INSTITUT
MONTAIGNE

Pour une véritable politique publique du renseignement

Sébastien-Yves Laurent

ÉTUDE JUILLET 2014

L'Institut Montaigne est un laboratoire d'idées - think tank - créé fin 2000 par Claude Bébéar et dirigé par Laurent Bigorgne. Il est dépourvu de toute attache partisane et ses financements, exclusivement privés, sont très diversifiés, aucune contribution n'excédant 2 % de son budget annuel. En toute indépendance, il réunit des chefs d'entreprise, des hauts fonctionnaires, des universitaires et des représentants de la société civile issus des horizons et des expériences les plus variés. Il concentre ses travaux sur quatre axes de recherche :

- Cohésion sociale (école primaire, enseignement supérieur, emploi des jeunes et des seniors, modernisation du dialogue social, diversité et égalité des chances, logement)
- Modernisation de l'action publique (réforme des retraites, justice, santé)
- Compétitivité (création d'entreprise, énergie pays émergents, financement des entreprises, propriété intellectuelle, transports)
- Finances publiques (fiscalité, protection sociale)

Grâce à ses experts associés (chercheurs, praticiens) et à ses groupes de travail, l'Institut Montaigne élabore des propositions concrètes de long terme sur les grands enjeux auxquels nos sociétés sont confrontées. Il contribue ainsi aux évolutions de la conscience sociale. Ses recommandations résultent d'une méthode d'analyse et de recherche rigoureuse et critique. Elles sont ensuite promues activement auprès des décideurs publics.

À travers ses publications et ses conférences, l'Institut Montaigne souhaite jouer pleinement son rôle d'acteur du débat démocratique.

> *L'Institut Montaigne s'assure de la validité scientifique et de la qualité éditoriale des travaux qu'il publie, mais les opinions et les jugements qui y sont formulés sont exclusivement ceux de leurs auteurs. Ils ne sauraient être imputés ni à l'Institut, ni,* a fortiori*, à ses organes directeurs.*

Il n'est désir plus naturel
que le désir de connaissance

INSTITUT
MONTAIGNE

À PROPOS DE L'AUTEUR

Sébastien-Yves Laurent est professeur à la faculté de droit et de science politique de l'Université de Bordeaux où il est co-directeur du Master professionnel « Sécurité globale et analyste trilingue ». Il enseigne aussi à Sciences Po Paris et à l'IEP de Bordeaux. Membre du conseil scientifique du Conseil supérieur de la formation et de la recherche stratégique (CSFRS), il est également expert et consultant sur les questions de sécurité. Il est l'auteur de nombreux ouvrages et articles dans des revues universitaires internationales

Pour une véritable politique publique du renseignement

par Sébastien-Yves Laurent

ÉTUDE - Juillet 2014

« La justice sans la force est impuissante. La force sans la justice est tyrannique. La justice sans force est contredite parce qu'il y a toujours des méchants. La force sans la justice est accusée. Il faut donc mettre ensemble la justice et la force, et pour cela faire que ce qui est juste soit fort ou que ce qui est fort soit juste. La justice est sujette à dispute. La force est très reconnaissable et sans dispute. Ainsi on n'a pu donner la force à la justice, parce que la force a contredit la justice, et a dit qu'elle était injuste, et a dit que c'était elle qui était juste. Et ainsi ne pouvant faire que ce qui est juste fût fort, on a fait que ce qui est fort fût juste ».

(Blaise Pascal, *Pensées,* 1670)

SOMMAIRE

ARGUMENT

Depuis que le *Livre blanc* de la Défense de 2008 l'a qualifié de cinquième fonction stratégique, le renseignement collecté et utilisé par l'État, intitulé désormais « connaissance et anticipation », a pris une ampleur considérable, formalisée par un second *Livre blanc* en 2013, deux lois de programmation militaire et de nombreuses transformations dans son organisation générale.

