Les enjeux du nouveau cadre juridique du renseignement

Bertrand Warusfel

(version de travail d'une communication au 3ème colloque annuel de l'AFDSD, 24 septembre 2015)
Article publié in Matthieu Conan & Béatrice Thomas-Tual (dir.),
Annuaire 2016 du droit de la sécurité et de la défense, Ed. Mare & Martin, 2016, pp. 405-423.

LES ENJEUX DU NOUVEAU CADRE JURIDIQUE DU RENSEIGNEMENT

Bertrand WARUSFEL

Professeur à l'Université de Lille
(Centre de recherches Droits et perspectives du droit – ERDP),
avocat au barreau de Paris

La loi du 24 juillet 2015 relative au renseignement ouvre une page nouvelle dans le droit français de la sécurité nationale [1]. Pour la première fois, en effet, dans notre droit une loi définit et encadre les missions des services spécialisés de renseignement de l'État tout en mettant en place un dispositif de contrôle administratif et juridictionnel dont le rôle – clairement rappelé par le Conseil constitutionnel dans sa décision relative à ce texte [2] – est de veiller à la proportionnalité des atteintes au respect de la vie privée qui pourront être autorisées afin de remplir les objectifs de sécurité nationale dont ces services ont la charge. Cette « légalisation du renseignement » est donc le fruit d'une révolution juridique qui vient conclure une séquence politique de près de vingt-cinq ans (depuis l'adoption de la loi du 10 juillet 1991 [3]) pendant laquelle – comme dans d'autres domaines de défense et de sécurité – l'État régalien a progressivement apprivoisé la légitimité du droit et la nécessité d'équilibrer ses prérogatives exorbitantes par un contrôle indépendant et démocratique [4].

Témoin de cette évolution, le nouvel article L. 801-1 du code de la sécurité intérieure (CSI) reprend en l'élargissant l'affirmation pionnière de l'article 1er de la loi du 10 juillet 1991 et pose en principe premier du nouveau cadre juridique du renseignement en France que « le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti par la loi » et que « l'autorité publique ne peut y porter atteinte 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 ».

Appliquer la loi de telle sorte que cette primauté de la liberté fondamentale ne soit pas vidée de son sens par des pratiques de renseignement trop invasives et insuffisamment proportionnées aux menaces à prévenir, voici donc l'un des principaux enjeux de la mise en œuvre de la nouvelle loi, notamment à l'occasion de l'inévitable (et par certains côtés nécessaire) « judiciarisation » du travail de renseignement. Mais le nouveau cadre juridique doit aussi démontrer son efficacité.

---

[1] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, J.O.R.F. du 26 juillet 2015. Pour de premiers commentaires : Xavier Latour, « La loi relative au renseignement : un État de surveillance ? », *La Semaine Juridique Administrations et Collectivités territoriales* n° 40, 5 octobre 2015, 2286 ; Christine Lazerges & Hervé Henrion-Stoffel, « Politique criminelle, renseignement et droits de l'homme - À propos de la loi du 24 juillet 2015 relative au renseignement », *Revue de sciences criminelles*, 2015, p. 761.

[2] Conseil constitutionnel, n° 2015-713 DC du 23 juillet 2015.

[3] Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, ultérieurement codifiée au livre II du Code de la sécurité intérieure, et dont les dispositions relatives aux « interceptions de sécurité » ont constitué la première brique d'une législation sur le renseignement.

[4] Voir notamment notre article : Bertrand Warusfel, « La légalisation du renseignement en France (1991-2015) » in Sébastien Laurent & Bertrand Warusfel, *Transformations et réformes de la sécurité et du renseignement en Europe*, Presses Universitaires de Bordeaux, 2015, pp. 133-153.

1/ Un enjeu de management public : assurer une bonne efficacité au nouveau système

Dans une période où la communauté du renseignement doit se mobiliser à son plus haut niveau de performance pour faire face aux menaces terroristes accrues auxquelles doit faire face notre pays, la loi du 24 juillet 2015 ne doit pas être vécue comme une contrainte supplémentaire mais plutôt comme la condition qu'il fallait remplir pour pouvoir doter les services spécialisés de nouveaux moyens de recueil de l'information sans pour autant prendre des risques d'illégalité ni même de dé-légitimation [5]. Cela passe d'abord par le développement d'une réelle culture juridique au sein des services et de leurs instances de coordination, mais aussi par le travail de doctrine et de « jurisprudence » qu'effectuera la nouvelle commission nationale de contrôle des techniques de renseignement (CNCTR) ainsi que par des progrès dans la relation renouvelée qui va s'instaurer entre le renseignement et la justice.

1a) Développer une culture juridique propre à la communauté du renseignement

Il serait incorrect de penser que les services de renseignement vivaient avant la loi de juillet 2015 totalement à l'écart du droit. Leurs activités s'inscrivaient en effet dans un cadre réglementaire bien défini et certaines pratiques (comme le recours aux interceptions de sécurité, les demandes de déclassification ou encore les échanges des spécialistes de l'antiterrorisme avec les magistrats spécialisés) pouvaient les amener à côtoyer les autorités administratives indépendantes (notamment CNCIS et CCSDN, ainsi que la CNIL en matière d'accès aux fichiers) voire l'autorité judiciaire. Mais cela restait marginal et n'impliquait qu'un nombre restreint de personnes plus particulièrement dédiées à ces tâches.

Avec la loi du 24 juillet 2015, c'est une part nettement plus significative des activités et des effectifs de ces services qui va devoir mettre en œuvre les procédures d'autorisation ou de contrôle prévues par ce texte. Il importe donc que son sens et ses modalités soient mieux connus des opérationnels et que des personnels ayant une compétence juridique appropriée soient recrutés ou nommés pour ce faire.

Au-delà des questions de gestion des ressources humaines propres à chaque service, il est certain que la responsabilité la plus importante en la matière pèse désormais sur l'académie du renseignement, créée en 2010 pour concourir « à la formation du personnel des services de renseignement » ainsi qu'à la « la diffusion de la culture du renseignement » [6].

Les questions juridiques qui étaient déjà au programme de certaines de ses sessions de formation continue devraient mobiliser encore plus largement ses efforts pour qu'elle puisse former assez rapidement de nombreux cadres des six services spécialisés [7], voire de certains services tiers qui vont être également autorisés en application de l'article L. 811-4 CSI à user de techniques de renseignement encadrées par la loi. La matière lui en sera notamment

[5] De l'affaire Dreyfus à celle du Rainbow Warrior, en passant par l'assassinat de Ben Barka, l'histoire française est coutumière de ces scandales de renseignement qui ont fortement contribué à alimenter une méfiance instinctive de l'opinion et des responsables politiques à l'encontre des pratiques des services de renseignement et de sécurité.

