Du fichage à la vidéosurveillance : enjeux et questionnements

La LDH a travaillé pendant trois ans, dans le cadre d'un programme soutenu par le conseil régional d'Ile-de-France, sur les questions relatives à l'impact des nouvelles technologies sur les libertés et les droits, notamment sur « fichage, biométrie et vidéosurveillance ». Conclusions et propositions.

Maryse Artiguelong, membre du Comité central de la LDH,
et Viviane de Lafond, déléguée générale de la LDH

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 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 en 2009, mis en place un groupe de travail « Libertés et technologies de l'information et de la communication », mené plusieurs campagnes contre les fichiers[1] et contre la vidéosurveillance. Elle a par ailleurs organisé des réunions publiques, déposé des recours au Conseil d'Etat[2], mis à disposition des outils de réflexion et d'analyse, et s'est impliquée dans plusieurs programmes européens, dont « Données personnelles, des droits ? Informer et sensibiliser les jeunes citoyens européens ».

> *« 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. »*

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

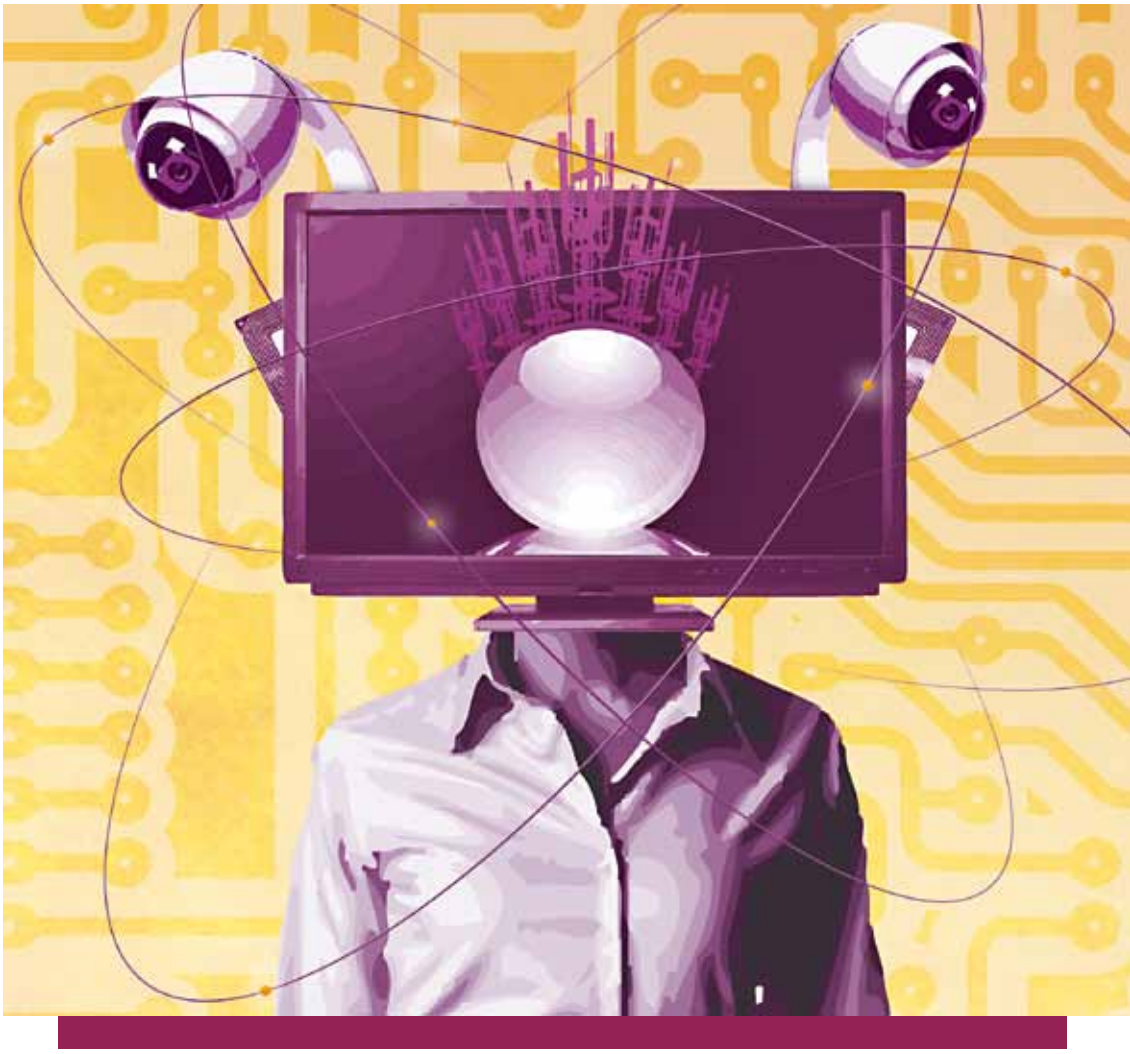
Sensibiliser plus particulièrement les jeunes à l'impact des Tic sur les libertés publiques et à leur importance grandissante dans leur relation à l'exercice de la citoyenneté a été l'objectif de ce programme. Celui-ci a comporté deux axes de travail, l'un autour des questions du fichage, de la vidéosurveillance 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. Ce deuxième volet ayant fait l'objet d'un dossier dans le numéro 157 d'*Hommes & Libertés*, nous avons choisi d'aborder ici le premier axe de travail, soit la question du fichage et de la vidéosurveillance, et d'en synthériser les débats : quels enjeux, quels questionnements et inquiétudes sur ces thèmes, et quelles propositions formulées par la LDH ?[3]