Ce rapport procède à un état des lieux et examine les trois enjeux majeurs de cette évolution notable : pour la sécurité de la Nation (1), du point de vue de la protection des libertés publiques (2) et en matière économique (3). Le développement récent du renseignement traduit concrètement une forte ambition française à l'heure où ses activités s'étendent à la « nouvelle frontière » du cyberespace. Il ne relève pas d'une politique publique comparable, par exemple à celles menées en matière de sécurité ou de défense. Au service direct et exclusif du pouvoir exécutif, la connaissance et l'anticipation touchent au « domaine très réservé ». Marquée structurellement par le secret et participant directement à l'exercice de la sécurité du pays, cette fonction, « stratégique » à plusieurs titres, doit – pour être efficace – se tenir à distance des exigences actuelles de transparence et demeurer protégée du dévoilement. Les services « secrets » qui sont aussi parfois qualifiés de « spéciaux » ne peuvent que demeurer singuliers. Une démocratie libérale comme la nôtre peut assumer cette singularité sans pour autant renier ses principes fondateurs. C'est toute l'ambition de ce rapport de le démontrer.

Dans notre société démocratique et ouverte, l'assentiment et la confiance des citoyens, sujets de droit et contribuables, est indispensable. Dans ce cadre, la mise en œuvre de cette fonction stratégique qui s'appuie sur des moyens budgétaires croissants, sur un statut administratif et un appareil juridique dérogatoires au droit commun, doit s'accompagner de contrôles sérieux, d'indicateurs pour le public et d'une information destinée en premier lieu à la représentation nationale avec un régime de publicité propre. En s'appuyant ponctuellement sur des comparaisons appropriées avec l'Allemagne, le Royaume-Uni et les États-Unis, le rapport détaille l'ensemble des évolutions souhaitables qui visent d'une part à rendre le renseignement plus efficace en le rationalisant et d'autre part à mieux garantir la protection des citoyens : 48 recommandations organisées en six ensembles complètent le document. Ces mutations, favorisant un climat de confiance, permettront également de préserver la légitimité de la dépense publique en la matière. En effet, celle-ci n'est rien d'autre qu'un investissement stratégique pour la sécurité des citoyens, mais qui bénéficie aussi à un secteur économique privé performant, celui de la confiance et de la sécurité, en forte croissance en France depuis quelques d'années, mais qui doit être encouragé et renforcé pour mieux préparer un avenir qui se décide aujourd'hui.

RÉSUMÉ

En quelques années, le renseignement semble être sorti de l'ombre en France. Il a même connu une véritable promotion sous l'appellation de cinquième « fonction stratégique », la « connaissance et l'anticipation », affirmée dans les *Livres blancs* sur la défense de 2008 et 2013, confirmée par des dispositions spécifiques des lois de programmation militaire de juillet 2009 et de décembre 2013. À l'origine de ce rapport se trouve une question : au terme de cette transformation le renseignement est-il devenu une politique publique à part entière ? On y a ici répondu en nous appuyant sur une soixantaine d'entretiens menés avec 51 personnalités, sur la documentation publique, abondante et en ayant conduit des comparaisons étrangères, principalement en Europe. Il s'agit en fait d'aller au cœur d'un « domaine très réservé » afin de réaliser un état des lieux global du renseignement en passant en revue quatre enjeux : le périmètre budgétaire, l'articulation politico-administrative des « services », leurs moyens techniques et juridiques ainsi que les conséquences directes sur les libertés publiques, enfin la perception du renseignement dans la société. Le rapport s'achève par des recommandations en vue de renforcer le renseignement public avec ses spécificités tout en le rapprochant de l'État de droit et des valeurs de la démocratie libérale.

LES SINGULARITÉS DES SERVICES FACE AU DROIT ET À LA DÉMOCRATIE

Ce domaine très singulier de l'action de l'État n'est naturellement pas soumis aux usages habituels de publicité et de contrôle parlementaire. L'efficacité même de la collecte de l'information « fermée » et celle de son utilisation exigent une discrétion relative ou absolue. En outre, et ce pour les mêmes raisons, le cadre juridique des moyens mis à la disposition des services de renseignement est-il particulier, échappant souvent au domaine de la loi et au droit commun, voire échappant à toute forme de cadre juridique. Notre idée est que la démocratie française, l'une des plus anciennes au monde, doit assurer sa solidité et sa pérennité en s'adaptant à cette situation singulière avec le souci permanent d'un examen attentif de l'état réel des libertés. Or la France connaît un « double retard », celui de la protection des libertés par rapport à l'exercice de la sécurité et celui de la protection des libertés par rapport aux mutations technologiques permanentes.