[6] Décret n° 2010-800 du 13 juillet 2010 portant création de l'académie du renseignement (article 2).

[7] Ceux visés dans le décret n° 2015-1185 du 28 septembre 2015 (qui a créé l'article R. 811-1 CSI qui désigne – sans surprise – les services suivants : DGSE, DGSI, DRM, DPSD, DNRED, Tracfin).

fournie par plusieurs dizaines de circulaires et d'instructions ministérielles qui sont prévues pour fixer les conditions d'application par chaque service du nouveau Livre 8 du code de la sécurité intérieure.

Mais au-delà de cette formation procédurale et administrative, on peut penser que l'Académie sera un lieu privilégié pour que l'expertise juridique disponible autour des questions de renseignement et de sécurité nationale puisse enrichir la pratique des opérationnels tout en s'enrichissant des échanges de point de vues dans le respect de la nécessaire confidentialité qui sied au domaine [8].

1b) Définition d'une doctrine d'emploi des techniques de recueil de renseignement

A côté de la culture juridique du renseignement qu'il appartient à l'Académie de développer, un rôle essentiel et très complémentaire revient à la nouvelle commission de contrôle, la CNCTR.

C'est elle en effet qui a, dès maintenant, la lourde tâche de concevoir et de roder les procédures d'autorisation et de contrôle en application du nouveau Livre 8 du code de la sécurité intérieure. Il va en résulter nécessairement une pratique, issue des avis que la CNCTR va rendre et des décisions de Matignon qui s'en suivront. On sait que l'un des avantages des autorités administratives indépendantes est, justement, de faciliter l'émergence de bonnes pratiques par la concertation en amont avec les acteurs du secteur et par des avis donnés en aval sur des cas concrets.

En matière de renseignement, les exigences opérationnelles imposent notamment que les fonctionnaires des services engagés dans la recherche d'informations ou la surveillance d'individus puissent connaître à l'avance les critères principaux sur la base desquels la CNCTR et le Premier ministre pourraient considérer favorablement leurs demandes d'autorisation. Dans cette matière, le souci de sécurité juridique et de prévisibilité des décisions rejoint clairement celui de l'efficacité. En fonction des différents domaines d'activité, chaque service devrait donc disposer assez rapidement d'une grille d'analyse lui permettant d'éviter les demandes manifestement peu susceptibles d'être satisfaites et de motiver suffisamment et correctement celles qui correspondraient avec les critères principaux posés par la pratique de la CNCTR.

De ce point de vue, le précédent de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) doit être considéré avec intérêt. Malgré les contraintes sécuritaires importantes qui restreignaient sa capacité à communiquer ouvertement sur le traitement au cas par cas des demandes d'interception, la CNCIS a réussi à produire chaque année des rapports nourris comportant des statistiques assez détaillées sur le volume de dossiers traités et leur ventilation en fonction des motifs et des services concernés. Mais on trouve aussi le résumé actualisé des pratiques de la Commission en relation avec les services du Premier ministre.

[8] Cette ouverture à l'expertise extérieure – notamment académique – devrait s'inscrire dans le sens de ce que notre collègue Sébastien Laurent appelait récemment de ses vœux dans une tribune : « Le renseignement et l'université ne doivent plus s'ignorer », *Libération*, 9 novembre 2015, p. 23.

De ce corpus, enrichi périodiquement par des commentaires extérieurs, des documents étrangers et de riches annexes, a émergé au fil des années une véritable doctrine du contrôle qui a d'ailleurs contribué à enrichir la future loi de 2015. Le passage de l'avis a posteriori à l'avis préalable ou la procédure d'urgence sont notamment issus de simples pratiques de la CNCIS qui avaient fini d'acquérir le statut d'une coutume et qui ont ainsi été repris dans la nouvelle loi.

2/ Un enjeu procédural : encadrer la judiciarisation des pratiques de renseignement

Comme nous l'écrivions « la sécurité nationale en France a toujours vécu à l'écart de la justice » [9], mais ce temps est sans doute révolu, non seulement en raison des progrès de l'État de droit, de la juridicisation corrélative de notre société libérale ouverte mais aussi du fait que la lutte contre la menace majeure actuelle du terrorisme implique une articulation accrue entre renseignement et judiciaire. L'ancien juge antiterroriste Marc Trividic affirmait déjà qu'il faut « judiciariser plus tôt » en cette matière, car « seul le judiciaire permet d'interpeller » [10].

Mais jusqu'alors, la judiciarisation du renseignement était à la fois assez unilatérale et généralement infructueuse. En effet, à défaut pour les services de renseignement de pouvoir communiquer officiellement leurs informations sur la base de pratiques autorisées par la loi, c'était plus souvent la justice qui cherchait à s'intéresser aux pratiques occultes de renseignement que le renseignement qui contribuait légitimement à la recherche de la vérité judiciaire. Et comme l'obstacle du secret de défense s'opposait le plus souvent à ce que les procédures judiciaires puissent aboutir, le bilan de la confrontation entre magistrats et services de renseignement était assez négatif : beaucoup de méfiance ou d'hostilité de part et d'autre pour peu de résultats judiciaires concrets (sauf dans quelques domaines particuliers de l'antiterrorisme).

Là aussi, la loi du 24 juillet 2015 pourrait constituer une étape significative. Non qu'elle recèle en elle-même beaucoup de dispositions concernant cette judiciarisation, mais parce qu'elle créé un mouvement de rapprochement entre le droit et les pratiques clandestines de sécurité nationale qui devrait faciliter, dans un second temps, une rencontre plus équilibrée entre juridictions et services de renseignement, au profit de la manifestation de la vérité et de la juste répression des atteintes aux intérêts de la Nation. La loi a déjà commencé à la prévoir vis-à-vis de la justice administrative. On peut penser que l'articulation avec la justice judiciaire, et particulièrement pénale, devrait suivre.

2a) La mise en place du nouveau contentieux spécialisé devant le Conseil d'État

L'émergence d'une doctrine de la CNCTR sera complétée et confortée par l'établissement progressif d'une véritable jurisprudence résultant des décisions rendues par la formation spéciale du Conseil d'État désormais compétente pour apprécier la légalité du recours aux techniques de renseignement visées par la loi. Cette compétence juridictionnelle spéciale est en soi une révolution supplémentaire, puisque – pour la première fois – une juridiction aura accès à l'ensemble des documents et informations classifiés sans que leur classification puisse lui être opposée.