Les Tic au service de l'obsession sécuritaire

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 Internet et les réseaux sociaux, le téléphone portable et le GPS. En même temps, ces Tic laissent des traces involontaires de leur passage. Les citoyens sont fichés, « vidéosurveillés », que ce soit dans leur entreprise, leur cantine, leurs lieux de loisirs ou les transports en commun.

Les facilités que procure l'utili-

sation des Tic fait ainsi oublier à la plupart les risques qu'elle comporte, et nombreux sont ceux qui ne perçoivent pas ou veulent ignorer ces risques d'atteinte à leur vie privée et aux libertés publiques. La volonté de surveillance des citoyens par l'Etat, au nom de l'ordre public, n'est pas nouvelle, mais elle est aujourd'hui exacerbée par l'obsession sécuritaire, l'idéologie du « risque zéro », et favorisée par les progrès des Tic. 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 (avec plus de quarante-deux lois sécuritaires en dix ans).



© DR

Interconnexion et inflation des fichiers

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, par l'élargissement de la finalité première, ou encore par les catégories de populations concernées par ce fichage.

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 est disproportionné par rapport à la finalité première du fichier, cet ADN pourrait révéler, selon les récentes découvertes de chercheurs, des informations importantes sur la santé des individus fichés, ce qui constitue une 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. 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, le Taj permettra de rapprocher des données et offrira des fonctionnalités d'identification des personnes. 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, qu'il s'agisse des nombreux fichiers mis en œuvre par l'Union européenne (Europol, Eurojust) ou des fichiers privés comme le dossier PNR (Passenger Name Record), utilisés

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.

(1) Fnaeg, Base-élèves, Edvige...
(2) Passeport biométrique, fichier Oscar...
(3) Les éléments techniques, juridiques et le détail des analyses sont disponibles dans les outils et documents publiés tout au long de ces trois années, avec deux numéros d'*Hommes & Libertés* (le hors-série « *Tous surveillés, tous surveillants* », printemps 2010, le numéro 157, « Médias, atouts technologiques, défis démocratiques », mars 2012), et deux guides juridiques, « La protection des données personnelles » (2010) et « La vidéosurveillance » (2012).

par les compagnies aériennes et transmis notamment aux Etats-Unis, ou des 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.

Vidéosurveillance : l'illusion de sécurité

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.). 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'en participant à hauteur de 50 % au financement des frais d'installation. En 2011, la Loppsi 2 a 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 soixante-dix mille, en mai 2012 le ministère de l'Intérieur l'estimait à trente-huit mille… 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 (trente millions d'euros) pour ces aides pose problème car il se fait au détriment d'autres dispositifs (patrouilles de polices, 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.

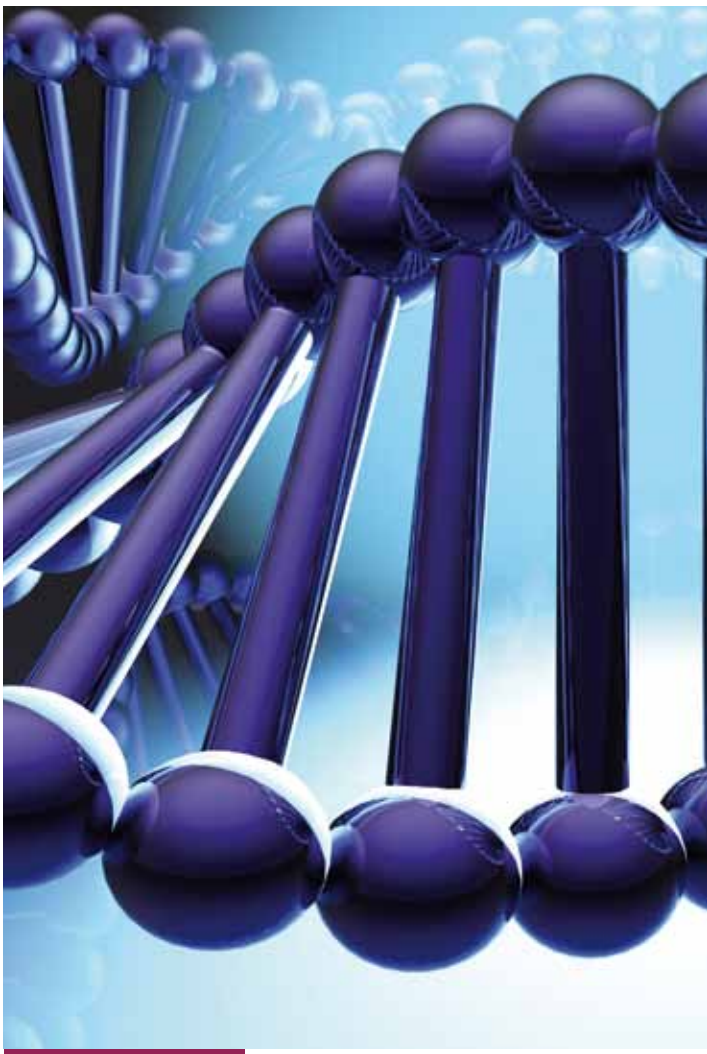
En dehors des sondages d'opinion biaisés qui semblent prouver que les citoyens sont demandeurs de « l'illusion de sécurité » que leur apporte la vidéosurveillance, celle-ci ne semble bénéficier qu'aux industriels. Elle constitue un risque d'atteinte à la liberté d'aller et venir librement, à la vie privée,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

La biométrie au service du contrôle

Les techniques visant à établir l'identité d'une personne en mesurant l'une de ses caractéristiques 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.).

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 leurs 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.

