Droits fondamentaux et lutte contre la cybercriminalité et le cyberterrorisme

Christiane Féral-Schuhl*
Ancien Bâtonnier de Paris, Cabinet FERAL-SCHUHL/SAINTE-MARIE
(* Les observations contenues dans cet article appartiennent à leur auteur et n'engagent pas d'autres organismes ou personnes)

Avec le développement de la cybercriminalité et du cyberterrorisme, de nouvelles techniques d'enquête et d'investigation ont été mises à la disposition des services de renseignement pour leur permettre d'identifier sur l'internet d'éventuels suspects. Les algorithmes tout particulièrement ouvrent de formidables possibilités de comparaison des données collectées et facilitent la conservation et l'exploitation des données, notamment des images grâce au passage de l'analogique au numérique. L'exploitation de telles données, leur croisement avec d'autres informations, le recours massif et indiscriminé à des technologies intrusives, sont autant de moyens de prédire la probabilité qu'un fait délictueux ou criminel se produise à tel endroit et à tel moment.

Mais, cette surveillance de masse sur internet peut s'avérer disproportionnée par rapport aux objectifs légitimes de prévention de la délinquance et de répression des infractions. Le sujet n'est pas récent puisque, dès 1997, Bill Gates dénonçait les « 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… »[1]. Mais c'est Edward Snowden qui a véritablement donné l'alerte en juin 2013, provoquant même un électro-choc 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 (Yahoo, Microsoft, Google…) 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], précisant que de « telles restrictions aux droits fondamentaux des citoyens européens ne sont pas acceptables dans une société démocratique » et ne constituent en rien de « modestes empiétements sur la vie privée permettant de prévenir les attentats », comme l'avait justifié Barack Obama[3].

Faut-il pour autant parler d'une dictature du numérique ? Certains – 57 % de français selon le baromètre Organe/Terrafemina publié le 25 février 2014 – considèrent que la surveillance des réseaux est « justifiée », précisément pour assurer la sécurité des citoyens. Toutefois, plus de la moitié d'entre eux soutiennent qu'« une volonté politique forte peut protéger la confidentialité des échanges privés sur Internet ». D'autres émettent de sérieuses critiques, invitant à rechercher un meilleur équilibre entre sécurité et libertés, à l'instar de la loi du 24 juillet 2015 qui a entrepris de renforcer les moyens de surveillance de l'autorité administrative.

1. B. Gates, La vie du futur (éd. R. Laffont 1997).
2. Avis du G29 du 10 avril 2014 sur la surveillance de masse des citoyens européens ; v. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf ; v. égalt. : « 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/
3. « Le FBI accède aux serveurs de Google, Skype et Facebook, Obama assume » Les Echos, 7 juin 2013.

Dossier spécial

LA LOI RENSEIGNEMENT NO 2015-912 DU 24 JUILLET 2015 A PLACÉ LA QUESTION DU RESPECT DES LIBERTÉS FONDAMENTALES – NOTAMMENT LE RESPECT DE LA VIE PRIVÉE ET LA PROTECTION DES DONNÉES PERSONNELLES – AU CŒUR DES PRÉOCCUPATIONS

Un texte censuré par le Conseil Constitutionnel pour atteintes aux droits fondamentaux des citoyens

Fait inhabituel, le Conseil Constitutionnel a été saisi par le Président de la République lui-même – une première sous la Ve République – et par 60 parlementaires. Si la Haute juridiction, dans sa décision du 23 juillet 2015[4], a validé dans sa globalité le dispositif, elle a néanmoins censuré certains articles en ce qu'ils représentaient une réelle menace pour le respect des droits fondamentaux des citoyens. En effet, ont été déclarés contraires à la Constitution les dispositions du nouvel article L. 821-6 CSI qui instituait une procédure dérogatoire d'installation, d'utilisation et d'exploitation des appareils ou dispositifs techniques de localisation en temps réel d'une personne, d'un véhicule ou d'un objet, d'identification d'un équipement terminal ou du numéro d'abonnement ainsi que de localisation de cet équipement ou d'interception des correspondances émises ou reçues par cet équipement « en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement ». Cette procédure dite d'urgence opérationnelle, encore plus dérogatoire que celle, exceptionnelle, de l'urgence absolue, constituait, ainsi que l'a relevé le Conseil constitutionnel, « une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances » (considérants 27 à 30). Cette disposition a été limitée par le Conseil constitutionnel à une seule hypothèse : l'urgence « absolue ». De même, s'agissant des dispositions de l'article L. 854-1 CSI qui prévoyait la réduction des contrôles a priori pour faciliter la surveillance des échanges entre une personne située en France et une personne située à l'étranger, le Conseil Constitutionnel a considéré que le législateur n'avait pas déterminé les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques » (considérants 76 à 79).