L' « INSÉCURITÉ JURIDIQUE » POUR LE CITOYEN ET POUR L'ÉTAT

Aujourd'hui les activités des organes de renseignement relèvent autant du code de la défense que du code de sécurité intérieure et du code pénal, et certaines de leurs pratiques touchent aussi directement à la limitation de certaines libertés publiques essentielles, en particulier à la liberté individuelle, au travers notamment de la liberté d'aller et venir et du droit au respect de la vie privée. La situation juridique des cinq services de renseignement qui s'inscrit dans un cadre réglementaire dépendant de l'exécutif, bien loin du domaine de la loi débattue publiquement, rend la question de la dimension juridique des outils utilisés par les services encore plus fragile. Cette situation déjà complexe naturellement l'est rendue plus encore par l'apparition de droits externes, communautaire et européen, dont l'influence sur le droit français ne cesse de croître. Du point de vue des services de renseignement, la dialectique pratique entre sécurité et libertés peut être observée en matière d'écoutes et d'interceptions de communication, de protection des données ou encore de classification de l'information. Sur l'ensemble de ces aspects, la dispersion des règles de droits, la prévalence du cadre de police administrative d'une part, et le rôle croissant du droit externe de l'autre, exposent de façon croissante l'État à « l'insécurité juridique » selon la formule du Conseil d'État et débouchant soit sur des censures du Conseil Constitutionnel par le biais de recours parlementaires, soit à des questions prioritaires de constitutionnalité, soit enfin l'exposant à une condamnation par la Cour de Strasbourg.

2008-2014 : UNE RÉFORME DE TRÈS GRANDE AMPLEUR POUR LES SERVICES

La promotion publique du renseignement s'est accompagnée à partir de 2008 d'une profonde réforme de la gouvernance générale des « services » qui s'est traduite par le renforcement des liens avec la Présidence de la République au détriment du Premier ministre. La tâche de coordination des services a été confiée à un coordonnateur rattaché à l'Élysée. Un Conseil national du renseignement, héritier du Comité interministériel du renseignement créé au début de la V^{e} République et dépendant de Matignon, a également été créé mais laissé en déshérence. Les services de renseignement intérieur ont été transformés avec la création de la DCRI, résultat de la fusion entre la DST et une partie des renseignements généraux. Enfin, un organisme parlementaire, la DPR, a été chargé d'une tâche de « suivi » de

« l'activité générale des services », pratiquement de portée assez symbolique. Les lois de programmation militaires de 2009 et 2013 ont complété la transformation en profondeur de la nouvelle fonction stratégique « connaissance et anticipation » en renforçant le budget des services de renseignement dépendant du ministère de la Défense (DGSE, DRM, DPSD), mais de façon très inégale, la DGSE ayant principalement bénéficié de l'effort budgétaire. La nouvelle DCRI a ainsi été le parent pauvre de l'effort budgétaire de la période 2008-2014. Il est heureux que l'alternance politique de 2012 n'ait pas remis en cause la réforme commencée en 2008 qui a été donc poursuivie, cette fois avec le rôle important de la Commission des lois de l'Assemblée nationale dont le président a proposé dans deux rapports parlementaires du printemps 2013 un ensemble de modifications, reprises en partie dans la loi de programmation militaire. Ainsi, à une première phase de réforme d'origine présidentielle, a succédé une seconde après 2012 au cours de laquelle l'Assemblée nationale a été associée. L'effort budgétaire a permis de rehausser la France par rapport à ses rivaux et partenaires, mais la question de sa poursuite dans les années à venir est susceptible d'être posée. L'établissement d'un authentique contrôle parlementaire des services est un acquis théorique très récent (décembre 2013) mais dépendra, pour être effectif, de la confiance établie entre les parlementaires et les services. Enfin, la transformation de la DCRI en DGSI en mai 2014 est une réforme administrative souhaitée par le service lui-même, notamment pour être en prise directe avec le ministre de l'Intérieur.

Cette étude entend donc faire un bilan de près de six années de réformes, d'en souligner la portée sans manquer d'en relever les absences ou les faiblesses. La valorisation publique du renseignement est nécessaire dans son principe : en effet le renseignement participe directement à l'exercice de la sécurité du pays sur son territoire comme à l'extérieur des frontières. En d'autres termes, s'il n'est pas un « service public », le renseignement rend un service au public, qui est essentiel. Des faiblesses organisationnelles, juridiques, techniques et budgétaires demeurent néanmoins, certaines étant préoccupantes.