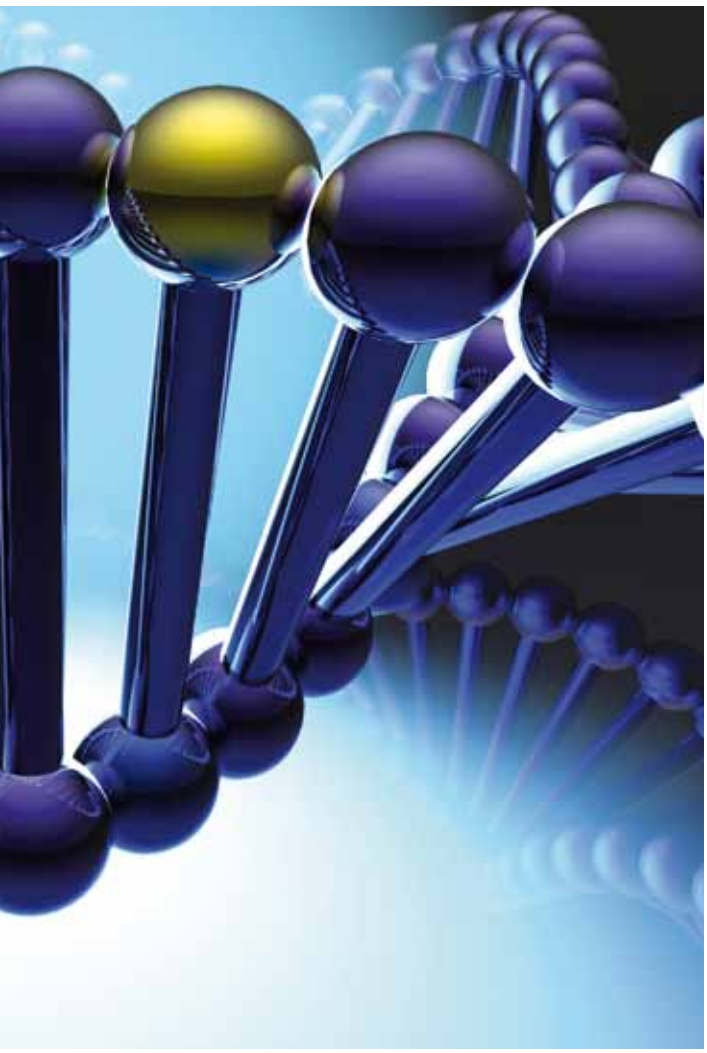


L'utilisation du corps comme « instrument de contrôle » est contestable. N'est-il pas dangereux, dans une société, de fonder les relations humaines sur l'identité biologique plutôt que sur l'identité déclarée ?

Ces données peuvent aussi être stockées dans des puces RFID[4] (passeports etc.), qui 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

(4) L'identification à distance par radiofréquence, de l'anglais *radio frequency identification*.



© DR

exemple, des clients ou salariés d'Ikea). Les débats, s'ils ont mis en lumière tout l'intérêt des nouvelles technologies pour des avancées en termes de citoyenneté, de démocratie et de liberté d'expression, 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.

Protéger les données personnelles

En effet les gouvernements mettent l'accent sur les questions de sécurité et communiquent abondamment sur ce sujet, tandis que la communication sur les droits à la vie privée et aux libertés est quasi inexistante. La tendance est à 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. Il est rare de trouver toutes les garanties nécessaires pour la sécurité ; en revanche existe 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 définis par l'UE, et qui restent à réaffirmer. L'ensemble des garanties doivent être pensées en articulation avec les niveaux local, national, européen et international : principes de nécessité, de finalité, de proportionnalité, de minimisation et de destruction en fin d'utilisation, de durée limitée au strict nécessaire, 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.

> ***« Est-il nécessaire 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 ? »***

Ce que la Ligue des droits de l'Homme suggère

La LDH propose la garantie constitutionnelle du principe de protection des données personnelles, et que la création de tout fichier de police soit réservée à la loi. Elle suggère aussi un « habeas corpus numérique », avec un « référé vie privée et vie personnelle », qui permettrait à chacun de nous de connaître rapidement les éléments de notre vie mis en fiches, et de faire rectifier par un juge indépendant les erreurs commises à nos dépens, et, enfin, des Autorités indépendantes (AA) en mesure de protéger nos libertés. Sur ce dernier point, il est essentiel, pour la LDH, que la composition de la Cnil garantisse mieux son indépendance à l'égard des majorités politiques (désignation par l'Assemblée nationale à la majorité des deux tiers). La Cnil doit par ailleurs 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, et être dotée de moyens comparables à ce qui existe ailleurs en Europe ; enfin, une Autorité européenne indépendante protégeant la vie privée doit être créée à l'échelle de l'Union.

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. ●