Un texte qui opère un élargissement significatif du champ des interceptions de sécurité

Avec le nouveau texte, entré en vigueur dans sa version expurgée le 3 octobre 2015, les moyens d'enquêtes deviennent accessibles non seulement aux services de police et de gendarmerie, mais également aux agents habilités des services des ministères de la Sécurité intérieure, de la Défense nationale, de l'Economie et du Budget.

Le dispositif permet de cibler, outre les suspects, les personnes appartenant à leur entourage, et de recueillir les données techniques de connexion les concernant. Il autorise la mise en œuvre (i) d'un recueil des données de connexion auprès des opérateurs de communications électroniques et des personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, des Fournisseurs d'Accès à Internet et des fournisseurs de services d'hébergement (visés à l'art. L851-1) ; ces dispositifs doivent permettre, 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 ou « boîtes noires ») (CSI, art. L851-3) ; (ii) de la géolocalisation, c'est-à-dire la localisation des équipements terminaux (CSI, art. L851-4) ; (iii) de balises, c'est-à-dire l'utilisation d'un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet (CSI, art. L851-5) ou encore l'IMSI *catcher*[5], c'est-à-dire un appareil ou dispositif technique qui permet de recueillir directement les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés (art. L851-6) ; semblables à des cellules téléphoniques, ces techniques permettent

4. Cons. Constit. décision n° 2015-713 DC du 23 juillet 2015.
5. International Mobile Subscriber Identity (IMSI) ;

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*) ; (iv) des interceptions de correspondances émises par la voie des communications électroniques (CSI, art. L852-1) ; (v) de la sonorisation de certains lieux et véhicules et la captation d'images à l'aide de micros et de caméras espions (CSI, art. L 853-1) ainsi que de donnés informatiques à l'aide de mouchards informatiques (CSI, art. L 853-2) ; (vi) de mesures de surveillance des communications électroniques internationales (CSI, art. L 854-1 à L 854-9).

Certes, le législateur encadre le recours à ces moyens et techniques de surveillance

Il pose les principes et finalités de la politique publique de renseignement, fixe la procédure d'autorisation des techniques de recueil du renseignement, définit la composition, les missions et les prérogatives de l'autorité administrative indépendante qui sera chargée de contrôler la mise en œuvre de ces techniques, introduit un recours juridictionnel permettant de contester cette mise en œuvre et encadre les conditions d'utilisation de chaque technique.

Ainsi, les mesures doivent-elles être préalablement autorisées par le Premier ministre (ou des personnes spécialement désignées par lui) et après avis de la Commission nationale de contrôle des techniques de renseignements (CNCTR[6]). Le Premier ministre assure également la traçabilité de la mise en œuvre des mesures autorisées, ainsi que la conformité de la centralisation, de l'exploitation, de la conservation et de la destruction des renseignements collectés.