UN BUDGET GLOBAL EN HAUSSE MAIS DÉSÉQUILIBRÉ POUR DES SERVICES BALKANISÉS

Résultat de la défense des périmètres ministériels et de leur sédimentation historique, les acteurs du renseignement forment un ensemble très épars, avec

des statuts divers (militaires, policiers, douaniers, analystes civils, ingénieurs et techniciens) et des prérogatives correspondantes extrêmement hétérogènes. En outre leur hiérarchie est éclatée entre trois ministères de tutelle différents. La création en mai 2011 du statut administratif des « services spécialisés » pour rassembler les six d'entre eux considérés comme les plus importants (DGSE, DCRI-DGSI, DRM, DPSD, DNRED, Tracfin) entendait favoriser la création d'une « communauté du renseignement ». Elle représente aujourd'hui entre 12 000 et 13 000 personnes. Une partie des moyens de renseignement utilisés par la DRM étant présente dans les forces, on peut penser toutefois que les effectifs réels sont nettement plus élevés. Au-delà de la difficulté à dénombrer précisément les effectifs véritables des six services, on peut s'interroger sur le fait qu'un certain nombre de services (RGPP et Gendarmerie, mais également la SDIG) constituent *de facto* un second cercle. Fort logiquement protégé de la curiosité extérieure, le budget des six services n'est pas aisé à connaître avec précision, notamment pour les services relevant de l'Intérieur et de Bercy. À partir des lois de finances on peut arriver néanmoins à un ordre de grandeur de plus d'1,5 Md€ annuels qui est une hypothèse très basse et qui ne tient pas compte du coût de la recherche publique sur les technologies utilisées par les services. De façon peu surprenante, la DGSE, service extérieur qui fournit le pouvoir exécutif en analyses à vocation stratégique, devance de loin l'ensemble des autres services. Aujourd'hui, la question de la préservation du budget de l'ensemble des services et notamment de la DGSE risque d'être posée : de notre point de vue, il faut non seulement le garantir, mais également l'accroître, de façon raisonnée. Les services, à commencer par la DGSE, pourraient toutefois se trouver sous la menace d'un « effet de ciseau » avec un budget décroissant et des coûts technologiques croissants. Par ailleurs, malgré l'annonce en mai 2014 des recrutements de personnels pour la DGSI au cours des cinq années à venir, il n'est pas assuré que ces emplois pourront être préservés étant donné l'état des finances publiques. Or, ils sont importants pour la diversification des personnels (techniciens, linguistes, analystes) dans une administration composée exclusivement de fonctionnaires de police.

POURSUIVRE LA CO-PRODUCTION PUBLIC-PRIVÉ DANS LE CYBERESPACE

Le cyberespace est devenu indispensable pour les services de renseignement : c'est un lieu de collecte d'information et de conduite d'opérations dont l'importance croît chaque jour, à mesure que l'espace numérique augmente. Pour les services

étrangers également. Ainsi, les données de nos concitoyens et de nos entreprises sont-elles l'objet de captations quotidiennes. En quelques années seulement l'État a réorganisé en profondeur le dispositif cybernétique défensif et offensif. Le domaine cybernétique est un lieu particulier où les besoins en matière de sécurité pour les intérêts nationaux sont tels que des industries de souveraineté, par ailleurs excellentes à l'export dans le domaine de la cybersécurité et de la cyberdéfense, se sont développées, telles Airbus-Defence and Space, Thales, Atos ou encore Sogeti pour les plus importantes. Sur le segment « confiance et sécurité », il faut se féliciter que la proximité naturelle avec l'État soit forte. À l'image naguère du secteur nucléaire et de certaines industries duales, le numérique – dans sa dimension sécurité et défense – doit s'inscrire désormais dans une perspective technologique et économique de co-production. Dans la mesure où il s'agit d'un secteur stratégique pour l'État, pour la protection des entreprises et celle des citoyens, ce secteur nécessite de très forts investissements en recherche fondamentale, en études amont et en R&D. Pour ce faire, il doit mobiliser des fonds publics et privés importants. Or, la ressource des pôles de compétitivité apparaît sous-utilisée et la recherche publique fondamentale dans ce domaine, pas assez financée. Le risque de décrochage par rapports aux autres puissances cybernétiques et économiques n'est pas exagéré.