[9] Bertrand Warusfel, « Justice et sécurité nationale : l'apport de la loi sur le renseignement », Cahiers de la sécurité et de la justice, n° 31, juillet 2015, p. 69.
[10] Interview in Le Télégramme (www.letelegramme.fr), 27 juin 2015.

Cela implique donc que se développe, au fil des premiers contentieux dont les juges du Palais Royal seront saisis, une pratique particulière de la procédure administrative contentieuse entre le juge administratif, la CNCTR (qui sera toujours saisie et participera à l'instance, en y apportant le fruit de ses contrôles), les services concernés, le cabinet du Premier ministre et - le plus souvent – le ou les requérants individuels.

Au cœur de cette nouvelle procédure, il y aura l'application du principe, très sensible, posé par le nouvel article L. 773-3 du code de justice administrative [11] selon lequel « les exigences de la contradiction mentionnées à l'article L. 5 du présent code sont adaptées à celles du secret de la défense nationale ». Cette « adaptation » qui doit permettre de réaliser un équilibre entre deux impératifs constitutionnels (comme l'a rappelé le Conseil constitutionnel [12]) va nécessiter de trouver des compromis procéduraux délicats afin d'éviter les deux écueils qui seraient soit la violation manifeste des droits de la défense (si une partie n'avait aucun moyen de discuter les éléments essentiels du litige) soit la compromission dommageable d'informations classifiées pouvant mettre en danger les sources ou les méthodes des services de renseignement. Or, on sait déjà que la voie est étroite, si l'on en croit notamment la manière vigilante avec laquelle le Conseil constitutionnel a censuré partiellement les dispositions de la loi sur la géolocalisation [13].

Pour l'instant, les dispositions du décret du 1er octobre sur le contentieux du renseignement, pris en application de la loi de juillet dernier, n'apporte que peu de réponses aux légitimes interrogations que ne va pas manquer de susciter le sujet [14]. On y apprend, sans surprise, que les mémoires et pièces transmises au juge ne seront communiquées au requérant que dans une version expurgée de toutes indications classifiées [15] ou encore que le requérant devra, une fois présenté ses observations se retirer avant les conclusions du rapporteur public [16]. Mais l'on s'étonnera que même que, au-delà du contenu précis de ces conclusions, le « sens » même des conclusions du rapporteur public ne pourra pas être connu des parties avant l'audience [17]. Tout au plus, est-il prévu que ces restrictions (sur la communication du sens des conclusions du rapporteur public, ou sur la présence lors de leur prononcé) ne jouent pas lorsque c'est la CNCTR elle-même qui a saisi le Conseil d'État et qui est donc le requérant[18]. Mais cette exception est de faible portée puisque dans un tel cas, il n'y aura a priori le litige se déroulera entièrement entre parties appartenant à l'administration et également habilitées au secret de la défense nationale.

En revanche, rien n'a été prévu pour permettre aux parties tierces non habilitées au secret de la défense nationale (c'est-à-dire, le cas du requérant qui se prétendrait victime d'un abus d'usage d'une technique de renseignement) de pouvoir obtenir un certain niveau de connaissance du sens (à défaut du détail précis) des éléments protégés concernant le litige ou

[11] Créé par l'article 10 de la loi du 24 juillet 2015.
[12] C. Const, décision du 23 juillet 2015 précitée, considérant 86.
[13] En l'espèce, le Conseil constitutionnel a refusé qu'une condamnation puisse se fonder même partiellement sur le résultat d'une géolocalisation sans que les parties puissent avoir accès aux informations opérationnelles touchant la manière dont la géolocalisation a pu être réalisée (C. Const, décision n° 2014-693 précitée).
[14] Décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État.
[15] Nouvel article R. 773-20 du Code de justice administrative.
[16] Nouvel article R. 773-24 du Code de justice administrative.
[17] Nouvel article R. 773-23 du Code de justice administrative.
[18] Exception pour les recours formés en application du 2° de l'article L. 841-1 CSI dans les articles R. 773-23 et R. 773-24 du Code de justice administrative.

de pouvoir faire valoir, même par personne interposée, des arguments en défense à l'encontre des preuves secrètes qui seraient opposées par l'administration.

Certes, on peut penser que le juge administratif transposera dans ce nouveau contexte sa jurisprudence classique issue de son arrêt Coulon de 1955 [19] (lui-même inspiré, en la matière, par la fameuse jurisprudence Barel, qui lui était légèrement antérieure [20]) qui, même dans le cas où le secret de la défense nationale interdit la communication d'une information, permet au juge administratif de prendre « *toutes les mesures de nature à lui procurer, par les voies de droit, tous éclaircissements nécessaires, même sur la nature des pièces écartées et sur les raisons de leur exclusion ; qu'il a ainsi la faculté, s'il y échet, de convier l'autorité responsable à lui fournir, à cet égard, toutes indications susceptibles de lui permettre, sans porter aucune atteinte, directe ou indirecte, aux secrets garantis par la loi, de se prononcer en pleine connaissance de cause ; qu'il lui appartient, dans le cas où un refus serait opposé à une telle demande, de joindre cet élément de décision, en vue du jugement à rendre, à l'ensemble des données fournies par le dossier"* [21].

Mais on pourrait aussi réfléchir au développement d'une autre alternative suivant la pratique de certains États démocratiques (notamment le Canada et le Royaume-Uni) et admise par la jurisprudence de la CEDH. Elle consisterait à ce que des « avocats spéciaux » (selon la terminologie anglo-saxonne) et dûment habilités puissent, pour le compte du requérant mais sans pouvoir lui rendre compte, accéder aux données classifiées transmises au juge et faire valoir en audience à huis-clos tout moyen de fait ou de droit au soutien des intérêts de son client [22].

2b) Favoriser une contribution plus encadrée du renseignement aux procédures judiciaires

La loi du 24 juillet ne s'est pas limitée à organiser le contrôle de la légalité des techniques de renseignement par le Conseil d'État. Elle organise quelques liaisons avec le domaine judiciaire, par exemple en prévoyant (aux fins de la protection juridique des fonctionnaires) l'information automatique du service concerné via le Procureur général et la Chancellerie dans le cas où une demande étrangère d'entraide judiciaire concernerait l'activité à l'étranger de ces services [23]. Mais a elle aussi prévu, dans deux de ses dispositions, que la justice judiciaire – et principalement la justice répressive – puisse connaître indirectement de certains aspects des pratiques de renseignement. Bien que très limitées, ces deux articles ouvrent la voie à une judiciarisation plus large qui pourrait être efficace mais qu'il faudrait d'autant plus encadrer qu'elle pourrait être aussi la source d'abus préjudiciable aux libertés.

