ANNUAIRE FRANÇAIS DE RELATIONS INTERNATIONALES

2016

Volume XVII

PUBLICATION COURONNÉE PAR
L'ACADÉMIE DES SCIENCES MORALES ET POLITIQUES

(Prix de la Fondation Edouard Bonnefous, 2008)

Université Panthéon-Assas
Centre Thucydide

LE RÉGIME JURIDIQUE DES INTERCEPTIONS DE SÉCURITÉ

La France entre l'Europe et les Etats-Unis

PAR

Roseline LETTERON (*)

La loi du 24 juillet 2015 vise tout à la fois à élargir les moyens techniques utilisés par les services de renseignement dans leur activité de surveillance et à donner à leur action un fondement juridique clair (1). Complétée par un second texte du 30 novembre 2015 sur la surveillance des communications internationales (2), elle constitue le cœur d'un ensemble législatif organisant les activités des services de renseignement, plus précisément celles relatives à la surveillance des communications électroniques.

Cette évolution législative française ne saurait être étudiée indépendamment de son environnement international. Elle est souvent expliquée par l'influence des Etats-Unis, qui ont, depuis bien longtemps, voté des lois relatives aux activités des services de renseignement. Dans son rapport préalable à la loi française, le président de la Commission des lois de l'Assemblée nationale affirme ainsi que, dans ce domaine, « *les Etats-Unis font figure d'exemple* » (3).

Il est vrai que la Central Intelligence Agency (CIA) a été créée par le *National Security Act* de 1947. Les interceptions de sécurité réalisées à des fins de renseignement, quant à elles, ont été légalisées dès 1978 par le *Foreign Intelligence Surveillance Act*. Plus récemment, le *Patriot Act*, adopté le 26 octobre 2001, a mis fin à la distinction entre la sécurité extérieure et la sécurité intérieure. Au nom de la lutte contre le terrorisme, tous les services de renseignements des Etats-Unis peuvent désormais accéder aux communications des particuliers et des personnes morales, sans autorisation préalable.

Bon nombre d'Etats européens semblent inspirés par cet exemple et sont en train de se doter de législations autorisant la surveillance de masse. Le 16 octobre 2015, le Bundestag a ainsi voté une loi permettant aux services de renseignements d'accéder aux communications passant par Internet et

(*) Professeur de Droit public à l'Université Paris-Sorbonne (France).

(1) Loi n°2015-912 du 24 juillet 2015 relative au renseignement, *JO*, 26 juil. 2015, p. 12 735.

(2) Loi n°2015-1556 relative aux mesures de surveillance des communications électroniques internationales, *JO*, 1er déc. 2015, p. 22 185.

(3) J.-J. Urvoas, *Rapport sur le projet de loi relatif au renseignement*, Assemblée nationale, Commission des lois, n°2 697, 2 avr. 2015.

de conserver ces données pendant une durée de dix semaines (4). L'Autriche et les Pays-Bas débattent également de textes autorisant la surveillance de toutes les communications circulant sur Internet. La Finlande envisage même de modifier sa Constitution pour alléger les contraintes liées au droit au respect de la vie privée, dans le but de voter un texte de même nature (5). Un mouvement de fond semble ainsi engagé, qui touche la plupart des pays européens, y compris ceux qui se revendiquent traditionnellement comme les plus attachés aux droits de l'homme. Une telle situation provoque de profonds clivages avec une population souvent très attachée à la protection de la vie privée, au point que beaucoup de saisines de la Cour européenne des droits de l'homme dans ce domaine sont le fait de militants associatifs actifs dans le domaine de la protection des données.

Cet « exemple » américain, invoqué lors des débats sur la loi française, ne doit cependant pas être surestimé.

S'il est vrai qu'un fondement légal a été donné à l'activité de certains services de renseignement des Etats-Unis, d'autres sont demeurés secrets. L'existence de la National Security Agency (NSA), qui a succédé en 1952 à l'Armed Forces Security Agency créée en 1949, n'a ainsi été reconnue par les autorités américaines qu'en 1957. Encore cette reconnaissance fut-elle quelque peu contrainte, les journaux américains mentionnant régulièrement la « *No Such Agency* » pour désigner cette institution dépourvue d'existence juridique mais connue des médias.

De la même manière, les interceptions électroniques se sont déployées aux Etats-Unis de manière confidentielle. Le premier réseau dans ce domaine, destiné à l'interception des communications privées et publiques, fut ainsi le système Echelon, fruit du Traité UKUSA conclu en 1946 entre les Etats-Unis et le Royaume-Uni, bientôt rejoints par le Canada, l'Australie et la Nouvelle-Zélande. Or ce traité était secret et il ne fut connu par l'opinion publique que dans le courant des années quatre-vingt-dix. En France, il suscita un rapport parlementaire « *sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale* », présenté par Arthur Paecht en octobre 2000 (6). Le Parlement européen, quant à lui, s'y intéressa en 2001, par un « *rapport sur l'existence d'un système mondial des communications privées et économiques* » (7).

Plus récemment, le système PRISM n'a été connu que par les révélations d'Edward Snowden, reprises par les médias américains en juin 2013. Cet instrument de surveillance mondiale des données circulant sur Internet trouve certes un fondement juridique dans la section 702 du *Foreign Intelligence Surveillance Act* amendé en 2008. Toutefois, nul n'avait

(4) M. Hohmann, « German Bundestag passes new data retention law », *Lawfare*, 16 oct. 2015.

(5) N. Muiznieks, « Europe is spying on you », *New York Times*, 27 oct. 2015.

(6) Assemblée nationale, *Rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale*, n°2 623, 11 oct. 2000.

(7) Parlement européen, *Rapport de la Commission temporaire sur le système d'interception Echelon*, 2001/2098 (INI), 11 juil. 2001.

envisagé l'ampleur des interceptions de masse mises en œuvre par les services américains ni d'ailleurs celle de la coopération des grandes entreprises du Web.