De même, il est prévu que la CNCTR peut s'autosaisir ou être saisie par « toute personne y ayant un intérêt direct et personnel ». Elle peut ainsi être saisie de réclamation par toute personne souhaitant vérifier qu'aucune technique suspectée n'est irrégulièrement mise en œuvre à son égard. Elle peut également être saisie par tout agent d'un service de renseignement qui aurait connaissance, dans l'exercice de ses fonctions, de faits susceptibles de constituer une violation manifeste du cadre légal. L'agent fait également l'objet d'une protection spécifique contre toute mesure défavorable qui pourrait être prise à son encontre en raison de ce signalement. Ce droit/devoir de signalement des agents fait l'objet d'une protection expresse contre toute mesure défavorable qui pourrait être prise à son encontre en raison de ce signalement (CSI, art. L. 861-3). La CNCTR peut alors saisir le Conseil d'Etat et en informer le Premier ministre. Elle a le devoir de saisir le procureur de la République, dans le respect du secret de la défense nationale, si elle estime que l'illégalité est susceptible de constituer une infraction. Elle doit alors transmettre l'ensemble des éléments portés à sa connaissance à la Commission consultative du secret de la défense nationale afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République. Elle procède aux vérifications nécessaires et notifie à l'auteur de la réclamation qu'il y a été procédé, sans confirmer ni infirmer la mise en œuvre de la technique. En cas de manquement estimé dans la délivrance d'une autorisation de mise en œuvre d'une technique, dans la mise en œuvre d'une technique autorisée ou dans la collecte, la transcription, l'extraction, la conservation ou la destruction des renseignements collectés, la CNCTR adresse au Premier ministre, au ministre responsable et au service concerné une recommandation tendant à l'interruption de la mise en œuvre de la technique en cause et/ou à la destruction des renseignements collectés. La CNCTR rend un rapport annuel circonstancié de son activité. Globalement, on peut observer que si la CNCTR dispose de larges missions, elle dispose dans les faits de moins de pouvoirs que ceux de la CNIS[7] qui pouvait opérer en temps réel.

Par ailleurs, le contrôle juridictionnel relève de la compétence d'une formation spécialisée du Conseil d'Etat. Statuant en premier et dernier ressort, celle-ci pourra être saisie par la CNCTR ainsi que par toute personne souhaitant vérifier qu'aucune technique suspectée n'est irrégulièrement mise en œuvre à son égard et justifiant

6. Autorité administrative indépendante dont la création a été prévue par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.
7. L'ancienne autorité administrative indépendante Commission Nationale Consultative des Interceptions de Sécurité (CNCIS) à laquelle s'est substituée la CNCTR.

(hors requête en référé) réclamation préalable auprès de la CNCTR. Elle peut également être saisie par la CNCTR (à la majorité absolue de ses membres) lorsque le Premier ministre ne donne pas suite à ses avis ou recommandations (CSI, art. L. 821-6) ou encore à la demande d'au moins deux membres de la CNCTR en cas de recours à des techniques particulièrement intrusives (CSI, L. 853-2). Enfin, la saisine peut encore être faite à titre préjudiciel par une juridiction administrative ou une autorité judiciaire saisie d'une procédure ou d'un litige dont la solution dépend de l'examen de la régularité d'une technique de recueil de renseignement. Le Conseil d'Etat peut donc prononcer l'annulation de la mesure et la destruction des données collectées lorsqu'il constate qu'une technique de recueil de renseignement est ou a été mise en œuvre illégalement ou que des renseignements ont été conservés illégalement. Il en informe alors le requérant ou la juridiction de renvoi et peut condamner l'Etat à indemniser le préjudice subi. Il avise le procureur de la République s'il estime que l'illégalité constatée est susceptible de constituer une infraction.

Mais le dispositif légal est insuffisant pour prévenir les risques d'atteinte aux droits et libertés fondamentales

L'article L. 851-3 du CSI nous en donne une illustration. En autorisant les opérateurs de communications électroniques et les fournisseurs de services à exploiter des informations et documents traités par leurs réseaux afin de détecter des connexions susceptibles de révéler une menace terroriste (détection de « signaux faibles » par la pose de « boîtes noires » chez les opérateurs), le législateur a ouvert la voie à la collecte massive et à un traitement généralisé de données personnelles.

