la connaissance des services de police, avec les auteurs présumés, les témoins et les victimes. Les origines « raciales » et « ethniques », les opinions religieuses, politiques, philosophiques, l'appartenance syndicale, des données relatives à la santé ou à la vie sexuelle, peuvent être enregistrées et conservées pendant dix à quarante ans, selon les infractions. Les employeurs du secteur de la sécurité sont tenus de demander si un candidat y figure. Ainsi, qu'elles soient témoins ou victimes ou même lavées de tout soupçon, les personnes qui y figurent peuvent être empêchées d'obtenir leur habilitation à travailler. De plus, un décret Guéant du 6 mai 2012 prévoit de rassembler le Stic et son équivalent à l'usage de la gendarmerie, le Judex, et de les connecter à la base Cassiopée (fichier des procédures judiciaires), qui devrait permettre les mises à jour automatiques des décisions de justice. Mais ce nouveau fichier Traitement des antécédents judiciaires (Taj) risque « d'hériter » de toutes les erreurs (dénoncées par la Cnil) que contiennent le Stic et le Judex. De plus Taj permettra de rapprocher des données (éléments communs dans des procédures différentes) et offrira des fonctionnalités d'identification des personnes (reconnaissance faciale des personnes à partir de la photographie de leur visage). Ainsi, les personnes impliquées dans une infraction, et dont le visage aura été filmé par une caméra de vidéosurveillance, pourront être automatiquement identifiées si elles sont déjà connues par les services de police et de gendarmerie. La Cnil considère que cette fonctionnalité présente des risques importants pour les libertés individuelles. De plus, le fichier « d'analyse sérielle », créé dans la foulée, permettra aux enquêteurs de regrouper toutes les données dont dispose l'Etat sur un individu, y compris celles accessibles sur les réseaux sociaux,

pour les infractions punies de cinq ans d'emprisonnement minimum.

Par ailleurs, de nombreux fichiers mis en œuvre par l'Union européenne (Europol, Eurojust) ou des fichiers privés comme le dossier Passenger name record (PNR), utilisés par les compagnies aériennes et transmis notamment aux Etats-Unis, les services de messagerie pour les transactions financières, tous contiennent des données personnelles qui peuvent être transmises à des pays tiers, dont la législation n'est pas aussi protectrice que la nôtre.

La vidéosurveillance

La vidéosurveillance est de plus en plus utilisée dans l'espace public et dans les espaces privés ouverts au public (halls de banques, parkings, etc.). Selon le ministère de l'Intérieur, lors du vote de la loi Loppsi 2, « le mot de "vidéosurveillance" est inapproprié car le terme de "surveillance" peut laisser penser à nos concitoyens, à tort, que ces systèmes pourraient porter atteinte à certains aspects de la vie privé. Dès lors, il y a lieu de remplacer le mot "vidéosurveillance" par le mot "vidéoprotection", qui reflète plus fidèlement tant la volonté du législateur que l'action conduite en faveur de nos concitoyen ». Ainsi devrions-nous utiliser le mot « vidéoprotection[2] ».

Depuis 2006-2007, l'Etat s'est fortement impliqué dans le développement des systèmes de vidéosurveillance, notamment en préconisant le triplement du nombre de caméras sur la voie publique ainsi qu'une participation à hauteur de 50 % de l'Etat pour le financement des frais d'installation. En 2011, la Loppsi 2 a encore favorisé son développement en augmentant la liste des motifs d'installation et des utilisateurs des images. La Cnil estime le nombre de caméras sur la voie publique à 70 000, en mai 2012 le ministère de l'Intérieur l'estimait à 38 000... Outre le fait que les aides au financement piègent les communes qui « oublient » d'intégrer dans leur budget les frais de fonctionnement annuels au-delà de

l'installation, l'utilisation de 60 % du fonds interministériel de prévention de la délinquance (30 millions d'euros) pour ces aides pose problème car il se fait au détriment d'autres dispositifs (patrouilles de police, éducateurs, etc.), bien plus efficaces dans le travail de prévention.

En France, la vidéosurveillance n'a pourtant fait l'objet d'aucune étude d'impact sérieuse et crédible. Mais le constat de sociologues et les bilans faits à l'étranger montrent « l'effet plumeau » des systèmes de vidéosurveillance, la baisse de la délinquance n'étant constatée que lors d'installations après concertation avec la population et associées à d'autres dispositifs de prévention. En outre l'outil serait plus efficace dans les lieux fermés d'où les délinquants ne peuvent fuir facilement une fois l'infraction commise (parkings, etc.). La vidéosurveillance permettrait tout au plus de confirmer après coup l'implication de suspects lorsqu'ils ont été repérés sur les images.