L'exemple américain est surtout marqué par son ambivalence. Il peut être invoqué, comme le font les promoteurs de la loi française, pour justifier la création d'un ensemble législatif offrant aux services de renseignement un cadre juridique connu de tous. Il est aussi, surtout en Europe, invoqué comme un contre-exemple, à l'appui d'une contestation de la surveillance de masse, incarnée dans les révélations d'Edward Snowden. La période récente a vu ainsi l'Union européenne comme le Conseil de l'Europe développer une conception beaucoup plus rigoureuse de la protection des données et de la vie privée que celle qui domine le droit américain. Avec la loi du 24 juillet 2015, le droit français semble renoncer au rôle essentiel qui était le sien dans ce mouvement d'émergence d'un standard européen de protection des données.

Un cadre juridique minimum

L'objet de la loi du 24 juillet 2015 est d'offrir un cadre juridique à l'action des services. Elle repose sur la définition du renseignement comme politique publique, affirmant ainsi le rôle exclusif de l'Exécutif dans la détermination de ses finalités comme de son organisation. En même temps, la loi protège cette domination en définissant un contrôle aussi minimaliste que possible sur l'activité des services de renseignement.

Le renseignement comme politique publique

La loi du 24 juillet 2015 a ajouté un Livre VIII au code de sécurité intérieure créé par une ordonnance du 12 mars 2012 (8). Son article L 811-1 affirme avec netteté que « *la politique publique de renseignement concourt à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la nation. Elle relève de la compétence exclusive de l'Etat* ». Il affirme ensuite que la politique publique du renseignement « *relève de la compétence exclusive de l'Etat* ». Ces formulations ne sont pas seulement déclaratoires. Elles inscrivent la loi de 2015 dans un mouvement général développé depuis 2008, qui interdit l'externalisation du renseignement et resserre son activité autour de l'Exécutif.

Le refus de l'externalisation

Elles révèlent d'abord un refus d'associer les entreprises de sécurité privée à l'activité de renseignement. La précision n'est pas sans importance, alors que la tentation d'externalisation s'est largement répandue dans le domaine de la sécurité privée. Dans la loi du 18 mars 2003, il était précisé que les entreprises exerçant des activités privées

(8) Ordonnance n°2012-351 du 12 mars 2012 relative à la partie législative du Code de la sécurité intérieure, *JO,* 13 mars 2012, p. 4533.

de sécurité sont « *associées aux missions de l'Etat en matière de sécurité publique* » (9). Cette formulation a ensuite été reprise par le Conseil constitutionnel dans sa décision du 9 avril 2015 pour justifier la loi qui soumet l'activité de ces entreprises à un agrément délivré par l'Etat, à la condition toutefois qu'elles soient dirigées par une personne de nationalité française ou d'un Etat membre de l'Union européenne ou de l'Espace économique européen (10). Les entreprises privées de sécurité participent donc au service public de la sécurité.

Le renseignement, quant à lui, demeure un domaine directement rattaché à la souveraineté de l'Etat et cette activité ne saurait donc être externalisée. Considérée sous cet angle, la politique publique du renseignement se trouve ainsi clairement dissociée du service public de la sécurité.

Cette distinction n'est pas pour autant aisée à mettre en œuvre, en particulier en matière d'intelligence économique. Depuis l'ordonnance du 7 janvier 1959, la défense économique est un élément de la défense globale (11). L'actuel Code de la défense reprend sensiblement cette formulation en confiant au ministre de l'Economie « *la protection des intérêts économiques de la nation* » (12). La loi renseignement, quant à elle, autorise le recueil de renseignements « *relatifs aux intérêts fondamentaux de la nation* », parmi lesquels « *les intérêts économiques, industriels et scientifiques majeurs de la France* ». La protection des entreprises françaises, de leur activité de recherche et développement et de leurs contrats internationaux peut donc nécessiter l'utilisation des techniques de renseignement.

Une telle doctrine peut s'analyser comme une réponse apportée à une pratique développée dès l'époque du réseau Echelon. Il est désormais bien connu que des écoutes américaines ont permis, en 1994, de faire échouer un contrat d'achat d'avions entre Airbus et la compagnie aérienne saoudienne, des informations sur les négociations ayant été interceptées et transmises à Boeing et Mc Donell-Douglas. C'est ce dernier qui obtint le marché. La même année, l'interception de communications entre Thomson-CSF et les autorités brésiliennes ont permis à l'entreprise américaine Raytheon d'emporter un marché portant sur un système de surveillance de la forêt amazonienne, la société française ayant été accusée d'avoir versé des commissions à des membres brésiliens du comité de sélection (13). Aux Etats-Unis, les entreprises sont un élément de la puissance américaine et tous les moyens de l'Etat doivent être mis à leur service. Considérée sous cet angle, la loi renseignement se borne à offrir aux entreprises françaises des moyens dont disposaient déjà leurs principaux concurrents.

(9) Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure, *JO*, 19 mars 2003, p. 4761.

(10) Déc. n°2015-463 QPC du 9 avril 2015 ; R. Letteron, « Le contrôle de l'Etat sur les activités privées de sécurité », *Liberté Libertés Chéries*, 9 avr. 2015.

(11) Ordonnance n°59-147 du 7 janvier 1959 portant organisation générale de la défense, *JO*, 10 janv. 1959, p. 691.

(12) Art. L 1142-3 du Code de la défense.

(13) Sur ces questions, *cf.* D. Campbell, *Surveillance électronique planétaire*, Allia, 2001, traduction d'un rapport réalisé pour le Parlement européen, « *Interception Capabilities 2000* ».

Le resserrement du renseignement autour de l'Exécutif

La loi du 24 juillet 2015 est le point d'aboutissement d'une démarche engagée dès le Livre blanc sur la défense et la sécurité nationales de 2008. Ce dernier déclare que « *les activités de renseignement ne disposent pas aujourd'hui de cadre juridique clair et suffisant. Cette lacune doit être comblée* » (14). Une réflexion unique reposant sur un « *continuum défense sécurité* » permet d'englober dans une perspective unique le renseignement intérieur et le renseignement extérieur.