Aussi, des garanties complémentaires apparaissent indispensables. Plusieurs propositions ont été formulées dans cet objectif, notamment par la Commission parlementaire de réflexion sur les droits et libertés à l'âge du numérique[8]. Celle-ci préconise d'« interdire le recours à des dispositifs algorithmiques de traitements de données transitant par les réseaux numériques aux fins de détection de « signaux faibles » ou de menaces, quelle que soit la finalité poursuivie » (Recomm. nº 69). Elle suggère également d'« encadrer par la loi le recours à l'ensemble des techniques et moyens susceptibles d'être à la disposition des services de renseignement pour remplir leurs missions et mettre un terme aux éventuelles pratiques illégales en sanctionnant plus durement les infractions à la législation » (Recomm. nº 70). Elle considère que, pour être véritablement protecteur des libertés fondamentales, il conviendrait d'« accorder aux citoyens des garanties fondamentales face aux activités de surveillance administrative par la définition précise des conditions et motifs des atteintes susceptibles d'être portées aux droits à la vie privée et à la protection des données personnelles, la réaffirmation de leur proportionnalité et subsidiarité, l'encadrement de la surveillance des communications à l'étranger et l'instauration de voies de recours effectives pour contester certaines pratiques » (Recomm. nº 72). Par ailleurs, elle invite à garantir l'indépendance institutionnelle de la CNCTR en instaurant « un contrôle externe permanent de la mise en œuvre des techniques de renseignement par la création d'une autorité administrative indépendante et impartiale, dotée des moyens humains, matériels, techniques et financiers suffisants » (Recomm. nº 73). En complément de ce contrôle externe doivent continuer de s'appliquer le contrôle interne et interministériel des services par l'inspection du renseignement mise en place en 2014[9] – dont il convient de renforcer les moyens et les prérogatives d'investigation afin d'en faire un contrôle interne méthodique et incontestable – et le contrôle politique de l'action du Gouvernement par la délégation parlementaire au renseignement créée en 2007[10]. Enfin, elle recommande de « confier à cette autorité des compétences élargies à l'ensemble des services de renseignement et à l'intégralité des mesures qu'ils sont susceptibles de prendre, en lui donnant des prérogatives de contrôle a priori, en cours d'opération et a posteriori ainsi qu'un pouvoir de recommandation et en lui permettant de saisir un juge en cas de méconnaissance des obligations légales par le pouvoir exécutif » (Recomm. nº 74).

8. Voir les travaux de cette commission co-présidée par C. Paul et C. Féral-Schuhl http://www2.assemblee-nationale.fr/14/autres-commissions/numerique ; voir le rapport http://www.assemblee-nationale.fr/14/pdf/rapports/r3119.pdf
9. Par le décret nº 2014-833 du 24 juillet 2014 relatif à l'inspection des services de renseignement.
10. En application de l'article 6 nonies de l'ordonnance nº 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

En conclusion, si la loi sur le renseignement s'inscrit dans l'objectif de préserver le droit à la sécurité du citoyen – dont on rappellera qu'il est « un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives » (CSI, art. L. 111-1 ; L. 21 janvier 1995[11]) – elle doit ménager un juste équilibre entre les nécessités constitutionnelles de préservation de l'ordre public et les droits de chacun au respect de sa vie privée, de sa correspondance, de son domicile et de ses données personnelles. D'une part, elle doit respecter le principe du secret des correspondances et des communications électroniques, qui ne peuvent être surveillées que « *dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* »[12], sous le contrôle de l'autorité judiciaire ou d'un mécanisme présentant des garanties suffisantes. D'autre part, elle doit être conforme à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 et à l'article 8 de la CESDH aux termes duquel il ne peut y avoir ingérence d'une autorité publique dans 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[13].

Dans cet objectif, ne serait-il pas temps d'« inscrire explicitement dans la Constitution le droit au respect de la vie privée et l'exigence de protection des données à caractère personnel afin de réévaluer l'importance accordée à ces libertés fondamentales en droit interne ? »[14] Cette consécration rapprocherait la France de plusieurs autres pays européens, notamment l'Allemagne et la Grèce, rappelant combien la protection de la vie privée doit rester une liberté fondamentale au XXIe siècle. Cela permettrait également une plus grande prise en considération de ces droits lors de l'élaboration des lois tendant à lutter contre la cybercriminalité et le cyberterrorisme.

11. L. nº 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.
12. CEDH, 6 septembre 1978, Klass et autres c. Allemagne.
13. CEDH, 24 avril 1990, Kruslin c. France, nº 11801/85.
14. Recommandation nº 47 de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique.