Ligue des droits de l'Homme

Résolution adoptée lors du 85ème congrès de la LDH

Société de surveillance, vie privée et libertés

La surveillance des citoyens au nom de l'ordre public, tantôt généralisée et tantôt ciblée sur des « classes dangereuses », est vieille comme l'Etat moderne. Il ne s'agit pas seulement des pratiques de régimes autoritaires telles que le fichier des Juifs de Vichy : c'est dès le règne de Louis XIV que l'on fiche prostituées, mendiants, nomades et mal-pensants ; et l'on sait aussi le profit que tira la police de l'« invention », deux siècles plus tard, des empreintes digitales... sous un régime républicain et démocratique.

A cet ancien tropisme s'ajoute une obsession plus récente qui, insidieusement, fait le lit de la surveillance universelle : l'idéologie du « risque zéro ». L'illusion que le progrès scientifique et technique permettrait une protection contre tous les risques du début à la fin de la vie conduit à accepter des restrictions des libertés et des atteintes à la vie privée. Au nom d'une conception exacerbée du « principe de précaution » ou de l'« insécurité zéro », la « tolérance zéro » remet en cause l'équilibre entre prises de risques inhérentes à la liberté personnelle et protection de l'ordre public. C'est en s'appuyant sur ces fantasmes et sur ces angoisses que l'Etat instrumentalise politiquement la demande sécuritaire et développe des systèmes de surveillance de plus en plus sophistiqués et généralisés.

L'acceptation par les citoyens de l'utilisation systématique des technologies de l'information s'appuie sur les services qu'elle apporte dans la vie quotidienne comme pour l'exercice de la citoyenneté. Sa généralisation est perçue comme inévitable, et elle est souvent organisée, voire imposée, sur des lieux de travail ou de vie en commun. Dans la plupart des cas, le bénéfice immédiat qu'elle procure fait négliger les risques qu'elle comporte. Cette situation est inédite en termes de perception par la population d'un enjeu majeur pour les libertés publiques.

En effet, les progrès immenses des technologies de l'information et de la communication ont aussi accru démesurément les moyens techniques du contrôle social :

- Développement de l'informatique, des techniques de numérisation et de transmission de l'information numérisée et plus précisément des possibilités de numérisation de masse, des capacités de stockage, de tri, de possibilités d'accès par des moteurs de recherche de plus en plus performants de télé-accès, des protocoles d'échanges de données et

d'interconnexion permettant la constitution et la copie de « méga-bases » de données et leur interrogation par des moteurs de plus en plus rapides et surpuissants ;

- Perfectionnement de la surveillance visuelle : la vidéosurveillance recourt désormais à des caméras numériques, parfois « réactives » (présentées comme capables, grâce à des logiciels d'étude du comportement, de détecter des individus devenant suspects et de leur adresser des injonctions phoniques) et d'ici peu d'une taille assez réduite pour permettre la généralisation d'une surveillance invisible ;
- Accroissement des contrôles sur les communications téléphoniques (à partir des opérateurs de téléphonie mobile) et électroniques (à partir des fournisseurs d'accès), d'abord quant à leurs protagonistes et à leurs date et heure de connexion, ensuite aussi quant à leur contenu ;
- Utilisation croissante de la biométrie : prise d'empreintes ADN alimentant des fichiers « génétiques », prise d'empreintes palmaires pour accéder aux lieux de travail ou à des services courants, « biométrisation » des documents d'identité ;
- pistes de « traçage » ouvertes par le perfectionnement des puces permettant une identification à distance par radiofréquence (RFID) et par le développement des nanotechnologies. On peut citer aussi, en tant que traitement pénal, le bracelet électronique dont les dérives croisent celles de la société de surveillance.

En outre, même si les standards imposés par les textes français et européens en matière de protection des données personnelles sont présentés comme plus élevés qu'en d'autres parties du monde, leur efficacité est remise en cause par le caractère transnational des protocoles web et par les échanges internationaux d'informations et de données. Comment appliquer l'obligation d'effacement des données au terme d'une période déterminée face à une entreprise dont le moteur de recherche analyse ses données et stocke ses archives à l'étranger, en particulier aux Etats-Unis ?