Dans un premier temps, les efforts ont tendu à assurer le contrôle de l'Exécutif sur le renseignement, avec la création d'un Conseil national du renseignement qui, réunissant sous l'autorité du Premier ministre les ministres, les hauts responsables civils et militaires compétents dans ce domaine, est chargé de définir les orientations stratégiques dans ce domaine (15). En même temps, un coordonnateur national du renseignement était créé, défini comme un « *point d'entrée des services de renseignement* » auprès du Président de la République (16).

Les services de renseignement faisaient en même temps l'objet d'un mouvement de centralisation, avec la fusion de la Direction de la surveillance du territoire (DST) et de la Direction centrale des renseignements généraux (RG) au sein d'une nouvelle Direction centrale du renseignement intérieur (DCRI), devenue Direction générale du renseignement intérieur (DGRI) en mai 2014 (17). De la même manière, la loi du 3 août 2009, qui place la Gendarmerie sous l'autorité du ministre de l'Intérieur, s'accompagne d'un redéploiement territorial qui diminue considérablement le nombre de brigades. Le rôle traditionnel des gendarmes dans le renseignement sur le territoire est ainsi largement remis en cause.

Le renseignement qu'on pourrait qualifier de « terrain » ou de « proximité » est donc mis au second plan. Ce choix relève précisément de la politique publique du renseignement, qui met désormais l'accent sur le renseignement électronique (ELINT) au détriment du renseignement humain (HUMINT). On pourrait évidemment discuter d'un tel choix et le rapport parlementaire sur l'affaire Mérah, publié en 2013, s'est montré sévère à son égard. Il estime en effet que « *le principal enseignement* » à tirer de cette affaire « *tient au défaut de surveillance qui pose la question des moyens humains pour le service de sécurité intérieure* » (18). Quoi qu'il en soit, cette préférence pour ELINT n'a pas été remise en cause et la loi

(14) *Livre blanc sur la défense et la sécurité nationale*, Odile Jacob/La Documentation française, Paris, 2008, p. 142.

(15) Art. R. 1 122-6 du Code de la défense.

(16) J. Guisnel, « Lettre de mission adressée à Bernard Bajolet par le Président de la République, le 23 juillet 2008 », *Le Point*, 13 oct. 2008.

(17) Décret n°2 014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la Sécurité intérieure, *JO*, 2 mai 2014.

(18) Rapport de la Commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux, président C. Cavard, rapporteur J.-J. Urvoas. Assemblée nationale, n°1 056, 24 mai 2013.

du 25 juillet 2015 est centrée sur l'utilisation par les services des moyens d'interception, qu'il s'agisse de la réquisition de données techniques chez les opérateurs Internet ou de l'utilisation de l'IMSI Catcher, qui permet d'accéder aux réseaux téléphoniques (19).

En consacrant une politique publique dans ce domaine, la loi impose que des ressources et des moyens, notamment technologiques, soient affectés aux services de renseignement. Le Conseil constitutionnel l'a d'ailleurs rappelé dans sa décision du 23 juillet 2015, en précisant que les crédits de la nouvelle Commission nationale de contrôle des techniques de renseignement (CNCTR) devaient figurer dans la loi de finances. Du point de vue juridique, l'existence d'une politique publique permet de mettre les services à l'abri de poursuites pour des actes liés à leur fonction. C'est ainsi que l'atteinte à la vie privée induite par les techniques d'interception n'est plus fautive dès lors qu'elle relève d'une politique publique mise en œuvre par la voie législative.

Des contrôles aussi modestes que possible

La consécration du renseignement comme politique publique et son resserrement autour de l'Exécutif ne s'accompagnent cependant pas d'un accroissement des contrôles. Au contraire, la loi du 24 juillet 2015 s'efforce de maintenir l'activité de renseignement dans la sphère administrative en limitant l'intervention du juge judiciaire. La justification apportée à cette exclusion est résumée par le Conseil constitutionnel, dans sa décision du 23 juillet 2015 : « *le législateur s'est fondé sur l'article 21 de la Constitution pour confier au Premier ministre le pouvoir d'autoriser la mise en œuvre des techniques de recueil de renseignement dans le cadre de la police administrative* » (20). Ayant pour objet l'ordre public, le renseignement est analysé comme une police administrative. Le recours aux interceptions de sécurité est donc autorisé par le Premier ministre et leur contrôle appartient au Conseil d'Etat.

L'autorisation : une compétence du Premier ministre

La procédure d'autorisation mise en place n'est pas inédite. Elle est directement inspirée par la loi du 10 juillet 1991 sur les écoutes téléphoniques (21). Distinguant clairement les écoutes judiciaires effectuées dans le cadre d'une enquête pénale des écoutes administratives réalisées à des fins de sécurité, le législateur avait alors choisi de soustraire ces

(19) Un IMSI Catcher (*International Mobile Subscriber Identity*) est utilisé pour l'interception du trafic de téléphonie mobile et pour pister les mouvements des terminaux et donc de leurs porteurs. Il fonctionne comme une fausse antenne-relais entre le téléphone mobile espionné et les antennes de l'opérateur téléphonique.

(20) Le Conseil constitutionnel affirme de même que « *le législateur s'est fondé sur l'article 21 de la Constitution* » pour confier au Premier ministre le pouvoir d'autoriser la mise en œuvre des techniques de recueil de renseignement dans le cadre de la police administrative.

(21) Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, *JO*, 13 juil. 1991, p. 9 167 ; C. Guerrier, *Les Ecoutes téléphoniques*, Editions du CNRS, 2000.

dernières à l'autorisation du juge judiciaire, en conférant au Premier ministre la compétence pour les autoriser, après avis d'une autorité administrative indépendante, la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

Cette influence de la loi sur les écoutes téléphoniques sur celle du 24 juillet 2015 n'est pas surprenante. On se souvient notamment que le texte de 1991 fut le premier à mentionner « *la prévention du terrorisme* » parmi les motifs susceptibles de justifier une interception, alors qu'il s'agissait de conférer un fondement juridique à une pratique que la Cour européenne avait sanctionnée précisément parce qu'elle ne s'appuyait alors sur aucun texte législatif (22).