Il s'agit tout d'abord de l'article L. 841-1 CSI (relatif à la saisine du Conseil d'État) qui prévoit qu'outre la CNCTR et toute personne intéressée, le juge administratif pourra être également saisi, à titre préjudiciel, « lorsqu'une juridiction administrative ou une autorité judiciaire est saisie d'une procédure ou d'un litige dont la solution dépend de l'examen de la régularité d'une ou de plusieurs techniques de recueil de renseignement ».

Ce renvoi préjudiciel qui pourra être décidé « d'office ou sur demande de l'une des parties »

[19] CE, *Secrétaire d'État à la Guerre c/ Coulon*, 11 mars 1955, *Rec.*, 149 ; *RDP*, 1955. p. 995, concl. Grévisse.
[20] CE, Ass., *Barel et autres*, 28 mai 1954, *Rec.* 308, concl. Letourneur.
[21] CE, *Coulon*, *op. cit.*
[22] Voir également sur ce point, notre article précité (in S. Laurent & B. Warusfel, *op. cit*., 2015) ainsi que celui publié par les Cahiers de la sécurité, précité, juillet 2015, p. 75.
[23] Nouvel article 694-4-1 du code de procédure pénale (créé par l'article 9 de la loi du 24 juillet 2015).

devrait notamment être fréquemment utilisé lorsque, devant une juridiction pénale, il apparaît que certaines information ou éléments de preuve ont été obtenus par un service de renseignement et pourrait être le produit d'une des techniques de renseignement contrôlées (interceptions, sonorisations, pénétration informatiques, recueil de métadonnées, par exemple). Le but de cette saisine du Conseil d'État serait de valider au préalable la légalité de la source de renseignement, et donc de purger la procédure pénale subséquente de tout vice tenant, par exemple, à la déloyauté du recueil du renseignement [24]. Cela paraît donc fort utile et cohérent, puisque la nouvelle compétence du Conseil d'État et sa capacité à accéder directement au contexte classifié du recueil de l'information produite pourront apporter un élément de garantie bienvenue au juge pénal concerné, ainsi qu'aux parties auxquelles le renseignement est opposé.

Pour autant, le législateur s'est arrêté en chemin car, maintenant qu'il existe une procédure permettant de garantir que la technique de renseignement utilisée a été autorisée et mise en œuvre dans le respect de la loi, on ne voit pas pourquoi le juge judiciaire ne pourrait pas être rendu plus facilement destinataire d'informations issues des services de renseignement. On pourrait notamment suggérer que le code de procédure pénale comporte dans l'avenir une disposition organisant, via par exemple le Parquet, la transmission officielle par tout service de renseignement (sur la base de l'article 40 du code de procédure pénale, notamment) de toute information susceptible de concourir à la manifestation de la vérité dans les informations judiciaires ouvertes dans des domaines intéressant la sécurité nationale ou les intérêts fondamentaux de la Nation. S'inspirant du dispositif mis en place (et validé par le Conseil constitutionnel) en matière de géolocalisation judiciaire, cette information communiquée au juge d'instruction et soumise au débat contradictoire, pourrait être accompagnée d'un procès-verbal classifié détaillant le contexte et les conditions de recueil de cette information, lequel pourrait notamment servir de base pour la saisine préjudicielle du Conseil d'État visant à vérifier la légalité du recueil. Bien évidemment, et comme l'a précisé le Conseil constitutionnel dans sa décision sur la loi relative à la géolocalisation, aucune condamnation ne pourrait être fondée directement sur cette information recueillie dans des conditions secrètes [25].

Cette organisation de la judiciarisation du renseignement paraîtrait également cohérente avec l'esprit d'une autre disposition de la loi évoquant les relations entre les juridictions et le secret de défense. Le nouvel article L. 861-1 CSI établit en effet un mécanisme visant à préserver la « légalité occulte » d'actes administratifs relatifs à l'organisation ou au fonctionnement interne des services spécialisés de renseignement [26]. Dans ce cadre, il prévoit que « lorsque, dans le cadre d'une procédure engagée devant une juridiction administrative ou judiciaire, la solution du litige dépend d'une question relative à un acte non publié en application du présent article ou faisant l'objet d'une signature numérotée, ce dernier est communiqué, à sa demande, à la juridiction ou au magistrat délégué par celle-ci, sans être versé au contradictoire. Si cet acte est protégé au titre du secret de la défense nationale, la juridiction peut demander sa déclassification et sa communication en application de l'article L. 2312-4 du code de la défense ».

[24] On se souvient de la relaxe par la Cour d'appel de Paris (CA Paris, 10e chambre, 24 février 2009) de cinq anciens détenus français à Guantanamo (suite aux interrogatoires menés sur place par la DST, hors de tout contexte judiciaire), arrêt finalement cassé par la Cour de cassation (Cass. crim., n° 09-81736, 17 février 2010).
[25] Cons. Const., décision n°2014-693 DC du 25 mars 2014.
[26] Sur la « légalité occulte » déjà reconnue dans la jurisprudence du Conseil d'État à quelques occasions concernant les services de renseignement, voir notamment notre commentaire sous l'arrêt CE, 24 juin 2002, Ministre de la Défense c/ M. Wolny, *Droit & Défense*, 2003/2.

On trouve bien, dans ce cas particulier, la possibilité pour le juge judiciaire d'accéder – comme peut le faire désormais le juge du Conseil d'État s'agissant de la légalité des techniques de recueil – à certains aspects couverts par le secret de défense. Ici, il s'agit d'un acte relatif à l'organisation ou au fonctionnement d'un service de renseignement. Dans le cas de renseignements utiles à l'enquête judiciaire, il s'agirait d'indications sur leurs conditions de recueil afin d'en garantir la légalité (appréciée éventuellement préjudiciellement par le juge administratif) et la loyauté (par le juge judiciaire lui-même). Tout cela pourrait donc permettre une judiciarisation encadrée des résultats du renseignement et notamment être utilement complété par la mise en place d'un mécanisme d' « avocat spécial » (déjà évoqué) pouvant exercer un droit de regard sécurisé sur les données classifiées auquel le requérant n'aurait pas accès. Cela serait à la fois conforme à l'évolution que nous avons souvent soutenue vers un accès organisé des juges au secret [27] et aux conditions que pose la Cour européenne des droits de l'homme pour accepter la communication d'éléments classifiés dans les procédures judiciaires touchant la sécurité nationale [28].

3/ Un enjeu politico-juridique : user du droit comme contrepoids permanent à la pente sécuritaire

Votée quelques mois après les attentats parisiens de janvier 2015 et entrée en vigueur très peu de temps avant les attentats particulièrement meurtriers du 13 novembre 2015, la loi du 24 juillet 2015 a été souvent vue comme une loi « sécuritaire » alors que sa conception d'origine (que l'on trouve exposée en détail dès le rapport Urvoas-Verchère de la commission des lois en 2013 [29]) est celle d'une réforme de fond et non d'une réponse conjoncturelle à la violence [30]. Dans le nouveau contexte politique et opérationnel créé par ce déchainement sans précédent du terrorisme, il importe d'autant plus que son application serve à illustrer et préserver une forme démocratique de sécurité nationale et non à favoriser les dérives propres à ces périodes troublées. Or, de ce point de vue, plusieurs sujets incitent à une particulière vigilance.

3a) Lever les ambiguïtés relatives aux capacités de filtrage numérique indifférencié

La disposition du projet de loi sur le renseignement qui fut la plus décriée, et donc la plus discutée, est celle qui permet d'autoriser la mise en place de dispositifs de filtrage sur les réseaux des opérateurs numériques afin d'effectuer une détection automatique de certains comportements en ligne qui seraient les signes révélateurs d'une intention terroriste. Ces mécanismes, communément dénommés « boîtes noires » et mettant en œuvre des algorithmes

[27] Sur l'ensemble de cette thématique, voir notre ouvrage Bertrand Warusfel, *Contre-espionnage et protection du secret – Histoire, droit et organisation de la sécurité nationale en France*, Éditions Lavauzelle, 2000 (essentiellement son chapitre 11 et sa conclusion).

[28] La Cour européenne a bien résumé sa position en indiquant que *« l'utilisation d'informations confidentielles peut se révéler indispensable lorsque la sécurité nationale est en jeu. Cela ne signifie cependant pas que les autorités nationales échappent à tout contrôle des tribunaux internes dès lors qu'elles affirment que l'affaire touche à la sécurité nationale et au terrorisme (...) La Cour attache de l'importance au fait que ... au Canada, une forme plus efficace de contrôle juridictionnel a été mise au point pour les affaires de ce genre. Cela illustre bien l'existence de techniques permettant de concilier, d'une part, les soucis légitimes de sécurité quant à la nature et aux sources de renseignements et, de l'autre, la nécessité d'accorder en suffisance au justiciable le bénéfice des règles de procédure »* (CEDH, Chahal c. Royaume-Uni du 15 novembre 1996, requête n° 22414/93, cons. 131). C'est à la suite de cet arrêt que le Royaume Uni implémenta la pratique du « special advocate ».

[29] Rapport de la mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, Commission des Lois, Assemblée nationale, document n° 1022 du 14 mai 2013

[30] Sur la généalogie de la loi, voir notamment notre article précité in S. Laurent & B. Warusfel, op. cit., 2015.

ont été considérés par une large de l'opinion et de la société civile (en particulier, celle qui s'exprime sur les réseaux numériques) comme ouvrant la porte à des pratiques de surveillance numérique massive.

C'est donc le nouvel article L. 851-3 CSI qui « pour les seuls besoins de la prévention du terrorisme » permet au Premier ministre d'autoriser la mise en œuvre chez les opérateurs et les intermédiaires techniques de l'Internet « la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ».

Le Conseil constitutionnel l'a validé sans aucune réserve d'interprétation, estimant qu'elle comportait – outre les garanties générales prévues par la loi - suffisamment de limitations spécifiques, et notamment : la restriction au seul objectif antiterroriste, le contrôle de la CNCTR sur les paramètres de l'algorithme, la limitation à deux mois de la première autorisation d'utilisation, le fait qu'elle ne peut être prolongée que si les premiers résultats sont pertinents [31], la limitation de la collecte aux seules données de connexion, leur destruction au bout de soixante jours, l'impossibilité de recourir à la procédure d'urgence ou encore la nécessité d'obtenir une nouvelle autorisation spécifique pour pouvoir éventuellement tenter d'identifier la ou les personnes pouvant correspondre à un profil suspect [32].

On peut cependant estimer que, malgré ces précautions, la rédaction même de l'article laisse place à des ambiguïtés qui pourraient, sous réserve d'une interprétation extensive, engendrer des abus et déboucher sur des pratiques de surveillance de masse. Rappelons en effet que toute production d'un droit technologique (au sens d'un droit sur la technologie) comporte le risque d'une dénaturation de la règle édictée du fait de l'insuffisante maîtrise de la terminologie employée. Dans le cas d'espèce de ce nouvel article L. 851-3 CSI, la chose est manifeste à plusieurs égards :

> 1°) une contradiction potentielle existe s'agissant des données qui font l'objet du filtrage algorithmique. Il est dit que « ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent ». Or, le Conseil constitutionnel a interprété les dispositions de l'article L.851-1 (qui porte sur le recueil des données de connexion) comme couvrant uniquement les données conservées par les opérateurs de communication électronique, à savoir celles qui « portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux et ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications » ainsi que celles conservées par les hébergeurs, qui sont « de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires » [33]. Dès lors on peut s'étonner que l'article L. 851-3 CSI prétende limiter

[31] « la demande de renouvellement comporte un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements » (art. L. 851-3 CSI).
[32] C. Const, décision du 23 juillet 2015 précitée, considérant 60.
[33] C. Const, décision du 23 juillet 2015 précitée, considérant 55.

le recueil à des informations ne permettant pas d'identifier les internautes, alors qu'au contraire les données de connexion faisant l'objet du filtrage ont pour principale caractéristique de favoriser leur identification.

2°) Cette incohérence est renforcée par le fait que, bien que l'on ne recueille à l'origine que des données « qui répondent à leurs paramètres de conception » (section I), on affirme quelques paragraphes plus loin, que s'il est détecté parmi ces données une suspicion de menace terroriste, il pourra être autorisé « l'identification de la ou des personnes concernées » (section IV), ce qui laisse supposer que les données initialement recueillies peuvent donc servir de base à une identification (ce que l'on appelle des données « indirectement nominatives ») et ne sont pas aussi anonymes que cela [34].

3°) l'obligation de destruction au bout d'un délai de soixante jours (considérée par le Conseil constitutionnel comme une garantie) ne porte en réalité que sur les données personnalisées recueillies après identification (les « données y afférentes ») qui s'avèreraient dans ce délai ne pas révéler « l'existence d'une menace terroriste attachée à une ou plusieurs des personnes concernée » (section IV du même article). En revanche, un doute sérieux existe sur la durée de conservation des données personnalisées accréditant une menace terroriste potentielle (et donc méritant d'être étudiées par des analystes) ainsi que des données supposées anonymes qui avaient été recueillies initialement. En l'absence d'indication précise de la loi, on peut penser qu'elles seraient peut-être soumises néanmoins à une obligation de destruction au bout de quatre années, en vertu de l'article L. 822-2 CSI qui prévoit cette durée pour « les informations ou documents mentionnés à l'article L. 851-1 » (c'est-à-dire justement les métadonnées). Mais l'interprétation du juge administratif sur ce point sera attendue avec intérêt.

Si l'on ajoute (comme de nombreux commentateurs ou mémoires déposés devant le Conseil constitutionnel l'ont fait) que le dispositif concerné est défini de manière extrêmement allusive (« traitement automatisé de données » utilisant des « paramètres de détection »), on peut penser qu'il ne serait pas très difficile de justifier sous le couvert de cette disposition la mise en œuvre d'un outil de filtrage massif des communications électroniques pratiquant le tri des données à partir d'une bibliothèque croisant un ensemble très important de paramètres, ce qui reviendrait à établir - sous couvert de prévention du terrorisme - un mécanisme de *big data* gouvernemental assurant une surveillance très fine des échanges numériques de la population. Il s'agirait certainement d'une dérive qui ne correspondrait pas à l'objectif voulu par le Parlement mais la détection de cette dérive serait pour autant très difficile à apporter que l'algorithme et ses paramètres sont classifiées et seront difficiles à inspecter en permanence.

Comme les débats autour de ce texte l'ont bien montré, on a pris conscience du fait que « la valeur des données de connexion et de leur traitement est égale voire supérieure à celle du contenu même des communications » [35] et, plus encore, que la surveillance non ciblée des communications tend à devenir une pratique largement répandue dans le domaine du

[34] Voir à ce sujet le mémoire d'*amicus curiae* de la Commission nationale consultative des droits de l'homme qui renvoie également à la délibération n° 2015-078 de la CNIL du 5 mars 2015 en la matière.

[35] Bertrand Warusfel, "Pour un approfondissement du cadre juridique des interceptions de sécurité", in *21ème rapport d'activité (2012-2013) de la Commission de contrôle des interceptions de sécurité*, Documentation française, 2014, p. 19.

renseignement technique [36]. Dès lors, le respect premier du à la vie privée, tel qu'affirmé en tête de la loi du 24 juillet 2015 (article L. 801-1 CSI précité) impose que l'application de cet article L. 851-3 CSI si controversé soit particulièrement vigilante. Non seulement, il faut veiller à ce que le dispositif ne puisse – en violation avec le texte – servir à intercepter le contenu de communications [37], mais encore – et surtout – que l'exploitation des seules métadonnées ne se traduise pas par un profilage contraire à la vie privée et aux libertés démocratiques [38].

Cela va être l'une des missions les plus délicates de la CNCTR (dont un seul membre, désigné par le Président de l'ARCEP, a des compétences particulières en matière de technologies de l'information) et il faut espérer que les allocations budgétaires et d'emploi consenties à la Commission lui donneront la possibilité de constituer une équipe d'experts techniques suffisant étoffée pour pouvoir expertiser les développements classifiés qui seront réalisés à la demande des services de renseignement pour assurer ce filtrage et le mettre à jour, ainsi que pour pouvoir réaliser régulièrement des inspections ou des audits techniques et physiques afin d'en vérifier l'adéquation au périmètre des autorisations accordées.

On peut aussi souhaiter qu'à l'occasion d'éventuels contentieux qui pourraient naître à terme sur l'application de ce texte, le Conseil d'État ainsi que, le cas échéant, la CEDH, puissent pallier par leur jurisprudence les lacunes actuelles de la loi. Rappelons en effet que le contrôle juridictionnel dans ces matières peut être efficace, comme l'ont montré ces dernières années les décisions successives de plusieurs cours suprêmes (dont, en particulier la Cour constitutionnelle allemande de Karlsruhe en 2010 [39]) puis de la Cour de justice de l'Union européenne, qui ont censuré respectivement certaines lois nationales sur la conservation des données de connexion et la directive 2006/24/CE de l'Union européenne sur le même sujet de la rétention des métadonnées [40].

3b) Le nécessaire développement d'un droit du renseignement d'État

S'il y a une relative urgence à ce que la nouvelle chaîne de contrôle sécurise juridiquement le recours aux moyens particuliers de collecte technique du renseignement, on peut déjà conjecturer que d'autres questions juridiques devront être résolues dans le cadre de l'application de la loi de 2015. A défaut de pouvoir imaginer à l'avance tous ces sujets (et notamment de pouvoir prédire les dérives qui pourraient être révélées à la CNCTR par le nouveau mécanisme de « lanceur d'alerte » [41]), on se contentera d'évoquer quelques

[36] Voir Sébastien Laurent, « Liberté et sécurité dans un monde anomique de données », *in* CNCIS, *22ème rapport d'activité. Années 2013-2014*, La documentation française 2015, p. 16 (renvoyant pour la distinction entre « targeted surveillance » et « dragnet surveillance » à l'intervention de J. Appelbaum au Conseil de l'Europe en janvier 2014).

[37] Un tel détournement serait d'autant plus clairement *contra legem* que l'article L851-7 CSI qui clôture le même chapitre du Code de la sécurité intérieure, affirme nettement que « le présent chapitre est mis en œuvre dans le respect de l'article 226-15 du code pénal », ce qui exclut toute interception par ce biais, laquelle violerait le secret des communications électroniques protégées par l'article 226-15 CP.

[38] X. Latour écrit que « la loi peut donner l'impression de favoriser le développement d'une surveillance de masse déclenchée par une autorité politique, le Premier ministre » (X. Latour, précité).

[39] Cour constitutionnelle allemande, 2 mars 2010, Rev. NJW 2010, p. 833, note B. Deshayes & D. Reinhold, *Communication Commerce Électronique*, n° 12, décembre 2010, étude 24.

[40] CJUE, 8 avril 2014 Digital Rights Ireland, C-293/12, qui a notamment reproché à la directive censurée de s'appliquer *« même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. (*§58).

[41] Nouvel article L. 861-3 CSI (créé par la loi du 24 juillet 2015).

orientations que pourrait suivre la doctrine et la jurisprudence en la matière dans les prochaines années.

La première piste devrait découler assez logiquement d'une affirmation que le Conseil constitutionnel a tenu à mettre en avant à l'occasion de sa validation de la logique d'ensemble de la loi. Souhaitant confirmer la nature administrative de l'action des services de renseignement, et donc la compétence exclusive du juge administratif pour connaître de la légalité de leurs pratiques, le Conseil a dit pour droit que le recueil de renseignement par les services spécialisés « relève de la seule police administrative ; qu'il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions ; qu'il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs » [42].

Ainsi est affirmée la nécessité démocratique de préserver une différence de nature et une séparation opérationnelle entre le renseignement de sécurité nationale et les pratiques judiciaires, y compris si celles-ci utilisent parfois les mêmes techniques. Si l'on a pu, en effet, relever qu'il existait matériellement une « quasi-gémellité avec les techniques judiciaires » autorisées aux services de police judiciaire depuis la loi Perben II de 2004 [43], il ne faudrait cependant pas confondre leurs finalités et leur cadre d'emploi.

Cette exigence pourrait paraître contradictoire avec ce que l'on a dit plus haut concernant la nécessité d'organiser la « judiciarisation » de certains résultats de renseignement. Mais il n'en est rien. Bien au contraire, c'est parce que le renseignement ainsi collecté par des moyens spéciaux n'ait pas une simple information venue à la connaissance fortuite d'un service public, qu'il ne peut pas être communiqué à une juridiction sans que l'on aménage cette communication. L'inscription dans le code de procédure pénale d'un mécanisme spécial et limité de contribution aux enquêtes judiciaires serait bien le signe de cette différentiation entre deux activités publiques qui peuvent amener à coopérer sans se confondre.

Inversement, il y aurait confusion des genres et des droits (et donc atteinte potentielle aux libertés et au droit au procès équitable) si la proximité pouvant exister entre des pratiques de renseignement judiciaire et celles du renseignement de sécurité nationale débouchait sur une mise en commun des moyens et des résultats effectuée hors du regard du juge judiciaire.

Cet effort de différentiation devrait être également complété par la détermination jurisprudentielle de critères permettant de fixer la frontière entre les domaines de la sécurité nationale et de la sécurité publique. Sans revenir en détail sur le nouveau concept juridique de « sécurité nationale » établi en 2009 [44], on rappellera seulement que ni la définition de la sécurité nationale donnée par l'article L. 1111-1 CDéf., ni celle de la sécurité intérieure donnée par l'article L.111-1 CSI ne suffisent à distinguer très clairement les deux notions et les contours de leur recouvrement partiel [45].

[42] C. Const, décision du 23 juillet 2015 précitée, considérant 9.
[43] Gildas Roussel, « Le régime des techniques de renseignement », *AJ Pénal*, 2015 p.520.
[44] Voir notamment Bertrand Warusfel, "Les implications juridiques et institutionnelles de la notion de sécurité nationale", in X. Latour & Chr. Vallar (dir.), *Le droit de la sécurité et de la défense en 2013*, Presses Universitaires d'Aix-Marseille, 2014, pp. 17-30
[45] Sur ce point, voir notamment Olivier Gohin, Introduction au commentaire du *Code de la sécurité intérieure*, LexisNexis, 2014, pp. 2-4.

Mais le Livre blanc de 2008 (dont est issue la notion de sécurité nationale) nous précise que – si la politique de défense concoure « en totalité » à la sécurité nationale, de même que la « sécurité civile » – la politique de sécurité intérieure, en revanche, n'y participe que « pour tout ce qui ne relève pas de la sécurité quotidienne et individuelle des personnes et des biens » [46]. Rapporté à la définition donnée par le second alinéa de l'article L.111-1 CSI, cela pourrait signifier que, parmi les objectifs de la sécurité intérieure :

- la « défense des institutions et des intérêts nationaux » ainsi que « le maintien de la paix » constituent aussi des objectifs de sécurité nationale, alors que

- le « respect des lois », le « maintien de l'ordre public » et « la protection des personnes et des biens » font partie de cette sécurité publique quotidienne qui ne relève pas de la stratégie de sécurité nationale ni du régime juridique dérogatoire qui y est attaché (dont notamment les prérogatives en matière de renseignement prévues par la loi de juillet 2015).

Mais si ce schéma théorique paraît intellectuellement cohérent, il n'évite pas que plusieurs domaines délicats se situent à la charnière entre ces différentes notions. Il en va ainsi plus particulièrement du domaine très vaste de la lutte contre la délinquance et la criminalité organisée, définie de manière très extensive – depuis la loi du 9 mars 2004 – par l'article 706-73 du code de procédure pénale.

En effet, de nombreux délits rentrant dans le champ d'application de cet article ressortissent à des objectifs de répression judiciaire de droit commun affectant (même très gravement) la seule sécurité des personnes et des biens plutôt qu'à des formes criminelles de grande ampleur pouvant affecter la vie de la Nation dans son ensemble (ce qui est le cas du terrorisme, par exemple, visé au 11° de l'article 706-73 CPP).

Comme les services de police judiciaire possèdent depuis cette même loi Perben II la possibilité de mettre en œuvre, sous contrôle judiciaire, des techniques de renseignement criminel proches de celles couvertes par la loi de juillet 2015, il serait approprié de considérer que la mission de « prévention de la criminalité et de la délinquance organisées » reconnue aux services spécialisés de renseignement (par le 6° de l'article L. 811-3 CSI) et le recours aux techniques administratives qui en découle ne peuvent concerner que les formes de délinquance et de criminalité organisée susceptibles de porter atteinte à des intérêts fondamentaux de la nation ou de constituer une menace de sécurité nationale.

En fixant ainsi progressivement les critères d'une telle différentiation, on évitera que des mêmes organisations criminelles puissent être alternativement ou parallèlement visées par des opérations de renseignement criminel ordonnées par le parquet ou par des investigations de renseignement administratif autorisées par le Premier ministre sur le fondement de la loi du 24 juillet 2014. Outre les difficultés opérationnelles que cela pourrait poser, cela compliquerait ensuite l'exploitation judiciaire des données recueillies par des voies concurrentes mais juridiquement distinctes [47].

A plus longue échéance, on peut aussi envisager que le contrôle sur le renseignement de

---

[46] *Livre blanc sur la défense et la sécurité nationale*, Ed. O. Jacob, 2008, Tome I, p. 62.