48 RECOMMANDATIONS EN FAVEUR D'UNE POLITIQUE PUBLIQUE

Pris dans son ensemble, le renseignement est en situation de balkanisation, les normes juridiques qui s'appliquent à lui sont dispersées, parfois imprécises, voire contradictoires, et le pilotage budgétaire au sens de la LOLF et incluant l'ensemble des acteurs du renseignement public au-delà des « services spécialisés » n'existe pas réellement : dès lors si la « connaissance et l'anticipation » relèvent effectivement d'une fonction stratégique, on ne peut considérer le renseignement comme constituant une authentique politique publique. Des évolutions raisonnées, évoquées parmi les recommandations, pourraient transformer ce constat. Les « services » sont indispensables pour la sécurité des citoyens : il faut les renforcer, mais aussi les contrôler. Leurs modes d'action sont singuliers : il faut les préserver, dans le cadre de la loi votée par le Parlement. Le secret est indispensable pour l'État : face aux désirs de transparence, il faut le garantir, mais aussi le réguler. Les dépenses publiques en matière de renseignement constituent pour la sécurité des citoyens un investissement. C'est pour cette raison que l'effort financier en la

matière doit être maintenu dans les années à venir, en dépit d'un contexte qui va affecter très fortement l'ensemble des dépenses publiques.

Ces évolutions souhaitables sont l'objet de 48 recommandations organisées en six lignes directrices :

1 - Atténuer la loi d'airain du fonctionnement de la « communauté du renseignement »

2 - Rationaliser pour gagner en efficacité et en reconnaissance publique

3 - Clarifier et moderniser les règles de droit dont les services relèvent

4 - Clarifier les règles et les pratiques dans la « cinquième dimension » au service de la souveraineté

5 - Conduire une réflexion de nature stratégique et prospective sur les activités de renseignement

6 - Engager la réforme culturelle du renseignement

INTRODUCTION

UNE NOUVELLE FONCTION STRATÉGIQUE FAIT-ELLE UNE POLITIQUE PUBLIQUE ?

Le *Livre blanc* sur la sécurité nationale de 2008 a transformé le « renseignement », pratique séculaire demeurant actuelle, exercée quotidiennement par une grande variété d'acteurs publics, en une nouvelle – et cinquième – fonction stratégique sous la dénomination de « connaissance et anticipation »[1]. Ce document et la loi de programmation militaire (LPM) 2009-2014 qui l'a suivi ont en outre souligné le caractère prioritaire de la nouvelle fonction. En vue d'accompagner la reconnaissance publique de cette évolution, la fonction « connaissance et anticipation » a fait l'objet d'une médiatisation sans précédent. La LPM de 2009, puis après l'alternance de 2012 le *Livre blanc* de 2013 et enfin la LPM 2014-2019 ont confirmé cette orientation nouvelle. L'ensemble de ces textes concernait cependant seulement les trois organes de renseignement du ministère de la Défense (DGSE, DRM, DPSD)[2] et non pas les services à la disposition de l'Intérieur (DCRI) et du Budget (DNRED, TRACFIN). Le « renseignement » devenu « connaissance et anticipation » en 2008, renvoyait donc au renseignement indispensable aux armées et au renseignement extérieur utile à l'information du gouvernement – que l'on appellera ici le « enseignement stratégique ». Le renseignement intérieur, de nature très divers, collecté par les services de police et notamment par la DCRI[3] n'a pas été pris en compte en tant quel, avec ses nombreuses spécificités dans la perspective nouvelle. Quoi qu'il en soit les **années 2008-2013** ont *de facto* installé officiellement et publiquement le renseignement, au service de la sécurité intérieure et extérieure, **comme une préoccupation du plus haut niveau politique :** l'objet de ce rapport est de savoir **si cela en fait ou non une politique publique.**

Première du genre pour un *think tank* cette étude plonge au cœur d'un **« domaine très réservé »** et entend réaliser un état des lieux global du renseignement en passant en revue quatre ensembles : son périmètre budgétaire, l'articulation politico-administrative des « services », leurs moyens techniques et juridiques ainsi que les conséquences directes sur les libertés publiques, enfin la perception du « renseignement » dans la société.

[1] Les quatre autres sont : la protection, la prévention, la dissuasion et l'intervention.
[2] *Cf.* la liste des sigles et acronymes page 67.
[3] Information générale, contre-espionnage, contre-ingérence et contre-terrorisme.

DES CARACTÉRISTIQUES ATYPIQUES : ABSENCE DE PUBLICITÉ, ABSENCE D'ÉVALUATION, CONTRÔLE EXTERNE SYMBOLIQUE

Ce domaine très singulier de l'action de l'État n'est naturellement pas soumis aux usages habituels de publicité et de contrôle par la représentation nationale. L'efficacité même de la collecte de l'information « fermée » et celle de son utilisation exigent une discrétion relative ou absolue. En outre, et ce pour les mêmes raisons, le cadre juridique des moyens mis à la disposition des services de renseignement est-il particulier, échappant souvent au domaine de la loi et au droit commun, voire échappant à toute forme de cadre juridique. Classiquement, l'espionnage est défini comme un « crime sans cadavre ». Dans le même esprit, on peut considérer que l'ensemble des atteintes et infractions que les services de renseignement doivent déceler, prévenir, voire réprimer, constituent des délits ou des crimes sans dommage mesurable et même parfois sans dommage apparent. Dans ces circonstances, la recherche d'une mesure d'impact est difficile, sinon impossible et les stratégies de communication des « services » sont ramenées à l'emploi d'arguments par défaut, comme le nombre d'attaques déjouées ou la mention de dangers écartés, autant d'éléments rassurants mais qu'il est naturellement impossible de confirmer. La seule exception concerne la libération des citoyens français pris en otage qui est tangible et en général fortement et efficacement valorisée médiatiquement. La fonction « connaissance et anticipation » ne peut donc être évaluée et son action est faiblement contrôlée par la représentation nationale. Il faut donc plutôt parler à ce stade d'une quasi-politique publique, entre les mains du seul pouvoir exécutif, sans contrôle externe.

LE « DOUBLE RETARD » DE LA PROTECTION DES LIBERTÉS À L'HEURE DU RECOURS CROISSANT AUX TECHNOLOGIES

L'équilibre entre l'exercice pratique de la sécurité, dont le renseignement est une composante reconnue désormais comme majeure, et les garanties apportées aux libertés est l'un des lieux de tension classique dans un régime démocratique et libéral. Or, tant du point de vue de la mise en œuvre que de la réflexion, la sécurité a toujours primé sur la liberté. La relation sécurité-libertés est une dialectique permanente, caractérisée par un déséquilibre au détriment des libertés qui s'est

accentué dans les pays occidentaux après les attentats aux États-Unis de 2001. La France n'a pas échappé à la règle avec les lois sur le terrorisme de 2001, 2004 et 2006.

Notre idée est que la démocratie française – c'est un devoir d'honnêteté de ne pas le masquer à l'orée de cette étude – l'une des plus anciennes au monde, doit assurer sa solidité et sa pérennité en s'adaptant à cette tension avec le souci permanent d'un examen attentif de l'état réel des libertés. Même si l'effet de la conjoncture post-2001 a été net, se pose clairement la question du retard libéral en France, que ce soit du point de vue de son système judiciaire[4] dont les caractéristiques amènent des condamnations régulières de la France par la Cour européenne des droits de l'homme ou encore du fonctionnement de son système parlementaire, domestiqué selon la volonté des constituants en 1958, malgré les promesses récurrentes de réhabilitation du rôle du Parlement. En ce qui concerne le système judiciaire, le chiffre des condamnations de la France devant la CEDH est éloquent : entre 1959 et 2010, la France a été condamnée à plus de 50 reprises pour violation du droit à la liberté et à la sûreté (art. 5 de la Convention européenne)[5]. La part croissante prise par les outils technologiques pensés comme préventifs (vidéosurveillance, interceptions de données, etc.) dans l'accomplissement de la mission de sécurité accroît le déséquilibre sécurité-libertés. La **France,** comme d'autres pays, connaît ainsi un « double retard », celui de **la protection des libertés par rapport à l'exercice de la sécurité** et celui de la **protection des libertés par rapport aux mutations technologiques permanentes.**

[4] On mentionnera, par exemple le recours à la détention provisoire, la législation antiterroriste, la durée de la procédure, le statut du parquet ou encore le régime de la garde à vue (*cf.* à ce propos Kami Haeri, « *Vous avez le droit de garder le silence… » Comment réformer la garde à vue,* Paris, Institut Montaigne, décembre 2010, 64 p.)