En dehors des sondages d'opinion biaisés qui semblent prouver que les citoyens sont demandeurs de « l'illusion de sécurité » que leur apporte la vidéosurveillance et qui confortent les élus locaux dans leurs décisions d'installer ces systèmes, la vidéosurveillance ne semble bénéficier qu'aux industriels. Elle constitue un risque d'atteinte à la liberté d'aller et venir librement, à la vie privée, que ses maigres résultats ne peuvent justifier.

La biométrie

Les techniques visant à établir l'identité d'une personne en mesurant une de ses caractéris-

2 Réaction sur owni.fr : «Y en a marre de tous ces glissements sémantiques ! « vidéoprotection » c'est limite un oxymore. En tous cas c'est tout sauf vrai, même si c'est dans la loi. Pour avoir été témoin d'une agression d'un chauffeur de bus, je peux témoigner que ça n'est pas la caméra qui s'est levée. C'est moi. Elle, elle n'a rien protégé du tout ».

tiques physiques (ADN, empreintes digitales ou palmaires, iris de l'œil, visage numérisé, flux veineux d'un doigt, etc.) sont de plus en plus utilisées. Les justifications en sont la fiabilité, la rapidité, les gains de temps autorisés par la fluidité des accès (aéroports, cantines, entreprises, etc.). Ainsi, ces techniques sont utilisées pour identifier avec certitude des personnes pour des raisons sécuritaires, ou pour leur donner accès à des services courants administratifs ou privés.

Des données biométriques sont intégrées dans de nombreux fichiers :

• le fichier des passeports biométriques (contient la photo numérisée et les empreintes digitales) ;

• le Fnaeg (contient les empreintes ADN – voir ci-dessus) ;

• le fichier Outil statistique de contrôle des aides au retour (Oscar) contient les données biométriques des bénéficiaires de « l'aide au retour humanitaire » accordée aux Roms reconduits dans leur pays d'origine. Suite à un recours en annulation de la LDH, le Conseil d'Etat a jugé pertinent et adéquat l'enregistrement de la photographie et des empreintes digitales, y compris pour des enfants de plus de 12 ans.

Ces données peuvent aussi être stockées dans des puces RFID (passeports, etc.), dont nous avons vu qu'elles ne constituent pas un support vraiment sécurisé.

Cette utilisation pose la question de la proportionnalité de la technologie utilisée par rapport à l'objectif visé. Est-il nécessaire, en effet, d'utiliser un identifiant biométrique pour qu'un enfant puisse accéder à la cantine ou pour qu'un voyageur puisse couper les files d'attente ?

Sur le plan éthique, l'utilisation du corps comme « instrument de contrôle » est contestable. N'est-il pas dangereux, dans une société, de fonder les relations humaines sur l'identité biologique plutôt que sur l'identité déclarée ? Par ailleurs, aucune garantie n'est donnée quant à la sécurité des supports, et des révélations récentes ont montré que les données de fichiers comme le Stic ou le Fnaeg pouvaient être divulguées par des individus peu scrupuleux (dont ont été victimes, par exemple, des clients ou salariés d'Ikea).

Circulation de l'information et liberté d'expression

La fluidité et la facilité dans l'échange des informations et des prises de position, pour un coût relativement modique, engendrent une évolution dans les formes du débat public et de la construction de l'opinion. Se développe là un espace alternatif à la presse traditionnelle et aux lieux et aux formes des débats habituels. Inscrit dans des réseaux qui ne connaissent ni trêve ni contrôle apparent, chacun peut avoir le sentiment d'être consommateur tout autant que producteur d'informations, à la fois acteur et spectateur dans un monde donnant toutes les apparences de la transparence.

L'internet et les sites web *versus* consommation de l'information

Internet, sur lequel la plupart d'entre nous passent un temps considérable, est devenu peu à peu indispensable, à la mesure de ce qu'il permet de faire au quotidien : accéder à des informations, faire des démarches pratiques, échanger, dialoguer, partager, etc.

