JURIDIQUE

Sécurité et libertés : vers un meilleur compromis ?

Retour sur l'encadrement de la surveillance de l'Internet. On ne peut opposer sécurité et droit à la protection de la vie privée. Mais l'équilibre est difficile et instable…

En 30 ans, les technologies ont bouleversé toutes nos règles sociétales, éducationnelles, institutionnelles, économiques, juridiques… Dans ce contexte d'évolutions permanentes, la préservation de nos libertés est une préoccupation de première importance, car, dans une société démocratique, il n'est pas pensable d'assurer la sécurité des citoyens au détriment de leurs libertés individuelles les plus fondamentales, telles que la liberté d'expression ou le droit au respect de leur vie privée. Nous savons depuis longtemps que nos données personnelles sont exploitées à notre insu[1]. Mais c'est Edward Snowden qui a véritablement donné l'alerte en juin 2013, provoquant même un électrochoc à l'échelle de la planète, en révélant l'existence du programme PRISM - ce logiciel qui permet à la NSA et au FBI d'accéder aux données détenues par les grands acteurs de l'internet et de consulter ainsi toutes les informations relatives aux internautes. Dans la suite de cette affaire, le G29 a dénoncé l'illégalité de cette *« surveillance massive, systématique et sans distinction des citoyens européens »*[2].

En France, l'essor de la cyberdélinquance, de la cybercriminalité et du cyberterrorisme a conduit le législateur à renforcer les pouvoirs et les moyens d'enquêtes des autorités chargées d'enquête dans l'environnement numérique.

Des interceptions limitées aux écoutes téléphoniques avant 1991 et pratiquées sur commission rogatoire

On rappellera que, avant 1991, les interceptions étaient limitées aux écoutes téléphoniques et étaient pratiquées exclusivement sur commission rogatoire, sur le fondement de l'article 81 du code de procédure pénale : *« le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité »*.

Mais l'arrêt Kruslin c. France de la Cour européenne des droits de l'homme (CEDH, 24 avril 1990) a rappelé qu'il ne peut y avoir ingérence d'une autorité publique dans

L'auteur

Christiane Féral-Schuhl, ***ancien Bâtonnier du Barreau de Paris, Avocate Associée du cabinet Féral-Schuhl/ Sainte–Marie qu'elle a fondé en 1988 avec Bruno Grégoire-Sainte-Marie, est spécialiste des nouvelles technologies.***

(1) Dès 1997, Bill Gates dénonçait des *« entreprises du secteur privé et des administrations (qui) possèdent (…) une masse d'informations sur notre compte »*, ajoutant que *« nous n'avons aucune idée de la manière dont elles l'utilisent et si elle est exacte… »* (B. Gates, La vie du futur - éd. R. Laffont 1997)

(2) *« Affaire PRISM : avis du G29 sur la surveillance massive des citoyens européens »*, http://www.cnil.fr/linstitution/actualite/article/article/affaire-prism-avis-du-g29-sur-la-surveillance-massive-des-citoyens-europeens/

l'exercice du droit au respect de la vie privée et familiale, du domicile et de la correspondance que pour autant qu'elle est prévue par une loi accessible et prévisible et qu'elle est nécessaire, dans une société démocratique, à la poursuite d'un but légitime. Estimant que *« les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance »*, la Cour a précisé qu' *« elles doivent se fonder sur une «loi»* d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner ».

C'est donc dans la suite de cet arrêt que la France a promulgué la loi du 10 juillet 1991 qui encadre les interceptions judiciaires et administratives.

Les interceptions judiciaires ont été placées sous le contrôle étroit de l'autorité judiciaire, *« gardienne des libertés individuelles »* (Constit., art. 66). Par ailleurs, les correspondances avec un avocat et celles avec un journaliste permettant d'identifier une source ne peuvent être retranscrites.

Pour les interceptions administratives, la loi s'articule autour de cinq piliers : (I) la protection du secret de toutes les correspondances et des communications électroniques[3] ; (II) la définition des motifs susceptibles de justifier qu'il soit porté atteinte à cette protection : la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité organisée et de la reconstitution ou du maintien de groupements dissous[4] ; (III) la compétence du Premier ministre pour décider de procéder à l'interception de correspondances par une décision écrite et motivée[5] ; (IV) la limitation du nombre et de la durée d'autorisation de l'interception[6] et de conservation des enregistrements des écoutes[7] ; (V) l'autorisation de la transcription des seuls enregistrements ayant reçu une autorisation, les enregistrements touchant à la vie privée ne pouvant être conservés lorsqu'ils ne sont plus indispensables à la réalisation de ces finalités.

La loi a prévu dans le même temps la création d'une autorité administrative indépendante, la Commission

Il faut donner des garanties au citoyen

Il ne s'agit en aucun cas d'opposer le droit à la protection à la vie privée au droit à la sécurité. En revanche, il faut donner au citoyen des garanties. C'est dans cet objectif que la Commission parlementaire de réflexion sur les droits et les libertés à l'âge du numérique installée par Claude Bartolone en juin 2014 a formulé plusieurs recommandations[11].

[3] Article L. 241-1 du code de la sécurité intérieure. [4] Articles L. 241-1 et L. 241-2 du même code. [5] Article L. 242-1 du même code. [6] Article L. 242-3 du même code. [7] Article L. 242-6 du même code.