La loi du 24 juillet 2015 reprend ainsi le principe posé en 1991 et confère au Premier ministre la compétence pour autoriser, pour une durée de quatre mois, à la demande des ministres compétents (23), le recours aux moyens d'interception électronique. Cette autorisation est délivrée après l'avis consultatif de la CNCTR, qui remplace désormais l'ancienne CNCIS. La nouvelle structure est composée de neuf membres, dont quatre parlementaires, deux membres du Conseil d'Etat, deux magistrats de la Cour de cassation et une personnalité qualifiée. Les magistrats de l'ordre judiciaire sont donc des membres comme les autres d'une autorité purement administrative. L'avis de la CNCTR ne lie pas la décision du Premier ministre. Elle participe à une procédure consultative ordinaire et le Premier ministre peut suivre son avis ou ne pas le suivre.

Derrière cette procédure apparaît clairement la volonté d'imposer une contrainte aussi légère que possible aux services de renseignement. Elle apparaît clairement dans les procédures d'urgence prévues par le législateur, procédures dont on rappellera qu'elles n'ont rien à voir avec l'état d'urgence mis en œuvre le 14 novembre 2015, mais qu'elles s'appliquent sur le fondement unique de la loi renseignement.

La première, figurant à l'article L 821-5 du Code de la sécurité intérieure, permet au Premier ministre de s'affranchir de toute procédure consultative auprès de la CNCTR « *en cas d'urgence absolue* », formule bien imprécise et qui ne fait l'objet d'aucun contrôle. La CNCTR est seulement informée *a posteriori* de l'autorisation donnée, information accompagnée cependant de quelques éléments de motivation sur éléments justifiant qu'elle ait ainsi été écartée de la procédure.

La seconde procédure d'urgence, voulue par le législateur, a été censurée par le Conseil constitutionnel, dans sa décision du 23 juillet 2015. Il est vrai qu'elle prévoyait d'écarter l'avis de la CNCTR à l'initiative des services de renseignements eux-mêmes. Invoquant une « *urgence opérationnelle* », définie comme « *liée à une menace imminente ou à un risque très élevé de*

(22) CEDH, 24 avril 1990, *Kruslin et Huvig c. France*, *D.* 1990. 353, n. Pradel.

(23) Art. L 821-2, Code de la sécurité intérieure : la demande est formulée par le ministre de la Défense, le ministre de l'Intérieur ou le ministre de l'Economie.

ne pouvoir effectuer l'opération ultérieurement », ils pouvaient alors utiliser, de leur propre chef, les moyens techniques de captation des données, balises ou interceptions des conversations. La CNCTR et le Premier ministre étaient seulement informés de cette utilisation et une procédure d'autorisation devait intervenir dans les quarante-huit heures suivant l'opération. On se trouvait dans une étrange situation, où la loi créait une procédure d'autorisation *a posteriori*. Le Conseil constitutionnel n'a pourtant pas sanctionné l'étrangeté de cette procédure. Il a simplement déclaré qu'elle portait une atteinte excessive au secret des correspondances et au droit au respect de la vie privée (24).

En revanche, le Conseil constitutionnel, dans sa décision du 26 novembre 2015, a admis la conformité à la Constitution de la loi relative à la surveillance des communications électroniques internationales. Ce texte prévoit pourtant que l'autorisation d'intercepter ces communications dont la réception et/ou l'émission est située à l'étranger peut être décidée par le Premier ministre, sans saisine préalable de la CNCTR (25).

Cette tentative d'écarter purement et simplement la procédure consultative dans l'hypothèse d'une urgence appréciée par les services eux-mêmes révèle néanmoins une certaine désinvolture du législateur à l'égard d'une procédure qu'il a pourtant lui-même instituée.

Le contrôle du Conseil d'Etat

Le contrôle des interceptions, quant à lui, incombe au Conseil d'Etat, saisi en premier et dernier ressort selon deux procédures bien distinctes.

L'initiative de la saisine appartient d'abord à la CNCTR, soit par son Président, soit par trois de ses membres, dans l'hypothèse où elle estimerait que son avis n'a pas été suivi d'effet, y compris lorsque le ministre n'en a pas tenu compte. Une telle saisine peut sembler bien peu probable si on considère l'importance des liens entre la Commission et le Conseil d'Etat, la CNCTR étant présidée par Francis Delon, lequel, lui-même membre du Conseil d'Etat, a exercé durant une décennie les fonctions de Secrétaire général de la défense et de la sécurité nationales (SGDSN).

Le droit de recours est également ouvert à « *toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard* » (26). Ce recours peut intervenir directement ou indirectement, au moyen d'une question préjudicielle posée devant les juges du fond.

Pour la première fois, le législateur de 2015 s'efforce de trouver un équilibre entre le droit au recours et les exigences du secret de la défense nationale. Comme les membres de la CNCTR, ceux de la formation

(24) Déc. n°2015-713 DC du 23 juillet 2015, *La Semaine Juridique,* Ed. générale, 14 sept. 2015, n. Verpeaux ; R. Letteron, « Loi renseignement : 'filtrer le moustique et laisser passer le chameau' », *Liberté Libertés Chéries*, 24 juil. 2015.

(25) Déc. n°2015-722 DC du 26 novembre 2015, *JO*, 1er déc. 2015, p. 22187.

(26) Art. L 841-1 du Code de la sécurité intérieure.

spécialisée du Conseil d'Etat compétente pour statuer sur les recours sont habilités au secret-défense. Ils peuvent donc connaître les motifs de la décision de procéder à des interceptions. En revanche, la situation de la personne qui craint d'être l'objet d'interceptions de ses communications est pour le moins difficile. Pour saisir le juge, il est nécessaire qu'elle ait au moins développé quelques soupçons à propos des mesures de surveillance dont elle est l'objet. Toutefois, comment pourrait-elle développer de tels soupçons, alors que les interceptions de sécurité ont nécessairement lieu à son insu ?