Quant aux échanges de données personnelles organisés entre Etats membres de l'Union européenne (notamment par l'extension en 2007 des dispositions du traité de Prüm) voire entre l'Union et des Etats tiers (en particulier l'accord PNR passé avec les Etats-Unis en matière de données relatives aux passagers de vols transatlantiques), ils amplifient considérablement les menaces que font peser ces techniques de surveillance sur la vie privée et les libertés, en élargissant de manière très insuffisamment contrôlée le champ de diffusion des données « sensibles » collectées puis transmises, y compris par des entreprises privées.

Nous sommes donc aujourd'hui très au-delà de l'état des techniques qui avait conduit le Parlement français, après la mobilisation citoyenne contre le projet « SAFARI », à l'adoption de la loi « Informatique, fichiers et libertés » créant notamment la CNIL en 1978.

*
* *

Parce qu'aujourd'hui comme hier « tout homme qui a du pouvoir est porté à en abuser », le renforcement récent et spectaculaire des capacités de surveillance doit, dans un état de droit, être équilibré par un réseau de règles, de contrôles et de procédures garantissant les libertés contre l'arbitraire et faisant échec à la

« société de surveillance » dont la CNIL elle-même craint l'avènement immédiat. Nous sommes très loin de cet équilibre : la multiplication des fichiers, les tentatives de plus en plus nombreuses d'interconnexion, l'explosion de la vidéosurveillance, le développement des puces RFID ont atteint un niveau tel que l'opinion commence à s'en émouvoir bien au-delà des cercles les plus attentifs à la défense des libertés.

Les garanties à renforcer d'urgence doivent s'appliquer à toutes les composantes de la personnalité humaine dont la protection est essentielle au respect de la vie privée et des libertés. C'est le cas des données personnelles (images, renseignements…) qui ne sont pas dans le domaine public comme des communications relevant du secret des correspondances au sens large (communications téléphoniques, SMS, MMS, mails, etc.).

Il s'agit d'abord de garanties substantielles :

- constitutionnalisation du principe de protection des données personnelles, avec inscription explicite de la protection des libertés et de la vie privée face aux technologies de surveillance dans le domaine réservé à la loi par l'article 34 de la Constitution ;
- principe de nécessité et de proportionnalité de la collecte de données personnelles ;
- principe de spécialité des bases de données, qui entraîne l'interdiction d'affecter l'exploitation d'un fichier à plus d'une finalité, affichée et connue du citoyen, la limitation stricte du champ des « utilisateurs » et l'exclusion des interconnexions, qu'il s'agisse de fichiers publics ou privés ;
- principe de transparence et d'accessibilité des résultats de la surveillance aux personnes surveillées ;
- principe d'actualisation périodique sous peine de destruction des données, avec effacement, sur des critères et dans des délais définis lors de la création autorisée du fichier, des images et autres données permettant la « traçabilité » des personnes, qu'elles soient collectées par caméras ou par d'autres procédés de saisie ;
- principe d'effacement automatique périodique par purge des données personnelles figurant dans les fichiers de police et de gendarmerie cinq ans après leur collecte sauf en matière criminelle, et au bout d'un an en l'absence de poursuites judiciaires ;
- interdiction d'inscription sur des fichiers de police et de gendarmerie des mineurs de moins de 16 ans et soumission à justification, au regard de conditions légales strictes et précises, de l'inscription des mineurs âgés de 16 à 18 ans ; purge des données en cas d'absence de nouvelle inscription dans les six mois du fait générateur de la précédente, et effacement des données à la majorité ;
- principe d'interdiction de la cession à des organismes privés des données recueillies par un organisme public.

Ces garanties, qui peuvent et doivent être conciliées avec d'autres objectifs constitutionnellement légitimes (tels que le maintien de l'ordre public), ne sauraient s'effacer devant ces derniers en aucune circonstance.

Il s'agit ensuite de garanties procédurales :

- contrôles parlementaires, y compris sur l'activité de services secrets de surveillance ;

- contrôles d'Autorités réellement « indépendantes » par leur composition, dont les décisions doivent être portées à la connaissance des citoyens et qui doivent disposer de pouvoirs juridiques réels (pouvoir d'autorisation des fichiers d'Etat, pouvoirs d'intervention et de contrôle sur la gestion des fichiers de police et de gendarmerie) et de moyens à la hauteur de leurs tâches; la CNIL doit en particulier retrouver les pouvoirs qu'on lui a retirés en 2004;
- extension de cette logique de protection des libertés contre l'interopérabilité des fichiers à l'échelle européenne, par la création d'une Autorité indépendante dotée de pouvoirs et de moyens conséquents à l'échelle de l'Union, et à l'échelle planétaire sous l'égide de l'ONU ;
- octroi de moyens effectifs au Parquet pour garantir l'effacement, dans les fichiers judiciaires et policiers, des données concernant des personnes mises hors de cause, relaxées ou acquittées, amnistiées ou graciées ;
- contrôles juridictionnels, avec l'attribution au juge du pouvoir d'ordonner la communication de données (soit aux intéressés, soit dans des cas tels que le « secret défense » à des personnes habilitées indépendantes de l'Administration), la rectification, l'effacement et l'anonymisation, dans le cadre d'une procédure de « référé vie privée et données personnelles »;
- consultation des citoyens, qui doivent être pleinement informés, éclairés, et valablement consultés pour tout projet les concernant de création de fichiers ou de mise en oeuvre des technologies de surveillance.

Toutes ces garanties doivent être pensées dans une articulation entre les niveaux local, national, européen et international, toute coopération interétatique devant être subordonnée à la « sécurisation » des droits des personnes visées par les procédés de surveillance au regard des différences de systèmes politiques et juridiques.

*
* *

Les libertés et la vie privée doivent être aussi protégées contre l'utilisation de ces mêmes outils intrusifs par des entreprises du secteur marchand, dont Google n'est que l'exemple le plus spectaculaire. Elles doivent même l'être contre les risques induits par le brouillage entre vie privée et vie publique en termes de communication « volontaire » mais éventuellement irréfléchie de données personnelles sur des « réseaux sociaux ».

Sur ce terrain, les garanties substantielles à promouvoir, qui supposent une définition précise de l'« identité numérique » à protéger, résident :

- dans le principe du « consentement éclairé et révocable » du citoyen, du consommateur, de l'internaute, du membre potentiel d'un « réseau social » ;
- dans le développement de l'information sur les risques ;
- dans le développement d'une pédagogie de l'exposition sur Internet ;
- dans l'interdiction de toute cession de données et de toute interconnexion sans le consentement exprès des personnes qui les ont fournies ;

Les garanties procédurales ne diffèrent pas ici sensiblement de celles qui doivent équilibrer l'augmentation des moyens administratifs et policiers de surveillance des citoyens. Il faut toutefois y ajouter l'ouverture de droits de rectification et d'effacement des données personnelles dont l'évolution de la diffusion, même

dans un cadre contractuel initial, doit rester dans toute la mesure techniquement possible sous le contrôle de la personne concernée – ce qui suppose là encore une concertation internationale et d'abord européenne.

*
* *

C'est un champ décisif de la défense des droits fondamentaux qui s'ouvre au débat, et qui revêtira à bref délai autant voire plus d'importance pour les libertés de chacun de nous que les objets classiques de vigilance face aux appareils de répression plus visibles. L'utilisation des nouvelles technologies de l'information et de la communication pour construire une « traçabilité totale » peut conduire, à l'échelle internationale, à une rupture avec les principes d'exercice démocratique des pouvoirs, sans que l'on puisse aujourd'hui mesurer toutes les conséquences des évolutions en cours. Cette situation impose une réflexion et une mobilisation à la hauteur des enjeux.

La LDH a pris toute sa part dans des réactions civiques qui se sont multipliées depuis plusieurs années : « Pas de zéro de conduite pour les enfants de moins de trois ans » ; refus de l'utilisation du numéro de Sécurité sociale pour le dossier médical personnalisé ; mobilisations contre « Base élèves » et contre « EDVIGE ». Ces mouvements ont contribué à une prise de conscience des enjeux des technologies de l'information et de la communication en termes de protection de la vie privée et des libertés. Ils ont obtenu des succès, mais nous devons rester mobilisés sur les questions essentielles que sont la diffusion de données nominatives, la durée excessive de leur conservation et les dangers d'interconnexions qui résultent notamment du recours à des identifiants nationaux même sectoriels.

La Ligue des droits de l'Homme entend contribuer au développement de cette prise de conscience et de l'intervention citoyenne, refusant que des avancées scientifiques soient détournées par les tenants du contrôle social, du conditionnement des consommateurs ou de l'idéologie sécuritaire. Elle réaffirme que ces technologies doivent être mises au service non de la surveillance généralisée mais de libertés, notamment d'expression et de communication, plus effectives pour l'ensemble des citoyens.