[11] V. ses recommandations http://www2.assemblee-nationale.fr/14/commissions-permanentes/numerique/a-la-une/recommandation-sur-le-projet-de-loi-relatif-au-renseignement

nationale de contrôle des interceptions de sécurité (CNCIS) chargée de veiller au respect de ces dispositions, les décisions motivées du Premier ministre lui étant communiquées en principe dans les 48 heures.

Les interceptions sont étendues aux données de connexion avec la loi de 2004

Avec la loi du 9 juillet 2004, les interceptions limitées jusque-là aux écoutes téléphoniques ont été étendues aux données de connexion. Leur accès devient possible à des fins de police judiciaire, mais toujours sur autorisation préalable du juge d'instruction dans le cadre d'une information judiciaire ou du juge des libertés et de la détention dans le cadre des enquêtes préliminaires et de flagrance.

Le périmètre de surveillance sur internet s'élargit significativement avec la loi du 18 décembre 2013 relative à la programmation militaire (LMP). Le législateur ouvre l'accès aux données de contenu et non plus seulement aux données de connexion. En effet, sont désormais susceptibles d'être réquisitionnés les *« informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications »* (CSI, art. L 246-1). Comme ces informations et documents peuvent être recueillis *« sur sollicitation du réseau et transmis en temps réel »* (CSI, art. L 246-3 du CSI), cela revient à un accès direct (dit « back door ») à l'image du programme américain PRISM évoqué précédemment, les agents de services de renseignement pouvant ainsi se raccorder directement aux réseaux des opérateurs.

Par ailleurs, les bénéficiaires du droit d'accès incluent désormais, outre les services de police et de gendarmerie, les agents habilités des services des ministères de la Sécurité intérieure, de la Défense nationale, de l'Économie et du Budget.

Enfin, les demandes d'accès doivent être soumises à une autorisation spécifique du Premier ministre (ou des personnes spécialement désignées par lui) et non plus du ministre de l'Intérieur. Comme chaque décision d'autorisation, délivrée pour une durée de 30 jours renouvelable, doit être communiquée au président de la CNCIS, de nombreuses associations de protection et de défense des droits des internautes ainsi que plusieurs acteurs de l'internet ont dénoncé un contrôle administratif a posteriori ouvrant la voie à un contrôle des pouvoirs publics sans précédent.

Si la loi du 28 mars 2014 autorise la géolocalisation, elle limite son recours à certaines infractions (punies d'au moins cinq ans d'emprisonnement pour les délits d'atteinte aux biens, de trois ans pour les délits d'atteinte aux personnes, de recel de crime ou d'évasion, et de cinq ans pour les délits douaniers). Elle exige le contrôle du juge d'instruction et le juge des libertés et de la détention. Elle interdit la géolocalisation dans les locaux professionnels et le domicile des avocats et des journalistes, dans les locaux et véhicules d'une entreprise de presse et dans les cabinets des médecins, notaires et huissiers et ne peut pas concerner les parlementaires et les magistrats.

Avec la loi sur la surveillance du 24 juillet 2015, une étape de plus est franchie : les autorités administratives peuvent recourir à des outils jusqu'ici dévolus à la sphère judiciaire (captation, fixation, transmission et enregistrement de sons, d'images et de données informatiques ; géolocalisation en temps réel) ou encore à des techniques nouvelles. Elles ont la possibilité d'imposer aux opérateurs la mise en place de dispositifs permettant au moyen d'algorithmes, d'identifier en temps réel dans la masse des données, des comportements suspects, par exemple, la fréquentation de certains sites, ou des connexions fréquentes avec certaines personnes *« préalablement identifiées comme présentant une menace »* (sondes). L'entourage d'une personne visée par une mesure d'interception de sécurité peut faire l'objet d'une surveillance électronique au moyen de dispositifs techniques de proximité de captation directe de métadonnées, voire du contenu des communications (IMSI-catcher[9]). Semblables à des cellules téléphoniques, ces techniques permettent d'intercepter de manière systématique et automatique des données relatives à des personnes pouvant n'avoir qu'un lien géographique avec un suspect : leurs numéros de téléphone, les SMS, le contenu des conversations et le trafic internet, les balayages de ports (port scanning), les enregistreurs de mots de passe ou de frappe (keyloggers). Pour pouvoir détecter ces « *signaux faibles* [10] », les services de renseignement sont également autorisés à introduire des appareils de captation, de transmission et d'enregistrement de sons, d'images et de données informatiques dans un véhicule, un lieu privé ou un système automatisé de traitement de données.

Certaines catégories de personnes restent préservées : les parlementaires, magistrats, avocats et journalistes ne peuvent pas être l'objet d'une demande de mise en œuvre d'une des techniques de renseignement à raison de l'exercice de leur mandat ou de leur profession (art. L. 821-7 et L.854-3).

La montée en puissance de la surveillance sur internet met la question du respect des libertés individuelles au cœur des préoccupations. Faut-il pour autant parler d'une dictature du numérique ? Si certains considèrent que la surveillance des réseaux est « justifiée » pour assurer la sécurité des citoyens, d'autres expriment de sérieuses inquiétudes, invitant à rechercher un meilleur équilibre entre sécurité et libertés. ■

[9] International Mobile Subscriber Identity (IMSI)

[10] Savoir que tel individu s'est connecté à tel autre individu bien connu des services depuis des années est une information qui s'appelle un « signal faible ». C'est en mettant ensemble les signaux faibles qu'il est possible de détecter un éventuel projet d'attentat