Les procédures d'autorisation et de contrôle sont ainsi largement dominées par l'autorité administrative, le juge intervenant étant le juge de l'administration.

La justification donnée à cette situation repose entièrement sur la qualification du renseignement, considérée comme police administrative et relevant en quelque sorte naturellement de la souveraineté de l'Etat. Elle ne présente cependant qu'une apparence de simplicité.

Les débats parlementaires font d'abord apparaître des motivations plus pragmatiques. Au député du parti Les Républicains (LR) Claude Goasguen, qui affirmait que, dans l'hypothèse où un groupe « *s'apprête à se livrer à des violences extrêmement graves* », il « *faut informer le procureur* », le ministre de la Défense, Jean-Yves Le Drian, répond tout simplement : « *On n'a pas le temps !* » (27). L'intervention du juge judiciaire, même extrêmement rapide, est donc perçue comme un frein à l'efficacité du travail des services de renseignement.

Il aurait pourtant été possible de s'appuyer sur l'article 66 de la Constitution pour conférer un fondement constitutionnel à la compétence de l'autorité judiciaire qu'il présente comme « *gardienne de la liberté individuelle* ». Rien n'interdisait, par exemple, de confier à un juge unique habilité au secret-défense la compétence pour l'autorisation des interceptions et à une formation spécifique leur contrôle.

Un tel choix est d'ailleurs celui fait par le droit américain, présenté comme un modèle durant les débats parlementaires. La Foreign Intelligence Surveillance Court (Fisa Court), créée en 1978 et modifiée par le *Patriot Act* de 2001, est compétente pour donner à l'administration, en l'occurrence la National Security Agency (NSA), l'autorisation de procéder à des interceptions de sécurité. Certes, le *Patriot Act* autorise la NSA à demander à la Fisa Court un mandat exigeant des opérateurs la communication de l'intégralité des données téléphoniques de leurs clients, selon une procédure marquée par la plus parfaite opacité (28).

Surtout, le *Freedom Act* du 2 juin 2015 réduit le champ de la surveillance de la NSA, après que des juges américains ont estimé que le *Patriot Act* ne

(27) Assemblée nationale, Première séance du lundi 13 avril 2015, discussion générale.

(28) *Cf.* par exemple G. Breenwald, « Fisa Court oversight: a look inside a secret and empty process », *The Guardian*, 19 juin 2013.

pouvait autoriser l'accès à l'intégralité des données des citoyens américains. L'administration américaine doit désormais formuler des demandes ciblées visant des comptes ou des individus spécifiquement désignés. Elle doit également justifier d'un lien « *raisonnable et détaillé* » avec la menace terroriste (29). La réforme demeure modeste et le fonctionnement de la Fisa Court n'est guère modifié, si ce n'est par la création d'un panel d'experts susceptible d'éclairer la Cour sur les interceptions électroniques et le choix d'imposer le caractère public de certaines de ses décisions.

En dépit de toutes ces imperfections, la procédure américaine relève néanmoins du pouvoir judiciaire. L'apparence de la séparation des pouvoirs est donc sauvegardée. Les juges américains du droit commun ont d'ailleurs livré un combat contre le *Patriot Act* qui est largement à l'origine de l'inflexion actuelle du système juridique.

Un frein a l'emergence d'un standard européen de protection

Ce choix américain d'une procédure juridictionnelle, aussi peu satisfaisante soit-elle, montre que l'« exemple » des Etats-Unis est invoqué, à propos de la loi française, de manière plus ou moins incantatoire. Les débats parlementaires témoignent d'ailleurs d'un certain désintérêt à l'égard de l'analyse comparée, qui ne figure, d'ailleurs modestement, que dans l'étude d'impact où sont résumés les systèmes britannique, italien et belge, sans que le lecteur soit informé des raisons qui justifient ce choix (30). Ce désintérêt est peut-être lié à la mise en œuvre par l'Exécutif de la procédure législative accélérée prévue par l'article 45 de la Constitution. La loi renseignement a ainsi fait l'objet d'un vote unique dans chaque assemblée, avant l'adoption définitive par une Commission mixte paritaire.

Derrière cette relative pauvreté des débats apparaît une autre forme d'influence américaine, beaucoup plus souterraine que celle qui peut apparaître en matière de procédure d'autorisation ou de contrôle des interceptions. Elle repose sur l'idée, désormais acquise, d'une inversion des relations entre l'individu et l'Etat. Sur ce point, la loi renseignement du 24 juillet 2015 marque un frein à l'émergence d'un droit européen de la protection des données personnelles.

L'inversion des rapports entre l'individu et l'Etat

Le droit public est marqué, depuis une trentaine d'années, par l'émergence de la notion de transparence, appliquée aux activités de l'Etat. Le mouvement a commencé aux Etats-Unis avec le *Freedom of Information*

(29) E. Nakashima, « With deadline near, lawmakers introduce bill to end NSA program », *The Washington Post*, 29 avril 2015.

(30) Projet de loi relatif au renseignement, Etude d'impact, Assemblée nationale, 18 mars 2015.

Act (FOIA) du 4 juillet 1966 conférant aux citoyens le droit d'accéder aux documents administratifs détenus par l'administration fédérale. Ensuite, le *Privacy Act* de 1974 leur permit d'avoir communication des informations nominatives les concernant conservées dans les fichiers fédéraux. Enfin, le *Government in the Sunshine Act* développa la transparence dans le fonctionnement des agences fédérales américaines. Tout ce mouvement reposait sur l'idée que les services de l'Etat devaient être aussi transparents que possible et qu'en même temps la vie privée des citoyens devait être protégée autant que possible.

Ce mouvement n'a pas disparu aujourd'hui. Le jour même de son entrée en fonctions, le président Obama a signé une circulaire sur le *Freedom of Information Act* déclarant close l'ère du gouvernement Bush marquée par le secret et imposant aux services fédéraux d'appliquer une présomption favorable à la communication du document demandé (31).