Internet est désormais le lieu par excellence de la recherche d'information et de services, et permet de mettre en pratique aussi bien le droit à l'information que le droit à la connaissance.

Cependant, s'il n'est pas possible de nier cet apport considérable, des questions se posent au sujet de cette masse d'informations et de services désormais disponibles :

• La validité de l'information

Ce qui fait la force d'un média, c'est aussi la confiance qu'on peut avoir dans la qualité de ses informations et l'intelligence de ses analyses. Où se trouve désormais la ligne de démarcation entre articles indépendants et informations publiées sous l'emprise de communicants ? Que pèsent les résistances individuelles des journalistes quand ils ne disposent pas collectivement des moyens et trop souvent de la volonté de mener des enquêtes indépendantes, et qu'un affaiblissement collectif des rédactions est constaté face aux pouvoirs économiques et politiques, entraînant des choix qui obéissent à des motivations de plus en plus mercantiles ? En effet si les nouvelles technologies permettent de multiplier les canaux et les formes de diffusion, leur introduction peut se traduire par une détérioration de la qualité du travail : sites adossés à des médias quand ils ne se bornent pas à rediffuser les contenus de ces derniers, pas de rédaction à proprement parler ou de rédaction qui se dédie à l'information et à l'enquête originale, alors même qu'on constate une multiplication exponentielle de chroniqueurs et d'éditorialistes, bien qu'il n'y ait pas de valeur ajoutée en terme de qualité d'information et d'investigation ;

• La place des nouveaux acteurs

Les Tic permettent l'irruption de l'amateur du « marchant » ou du gourou dans la production et la diffusion d'informations et de commentaires : l'information est disponible, mais les règles établies qui contrôlaient l'espace public ne sont plus respectées. Ce qui donne des possibilités de diffusion d'informations erronées, déformées, directement sous influence mercantile, économique ou politique, et permet aussi l'émergence facile de nouveaux gourous tels que les programmes d'enseignement scientiste. Là encore se pose la question de la validité de l'information donnée, avec la question du choix de la source de l'information et de la connaissance. Comment, dans ce foisonnement, discerner une information fiable d'une information biaisée ou d'une désinformation ? Comment repérer ce qui relève de la co-construction d'une connaissance éclairée de la volonté délibérée ou non « d'intox » ? Wikipédia a pu mettre en œuvre des procédures per-

mettant une certaine fiabilité de son contenu en ligne, mais la vigilance reste de mise ;

• Le rôle des moteurs de recherche

La sélection proposée par des moteurs de recherche liés à des buts de profit et fonctionnant sur des critères qui peuvent largement biaiser l'accès à l'information et à la connaissance peut mettre en avant des sites selon des critères très éloignés de l'accès objectif à l'information recherchée ou à la connaissance ;

• L'accès pour tous ?

Enfin l'accès pour tous aux services, et en particulier aux services publics, est un des aspects de la démocratie qu'Internet contribue à faciliter et à améliorer. Il est cependant nécessaire de veiller à ce que ces services restent gratuits et accessibles aux guichets pour ceux qui ne disposent pas de l'accès à Internet.

Les réseaux sociaux web 2.0 Internet *versus* liberté d'expression et émission de contenus

Un des points forts d'Internet est la concrétisation de la liberté d'expression. Aujourd'hui tout un chacun peut prendre la parole sur le web. C'est aussi un lieu possible de co-construction de la connaissance et de l'information, un lieu d'émergence de nouvelles pratiques de mobilisations démocratiques et citoyennes, un lieu aussi de contre-pouvoir, du fait de sa facilité d'utilisation et de diffusion des messages, du fait aussi de son coût réduit.

Le web 2.0 permet donc à ses usagers d'être à la fois récepteurs et émetteurs de contenus. Les usagers constituent le réseau et le font vivre, en participant activement, sur des contenus qui peuvent avoir pour objectif l'exposition de soi ou/et sur des contenus à teneur plus générale et en particulier démocratique et citoyenne.

S'il est maintenant de nombreux exemples de mobilisations démocratiques et citoyennes, l'expression n'y est pas aussi libre qu'il y paraît.

D'une part parce qu'il y a une certaine diabolisation du web et donc mise sous surveillance. Sur Internet nous sommes surveillés et présumés suspects sous prétexte de sécurité. D'autre part, parce que les données agrégées peuvent aussi être utilisées à des fins intéressées d'ordre commercial ou même à des fins policières.