[47] G. Roussel n'hésite pas à pronostiquer « la requalification en opération de police judiciaire » et que « la mise en oeuvre d'une technique débouche à l'avenir sur un conflit de compétence qui devra être tranché par le Tribunal des conflits » (G. Roussel, 2015, précité).

sécurité nationale évolue de celui des seules techniques de renseignement vers celui des missions de renseignement. En effet, si la loi du 24 juillet 2015 ne prévoit expressément l'autorisation et le contrôle que de l'emploi par les services de quelques techniques de recueil d'informations particulièrement intrusives, elle a cependant fixé aux nouveaux articles L. 811-1 et L. 811-2 CSI un cadre général à la politique publique de renseignement et à l'action des services spécialisés qui en découle.

La politique de renseignement ne peut avoir comme objectif que de concourir « à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation » (art. L. 811-1 CSI) et les services spécialisés de renseignement ont, dans ce cadre, mission de rechercher « des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation » afin de les anticiper, les prévenir ou les entraver.

Il serait faux de croire que ces affirmations législatives resteront sans efficacité politique et juridique. Juridiquement, en effet, le recours aux techniques particulières de renseignement prévues par la loi, est lui-même dépendant de la détermination du champ des missions confiées aux services concernées puisque elles ne peuvent être utilisées par les services que « pour le seul exercice de leurs missions respectives » (article L. 811-3 CSI) et que leur mise en œuvre ne peut être autorisée que si « elles sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 » (article L. 801-1 CSI 4°). De ce fait, la légitimité d'une opération de renseignement dont l'objectif serait manifestement en dehors du champ des missions confiées au service concerné pourrait être contestée à l'occasion du contrôle sur les techniques de recueil de renseignement qui y seraient employées.

Mais c'est également le contrôle politique qu'exerce – plus particulièrement depuis la réforme de décembre 2013 [48] - la délégation parlementaire au renseignement, qui pourrait s'appuyer sur ces nouvelles dispositions définissant les missions et les limites des pratiques de renseignement. Et ce d'autant que la CNCTR et la délégation parlementaire sont désormais amenées à s'informer et à coopérer en application des nouveaux articles L. 833-10 CSI (transmission à la DPR des observations de la CNCTR au Premier ministre) et L. 833-11 CSI (demande d'avis de la DPR à la CNCTR).

Conclusion

Tout autant que l'adoption de la loi relative au renseignement en juillet 2015, sa mise en oeuvre par la communauté française du renseignement et l'acculturation de celle-ci aux nouvelles logiques juridiques qu'elle instaure vont apporter une contribution majeure à la constitution progressive d'un droit français de la sécurité nationale.

L'émergence de ce nouveau droit consacre un renversement de la perspective entre exercice du pouvoir régalien - dans ses aspects les plus secrets et les plus souverains - et droit. La pratique classique, basée sur une raison d'État implicite, assurait une large immunité à l'« État secret » mais sans offrir de garantie individuelle à ses agents ni procurer de reconnaissance

[48] Voir les modifications de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 (à nouveau modifié par la loi du 24 juillet 2015) introduites par l'article 12 de la loi de programmation militaire du 18 décembre 2013.

démocratique aux missions de renseignement. A cette situation devenue très instable, les récentes réformes de sécurité nationale veulent substituer un nouvel équilibre entre des activités plus encadrées et, en contrepartie, une légitimité politique mieux assurée et une légalité contrôlée.

Cette sécurité nationale, en charge de protéger les intérêts vitaux de notre collectivité, bénéficie ainsi d'un régime juridique spécial autorisant, de ce fait et sous réserve d'une juste proportionnalité, des restrictions aux libertés individuelles plus importantes que celles usuellement autorisées au titre des missions habituelles de sécurité publique.

Mais cette superposition d'un régime de sécurité nationale aux dispositifs sécuritaires de droit commun (qu'il s'agisse de police administrative ou de police judiciaire) ne restera conforme aux principes de l'État de droit qu'à deux conditions : d'une part, que la frontière entre droit commun et droit spécial soit clairement établie et juridictionnellement contrôlée et, d'autre part, que l'on évite – malgré la gravité des menaces contemporaines - d'interpréter trop largement les nouvelles dispositions légales (et notamment celles de la loi relative au renseignement) ce qui reviendrait à inverser le principe (c'est-à-dire les règles administratives et pénales de droit commun) et l'exception (le régime de sécurité nationale).

Ce dernier risque n'est pas théorique. Il s'est déjà matérialisé durant la dernière décennie dans de grandes démocraties, à commencer par les États-Unis, où l'on sait aujourd'hui qu'en sus des dispositions très intrusives du Patriot Act, la présidence s'est livrée après 2001 à un véritable contournement des garanties légales préexistantes et en particulier de celles du FISA Act [49].

L'essor actuel des pratiques de renseignement, non seulement pour prévenir les menaces et les crises extérieures, mais aussi pour orienter précocement les instruments de contrôle social et de répression intérieure (ce que les Anglo-saxons appellent « Intelligence-led-policing »[50]) recèle intrinsèquement une dimension paranoïaque. Et celle-ci est accrue par les nouvelles espérances que font entrevoir les technologies numériques (algorithmes, big data, deep packet inspection, …) qui donnent l'illusion qu'un renseignement technique de haute intensité pourrait détecter précocement la plupart des menaces [51].

Face à ces logiques prédictives et préemptives qui entretiennent une suspicion généralisée et poussent à la surveillance de masse, l'État de droit impose la mise en oeuvre d'une contre-logique qui neutralise en permanence cette pente sécuritaire. C'est tout l'enjeu de ce droit démocratique de la sécurité nationale qui se construit sous nos yeux mais qui aura besoin de notre vigilance pour qu'il produise à la fois efficacité opérationnelle, acceptabilité sociale et respect des libertés.

---

[49] Voir notamment Elizabeth Goitein and Faiza Patel, *What Went Wrong With The FISA Court*, Brennan Center for Justice, 2015 ; également Sébastien Mort, « Surveillance des correspondances privées dans le cyberespace aux États-Unis : un contrôle marqué au sceau du secret », *Revue française d'études américaines* 2010/1 (n° 123), p. 33-53.

[50] Pour un document officiel américain caractéristique de cette nouvelle approche : *Intelligence-Led Policing: The New Intelligence Architecture*, US, Dept of Justice - Bureau of Justice Assistance, NCJ 210681, septembre 2005.

[51] Voir l'article de S. Laurent, précité (CNCIS, *op. cit.*, 2015), pp. 15-18. Chr. Lazerges et H. Henrion-Stoffel estime, pour leur part que « le risque d'un « état panoptique » est donc à prendre au sérieux et un contrôle efficace des opérations de recueil du renseignement est essentiel » (*RSC*, 2015 précité).