Le droit français a connu un mouvement semblable, à peine plus tardif. La loi du 6 janvier 1978 autorisa l'accès aux informations nominatives conservées dans des fichiers, considérant, pour la première fois, la protection des données comme un élément de la vie privée des personnes. Ensuite, la loi du 17 juillet 1978 autorisa l'accès aux documents administratifs et la loi du 11 juillet 1979 la motivation des actes administratifs défavorables (32).

Cet ensemble législatif, qualifié à l'époque de « Troisième génération des droits de l'homme » n'a pas disparu aujourd'hui. Il s'est même théoriquement renforcé avec le projet de loi pour une République numérique porté par Axelle Lemaire. Ce dernier envisage la création d'un « service public des données publiques » permettant d'obtenir la communication de tous les documents d'intérêt général, ce qu'il est convenu d'appeler la « littérature grise » de l'administration. De même, la fusion de la Commission nationale de l'informatique et des libertés et de la Commission d'accès aux documents administratifs dans une seule autorité administrative indépendante permettrait aux citoyens de disposer d'un guichet unique pour demander l'accès aux données nominatives les concernant, qu'elles soient ou non conservées dans un fichier informatique (33).

La loi du 24 juillet 2015 témoigne d'un dessein radicalement différent. L'objet n'est plus d'assurer la transparence de l'Etat et le secret de la vie privée des individus. Il est, au contraire, de protéger les secrets de l'Etat et de permettre la transparence de la vie privée des individus. A cet égard, la loi française semble effectivement inspirée par une législation américaine qui repose précisément sur ce principe.

(31) E. Zoller, « Le principe de transparence et les nouvelles technologies de l'information aux Etats-Unis », communication à la Conférence-débat du CDPC sur la transparence administrative et ses déclinaisons technologiques récentes, 15 avr. 2013.

(32) R. Letteron, « La transparence administrative », *Problèmes politiques et sociaux*, n°679, 1992.

(33) Projet de loi pour une République numérique, disponible sur le site Internet www.republique-numerique.fr/pages/projet-de-loi-pour-une-republique-numerique ; R. Letteron, « 'La fusion entre la CNIL et la CADA à l'ordre du jour », *Liberté Libertés Chéries*, 8 nov. 2015.

La protection des secrets de l'Etat apparaît clairement au regard de la procédure mise en œuvre devant le Conseil d'Etat. Certes, les membres de la formation spécialisée chargée de connaître de la régularité de la mise en œuvre des techniques de renseignement sont habilités au secret-défense. En soi, c'est évidemment un élément favorable à l'efficacité de son contrôle, en rupture avec le principe traditionnel d'opposabilité du secret-défense au juge.

Il n'en demeure pas moins que la procédure demeure marquée par son caractère dérogatoire. C'est ainsi que l'instruction est non contradictoire et couverte par le secret de la défense nationale. L'audience n'est pas davantage contradictoire. Elle est, en quelque sorte, dédoublée, avec une audience séparée pour le requérant et une autre audience pour les services, cette dernière se tenant à huis clos. Enfin, la décision de justice rendue est limitée à son dispositif, ce qui signifie que le requérant n'a aucune connaissance du raisonnement juridique développé par le Conseil d'Etat.

Dans certains cas, notamment lorsqu'il est saisi d'un recours motivé par sa crainte d'être l'objet d'interceptions de sécurité, le Conseil d'Etat peut se borner à affirmer que les vérifications imposées par la loi ont été effectuées. Il déclare alors, soit qu'aucune illégalité n'a été commise, soit, au contraire, qu'une illégalité a été commise. Dans les deux cas, le requérant n'en saura pas davantage, même si, dans la seconde hypothèse, il pourra se voir octroyer une indemnité pour réparer le préjudice subi.

La quasi-absence de contrôle parlementaire sur le renseignement complète ce dispositif de protection des secrets de l'Etat. La Délégation parlementaire au renseignement, commune au Sénat et à l'Assemblée nationale, a été créée par la loi du 9 octobre 2007 (34). Son contrôle sur le renseignement demeure cependant embryonnaire. Certes, il s'agit d'une institution permanente, mais elle ne dispose pas des compétences qui sont celles d'une commission d'enquête, contrairement aux dispositifs mis en place par l'Assemblée nationale et le Sénat pour assurer le suivi de l'état d'urgence (35).

Au contraire, le législateur a fixé avec précision l'étendue de son contrôle, le limitant à l'évaluation générale de la politique publique du renseignement. C'est ainsi qu'elle n'est destinataire que de documents d'ordre général relatifs à la stratégie nationale du renseignement, d'« *éléments d'information issus du plan national d'orientation du renseignement* » ou d'« *éléments d'appréciation relatifs à l'activité générale* [...] *des services de renseignement* », sans oublier un « *rapport annuel de synthèse des crédits consacrés au renseignement* ». Il est même précisé par la loi du 9 octobre 2007 que les informations délivrées à la Délégation « *ne peuvent porter ni sur les opérations en cours, ni sur les instructions données*

(34) Loi n° 2 007-1442 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement, *JO*, 10 oct. 2007, p. 16 558.

(35) R. Letteron, « Les habits neufs du contrôle parlementaire », *Liberté Libertés Chéries*, 10 déc. 2015.

par les pouvoirs publics [...], *ni sur les échanges avec les services étrangers* ». Dans ces conditions, il n'est pas surprenant que le législateur ait accordé aux membres de la Délégation le droit d'avoir accès à des informations classifiées, dès lors que les documents transmis leur interdisent d'avoir une connaissance précise de la réalité du fonctionnement des services de renseignement. La mise en œuvre de la loi du 24 juillet 2015 sur le recours aux techniques d'interception des communications ne saurait donc faire l'objet d'un contrôle parlementaire efficace.

Ces interceptions permettent aux services de renseignement d'accéder à l'intégralité des communications d'une personne, y compris celles qui relèvent de sa vie privée. La loi du 24 juillet 2015 autorise ainsi l'utilisation des techniques les plus sophistiquées d'interception : sonorisation des lieux et des véhicules, captation d'images, collecte des communications électroniques, boîtes noires algorithmiques placées auprès des fournisseurs d'accès pour déceler des comportements suspects en croisant les données, IMSI Catchers permettant d'intercepter les conversations téléphoniques dans une zone située à proximité d'une cible.

Les débats qui ont précédé la loi se sont largement centrés sur ces aspects techniques et ses détracteurs ont dénoncé la mise en œuvre d'un système de surveillance de masse. Il est vrai que la loi impose, de fait, la transparence de la vie privée de tout individu, vie privée désormais accessible aux services de renseignement. Le principe du consentement de la personne à la collecte et à la conservation de telles données est en effet totalement écarté.

Il n'en demeure pas moins que la loi met en place un système de collecte de masse et non pas de surveillance de masse. Le but n'est pas de conserver toutes les données accessibles pour une utilisation purement hypothétique. Il est de déceler, dans un flux permanent de données, celles qui sont pertinentes pour identifier les personnes représentant un danger pour l'ordre et la sécurité publics. Il est à la fois impossible et inutile de surveiller toute une population. Les services de renseignement veulent opérer une sélection par la mise en œuvre d'un filtrage électronique des données. L'ensemble de cette politique repose ainsi sur la fiabilité des algorithmes, ceux-là mêmes qui sont chargés de déceler les comportements suspects sur Internet.

Menaces sur le droit européen de la protection des données

Le droit européen, quant à lui, s'appuie sur la notion de protection des données personnelles, considérée comme un élément du droit au respect de la vie privée. Ce principe, acquis dès la Convention du 28 janvier 1981 sur la protection des données initiée par le Conseil de l'Europe, a été repris par l'Union européenne dans l'article 8 de la Charte européenne des droits fondamentaux. Elle affirme : « *Toute personne a droit à la protection des données à caractère personnel la concernant* ». De manière plus effective, la directive du 24 octobre 1995 énonce que « *les Etats membres assurent,*

conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel » (36). Le projet de règlement, adopté par un accord du 15 décembre 2015 intervenu entre le Parlement européen, la Commission et le Conseil, mentionne, une nouvelle fois, le droit des personnes physiques « à la protection des données à caractère personnel » (37).

L'article 1er de la loi du 24 juillet 2015 affirme certes, de manière un peu emphatique, que « *le respect de la vie privée, dans toutes ses composantes, notamment* [...] *la protection des données personnelles* [...], *est garanti par la loi* ». Cependant, cette affirmation s'accompagne immédiatement de la liste des conditions offertes aux services de renseignement pour porter atteinte à ce principe par l'interception des communications privées. Certaines d'entre elles sont liées à la compétence des services de renseignement et à l'existence d'une procédure d'autorisation. Les conditions de fond sont néanmoins les plus importantes, car elles témoignent d'une volonté de faire prévaloir la « *stratégie de sécurité nationale* » sur le droit à la protection des données.

D'une part, les interceptions doivent être justifiées par les menaces liées « *aux intérêts fondamentaux de la nation* » (38). Parmi ceux-ci figure le terrorisme, qui a permis d'offrir aux promoteurs de la loi un élément de langage précieux pour convaincre les parlementaires et l'opinion publique de la nécessité du texte. Comme d'autres lois avant elles, la loi renseignement a ainsi bénéficié de l'effet d'aubaine du terrorisme, invoqué dans ce cas pour justifier un texte qui englobe l'ensemble de l'activité des services et ne se limite pas à la lutte contre le terrorisme. D'autre part, le texte impose le respect du principe de proportionnalité entre les motifs invoqués pour justifier une interception et le respect de la vie privée des personnes qui en sont l'objet. L'appréciation de cette proportionnalité relève cependant largement du pouvoir discrétionnaire des services de renseignement et du Premier ministre, dans le cadre de la procédure d'autorisation prévue par la loi.

La vie privée, en tant que telle, n'est plus considérée comme susceptible d'une protection spécifique et on voit alors se développer un discours qui affirme que celui qui n'a rien à cacher ne doit pas s'inquiéter des intrusions dans sa vie privée. La notion même de secret de la vie privée devient suspecte.

Cette démarche qui consiste à écarter la protection de la vie privée en faisant prévaloir la sécurité n'est pas, à proprement parler, contraire

(36) Directive 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JO*, L 281, 23 nov. 1995, p. 31.

(37) Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(38) Art. L 811-3 du Code de la sécurité intérieure.

au droit européen, qu'il trouve son origine dans la jurisprudence de la Cour européenne des droits de l'homme ou dans des normes de l'Union européenne. Les conditions de sa mise en œuvre sont cependant soumises à des conditions rigoureuses dont le respect n'est pas toujours clairement assuré par la loi du 24 juillet 2015.

Depuis l'arrêt *Klass et autres c. Allemagne* du 6 septembre 1978, la Cour européenne des droits de l'homme considère que la surveillance des communications, à l'époque téléphoniques, à l'insu de l'intéressé peut constituer une « *ingérence nécessaire dans une société démocratique* » (39). Des motifs de sécurité publique peuvent, aux yeux de la Cour, justifier une telle surveillance. Encore faut-il cependant que ces interceptions soient prévues par la loi. Concernant cette fois le droit français, cette exigence a été reprise dans les arrêts *Kruslin et Huvig c. France* du 24 avril 1990, suscitant le vote de la loi de 1991 sur les écoutes téléphoniques (40). C'est précisément pour répondre à cette exigence d'un fondement législatif que la loi du 24 juillet 2015 a été votée.

L'éventuelle censure de son dispositif par la Cour européenne n'est néanmoins pas tout à fait exclu. L'arrêt *Roman Zakharov c. Russie*, rendu le 4 décembre 2015 montre que la jurisprudence récente de la Cour impose de nouvelles exigences en matière d'interceptions de sécurité (41), exigences que la loi française ne semble pas avoir totalement prises en considération. En l'espèce, le rédacteur en chef d'une maison d'édition se plaignait devant la Cour du fait que les opérateurs de réseaux mobiles en Russie étaient tenus, en vertu d'une loi, d'installer des dispositifs électroniques permettant aux services de police et de renseignement de procéder à des interceptions, situation absolument identique à ce qu'autorise désormais le droit français. Or la Cour européenne sanctionne le droit russe, non pas pour l'existence de ces interceptions, mais pour les défaillances de leur encadrement juridique. Elle observe ainsi que les motifs de ces interceptions ne sont pas clairement définis par la loi, pas plus que les conditions de leur levée. Elle dénonce en même temps les insuffisances des procédures d'autorisation et de contrôle, insistant sur les difficultés de preuve auxquelles se heurte l'éventuelle victime, en l'absence évidente de possibilité d'accès aux informations pertinentes sur la mesure dont elle est l'objet.

La loi de 2015 n'est évidemment pas à l'abri d'une éventuelle censure au nom de l'article 8, qui protège la vie privée des personnes. La jurisprudence de la Cour européenne va d'ailleurs probablement se préciser sur ce point car différentes requêtes ont été déposées au Royaume-Uni par

(39) CEDH, *Klass et autres c. Allemagne*, req. n° 5 029/71, 6 sept. 1968.
(40) CEDH, *Kruslin et Huvig c. France*, *D.* 1990. 353, n. Pradel, 24 avr. 1990.
(41) CEDH, GC, *Roman Zakharov c. Russie*, req. n° 47 143/06, 4 déc. 2015.

des personnes ou des organisations auxquelles les révélations d'Edward Snowden ont appris qu'elles faisaient l'objet de mesure de surveillance (42).

Au regard du droit de l'Union, la loi du 24 juillet 2015 semble moins directement menacée. Depuis la directive du 24 octobre 1995, le droit de l'Union en matière de collecte et de conservations de données personnelles à des fins de sécurité publique repose sur les principes de nécessité, de proportionnalité et de légalité (43). De même, la mise en œuvre de ces traitements doit être précédée d'une procédure d'autorisation faisant intervenir une autorité indépendante et doit offrir aux personnes un véritable droit à un recours juridictionnel. Le projet de directive intégré au « Paquet protection des données » reprend exactement ces principes sans imposer aucune exigence nouvelle au regard des garanties aux personnes faisant l'objet d'interceptions et de fichages. Il laisse, au contraire, aux Etats membres une très large autonomie dans la définition du droit applicable, son objet étant de favoriser l'échange de renseignement au sein de l'Union.

La loi du 24 juillet 2015 est donc parfaitement conforme au droit de l'Union européenne lorsqu'elle affirme que les autorités ne peuvent porter atteinte à la protection des données « *que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité* » (44).

Si le texte français ne porte pas atteinte au droit de l'Union européenne, il va néanmoins à l'encontre d'un système juridique européen qui vise à développer un standard de protection très élevé au regard de la protection des données personnelles. Des progrès considérables ont été enregistrés dans ce domaine et l'Union européenne a pu imposer aux entreprises américaines de l'Internet le respect des principes fondamentaux de la protection des données. C'est ainsi que la Cour de justice de l'Union européenne, dans sa décision *Google Spain NL* du 13 mai 2014 (45), a consacré le droit à l'oubli, qui, à l'égard d'un moteur de recherches, se traduit par un droit au déréférencement.

En matière de données personnelles collectées et stockées pour des motifs de sécurité publique, la Cour de justice se montre également soucieuse du respect de protection des données personnelles. Sa décision du 6 octobre 2015 le montre clairement. En l'espèce, était contesté le transfert de données personnelles de Facebook Irlande à Facebook Etats-Unis, les révélations d'Edward Snowden ayant montré que ces données conservées sur des serveurs américains sont accessibles aux services de

(42) Requêtes pendantes : *Big Brother Watch et autres c. Royaume-Uni*, req. n°58 170/13 ; *Bureau of Investigation Journalism et Alice Ross c. Royaume-Uni*, req. n°62 322/14.

(43) Directive 95/46 du 24 octobre 1995 sur la protection des données à caractère personnel, *JO*, L 281, 23 nov. 1995.

(44) Art. L 801-1 Code de la sécurité intérieure.

(45) CJUE, *Google Spain SL, Google Inc. c. Agencia española de proteccion de datos (AEPD),* Mario Costeja Gonzalez, Aff. C-131/12, 13 mai 2014.

renseignements américains, la NSA en particulier. Ces transferts de données vers un pays tiers ne sont possibles, au regard de la directive du 24 octobre 1995, que si cet Etat « *acquiert un niveau de protection adéquat* », c'est-à-dire sensiblement identique à celui garanti dans l'Union européenne, cette équivalence étant concrétisée par un accord dit de « Safe Harbor ». Dans sa décision du 8 octobre 2015, la Cour de justice de l'Union écarte l'accord de Safe Harbor conclu en l'an 2000 entre l'Union et les Etats-Unis, estimant fort simplement que le niveau de protection des données est bien inférieur aux Etats-Unis que sur le territoire de l'Union (46).

La loi française du 24 juillet 215 repose ainsi sur une conception traditionnelle du renseignement, instrument de la puissance souveraine de l'Etat. La protection des données personnelles, notion qui constitue pourtant le socle du droit européen, passe au second plan, comme en témoigne la faiblesse des recours offerts à la personne qui se pense victime d'interceptions de sécurité. Sur ce plan, le texte français témoigne, à l'évidence, d'un rapprochement avec la définition américaine des données personnelles. Elles ne sont pas la propriété de la personne qui doit donner son consentement à leur utilisation. Elles sont un bien susceptible d'appropriation, soit par des entreprises privées, soit par des Etats.

(46) CJUE, *M. Schrems c. Data Protection Commissioner*, Aff. C-362/14, 6 oct. 2015.