La législation impose ces possibilités de surveillance sur Internet, alors qu'en parallèle la violation de la vie privée ne donne pas lieu à la mise en place de mesures véritablement protectrices. Enfin, à la surveillance institutionnelle de l'Etat, à celle à visée mercantile des entreprises, s'ajoute, sur les réseaux sociaux, une surveillance interpersonnelle, la « surveillance latérale ».

• La législation et la surveillance de l'utilisation du réseau

Plusieurs lois en France autorisent en effet la surveillance. Hadopi, conçue pour protéger les créateurs et l'industrie contre le partage illégal des fichiers, oblige les fournisseurs de services Internet à remettre les identités des internautes associés aux adresses IP (considérées comme des données personnelles) des ordinateurs soupçonnés de piratage. Les internautes sont alors tenus de prouver leur innocence alors que dans un Etat de droit, c'est l'accusateur qui est sensé prouver la culpabilité de l'accusé. La Loppsi 2 autorise l'utilisation de cookies par les pouvoirs publics pour accéder, collecter, enregistrer, stocker et échanger les données informatiques des personnes à leur insu et sans contrôle judiciaire. L'ensemble des moyens de surveillance, basée sur une utilisation accrue des Tic peut conduire à des erreurs reprises par les médias, qui mettent cependant en lumière le degré de surveillance de l'utilisation de la liberté d'expression sur les Ntic.

• La protection des données personnelles

Les réseaux sociaux semblent « être entrés dans les gênes » des nouvelles générations, et s'ils leur permettent une vie sociale virtuelle plus ou moins riche, celle-ci n'est pas toujours sans danger dans la mesure où la diffusion virale des informations peut amplifier dramatiquement des attitudes néfastes comme le cyber-harcèlement dont sont victimes certains adolescents.

Si la violation de la vie privée résulte bien souvent d'un manque de prise de connaissance des possibilités de paramétrage des outils offerts par les réseaux sociaux qui permettent aux utilisateurs de protéger leurs données à caractère personnel, elle est aussi la conséquence de mesures de sécurité insuffisantes. De plus, les fournisseurs de service n'adoptent pas de politique transparente sur la façon dont les données des utilisateurs sont traitées ou partagées. La large couverture médiatique des problèmes rencontrés par certains adeptes des réseaux sociaux ou blogueurs a permis de sensibiliser les utilisateurs qui sont de plus en plus nombreux à exiger au moins le droit à la suppression des données les concernant. Cependant de nombreuses failles demeurent :

- les conditions générales d'utilisation ne sont pas facilement accessibles ou claires et ne sont généralement pas connues ;

- un véritable contrôle doit être proposé et facilement utilisable pour déterminer à quel public les données publiées sont rendues accessibles (limiter l'accès à ses amis ou les rendre totalement publiques) ;

- les données publiées sur les réseaux sociaux peuvent être accessibles sans autorisation ou sans que la personne le sache ;

- le profilage à des fins commerciales reste possible (publicité ciblée) ;

- les données peuvent être conservées, parfois de façon permanente, sans véritable information de l'utilisateur ;

- se désinscrire et supprimer réellement et complètement ses données reste une affaire complexe.

• Vie privée, vie publique, espace privé, espace public

Les réseaux permettent une exposition de soi qui peut autoriser la circulation d'informations que l'utilisateur ne souhaitait pas voir largement divulguées, par la « surveillance latérale ». Il existe toujours le risque de voir des personnes n'appartenant pas au cercle de contacts de prendre connaissance ou de faire usage de ces informations. De ce fait la surveillance devient aussi un contrôle que chacun exerce sur lui-même et sur les autres. Or si les règles du vivre ensemble nous permettent de voir sans regarder, ou d'entendre sans écouter dans des espaces confinés, cet apprentissage est à élargir à cet espace clair-obscur qu'est le web social.

CONCLUSIONS ET RECOMMANDATIONS

Si les débats ont mis en lumière tout l'intérêt des nouvelles technologies pour des avancées en terme de citoyenneté, de démocratie et de liberté d'expression, ils ont cependant fortement souligné les risques et la nécessité d'instaurer des règles plus restrictives en ce qui concerne les détournements possibles des données personnelles à des fins de surveillance et de sécurité.

En effet les gouvernements mettent l'accent sur les questions de sécurité et communiquent abondamment à ce sujet, tandis que la communication sur les droits à la vie privée et aux libertés est quasi inexistante. Les tendances montrent la pression des Etats pour développer de plus en plus de bases de données centralisées contenant des informations sensibles, pour interconnecter les fichiers ou pour développer des systèmes de surveillance directe.

L'autre tendance générale est de mobiliser des informations sensibles au travers de l'utilisation de puces et lecteurs RFID, et de créer des bases de données sans réelle nécessité, souvent sans toutes les garanties nécessaires pour la sécurité, mais avec la possibilité d'une éventuelle utilisation commerciale sans le consentement ou l'information de l'utilisateur.

Ce renforcement récent et spectaculaire des capacités de surveillance doit, dans un Etat de droit, être équilibré par un ensemble de règles, de contrôles et de procédures garantissant les libertés contre l'arbitraire et faisant échec à la société de surveillance.

Les garanties à renforcer d'urgence doivent s'appliquer à la protection de la vie privée et des libertés, aussi bien pour les données personnelles qui ne sont pas dans le domaine public, comme les communications relevant du secret des correspondances au sens large (communications téléphoniques, SMS, MMS, courriels, etc.), que pour celles qui sont dans les fichiers administratifs et de police.

Les orientations données par les débats sont de façon générale fondées sur les principes de protection des données personnelles, notamment définies par l'UE, qui restent à réaffirmer, l'ensemble des garanties devant être pensées en articulation avec les niveaux local, national, européen et international :

- principe de nécessité ;
- principe de finalité ;
- principe de proportionnalité ;
- principe de minimisation et de destruction en fin d'utilisation ;
- principe de durée limitée au strict nécessaire ;
- principe de sécurité de conservation des données ;
- droit à l'information préalable au recueil des données ;
- nécessité du consentement libre et éclairé ;
- droit d'accès avec possibilité de rectification et d'effacement ;
- norme internationale de référence ;
- accords préalables pour les échanges possibles avec des pays tiers, en conformité avec les normes européennes.

Tous ces principes et obligations doivent être garantis et contrôlés par des autorités indépendantes dotées de moyens suffisants pour les exercer.

La LDH propose :

- la garantie constitutionnelle du principe de protection des données personnelles ;
- que la création de tout fichier de police soit réservée à la loi ;
- un « habeas corpus numérique », avec un « référé vie privée et vie personnelle », qui permettrait à chacun de nous de savoir rapidement les éléments de notre vie mis en fiches et de faire rectifier par un juge indépendant les erreurs commises à nos dépens ;

• des Autorités indépendantes en mesure de protéger nos libertés :

- la composition de la Cnil doit mieux garantir son indépendance à l'égard des majorités politiques (désignation par l'Assemblée nationale à la majorité des deux tiers) ;

- elle doit retrouver les pouvoirs qui lui ont été ôtés en 2004, notamment pour s'opposer à la mise en place des fichiers de police ;

- elle doit contrôler toute mise en place de vidéosurveillance numérisée ;

- elle doit être dotée de moyens comparables à ce qui existe ailleurs en Europe ;

- une Autorité européenne indépendante protégeant la vie privée doit être créée à l'échelle de l'Union européenne.

La LDH a pris toute sa part dans les réactions civiques qui se sont multipliées depuis quelques années. Elle entend contribuer au développement de cette prise de conscience et de l'intervention citoyenne, et réaffirme que ces technologies doivent être mises au service non de la surveillance généralisée mais des libertés, notamment d'expression et de communication, plus effectives pour l'ensemble des citoyens.

PUBLICATIONS DE LA LDH

- Hors série ***Hommes & Libertés***
Tous surveillés, tous surveillants ?

- ***Hommes & Libertés*** n°157
Médias, atouts

- ***Guide juridique*** *LDH*
La protection

- ***Guide juridique*** *LDH*
La vidéosurveillance

- ***Une société de surveillance ?***
Etat des droits de l'Homme en France (édition 2009), Ligue des droits de l'Homme, Éditions la Découverte, avril 2009.

- ***Ceux qui nous veulent du bien***
17 mauvaises nouvelles d'un futur bien géré.

- ***Sous surveillance*** - Bande dessinée.

LA LIGUE DES DROITS DE L'HOMME

138, rue Marcadet - 75018 Paris

www.ldh-france.org
ldh@ldh-france.org

Tél. : 01 56 55 51 00

Ligue des droits de l'Homme