[5] Soit 7 % de l'ensemble des condamnations de la France.

CHAPITRE I

UN RENSEIGNEMENT EN FORME D'ARCHIPEL

1.1. AUX ORIGINES DE LA CONVERSION FRANÇAISE AU RENSEIGNEMENT

Dans le *Livre blanc* sur la défense de 1994, premier bilan postérieur à la fin de la guerre froide qui prenait acte du changement stratégique profond intervenu, le renseignement occupait une place encore bien mineure. En cela, il reflétait une position classique dans la conception que les armées se sont toujours faites de ce qui était un outil subordonné à l'usage de la force. Si la puissance publique dans son ensemble accordait également une importance mineure au renseignement, le gouvernement prêtait cependant plus d'attention au renseignement politique intérieur, conçu de longue date comme un outil de gouvernement. Afin de pouvoir mieux comprendre l'évolution qui a fait d'un outil une « fonction stratégique » en seulement quelques années, il est nécessaire d'éclairer le contexte de court et moyen termes.

La réalité internationale a considérablement changé : la fin de la guerre froide est un des principaux facteurs de valorisation d'un renseignement qui est censé apporter un éclairage sur l'avenir, une évaluation des menaces, voire nourrir des *scenarii* de crise dans un contexte d'incertitudes croissantes et de « nouvelles menaces », selon l'expression désormais popularisée et qui débouche sur la volonté de mettre en place une « sécurité globale ». La France est également entrée à la même époque, au milieu des années 1990, dans la société de l'information avec un effet immédiat : la croissance du « monde numérique » est à l'origine d'un phénomène de saturation rendant la perception du présent fragile et l'appréhension de l'avenir plus complexe.

Il est enfin une dimension importante, propre au contexte politique français : celui-ci a en effet été marqué par la montée en puissance de la thématique du « renouveau du service public » dans les années 1990 jusqu'à la LOLF votée en 2001, en passant par la « réforme de l'État ». Ceci illustre la porosité de la technostructure aux thématiques du *New Public Management* qui entend réduire le coût et le périmètre de l'État, tout en améliorant son efficacité et en promouvant la capacité d'évaluation de sa performance. Cette dimension a eu un fort impact sur la réforme du renseignement mise en œuvre à la fin des années 2000.

1.2. 2007-2009 : UNE RÉFORME ÉLYSÉENNE D'ENVERGURE, MAIS DÉSÉQUILIBRÉE

Cette réforme du renseignement a débuté avec la création d'un organisme parlementaire de contrôle à l'été 2007[6]. L'une des dernières structures de « contrôle » à être créée au sein de l'Union européenne – la « délégation parlementaire au renseignement » (DPR) – avait une ambition modeste, chargée selon la loi n° 2007-1443 du 9 octobre 2007 de « suivre l'activité générale et les moyens » des services. Ainsi que l'attestent les très brefs rapports d'activité de la DPR[7], celle-ci n'a pas cherché à élargir son périmètre, réduisant la réalité du « contrôle » dont le terme même était d'ailleurs absent de la dénomination et du texte. Il n'en reste pas moins que cette structure, créée à l'initiative du gouvernement, a constitué en son temps une rupture vis-à-vis du domaine « très réservé » de l'exécutif caractérisant depuis toujours le renseignement[8].

La réforme 2007-2009, menée très largement, sinon exclusivement par l'Élysée, présente quatre principales caractéristiques. L'esprit général est inscrit dans le *Livre blanc* de 2008 qui a précédé et accompagné la plupart des composantes de la réforme.

- Un point important est la réforme de gouvernance, caractérisée par le renforcement de la présidentialisation du renseignement. Ceci s'est traduit sur le plan des structures avec la création auprès du Président de la République d'un « coordonnateur du renseignement » (*de facto* en juillet 2008, puis *de jure* par le décret n° 2009-1657 du 24 décembre 2009) et d'un « Conseil national du renseignement » (*de facto* en octobre 2008, puis *de jure* par le décret précédemment cité) qui est une formation spécialisée et restreinte du Conseil de défense et de sécurité nationale. Cette partie de la réforme a levé une ambiguïté : jusqu'en 2008, c'était au Premier ministre qu'incombait la charge de la coordination en matière du renseignement depuis l'ordonnance sur la défense de 1959[9], mais le rôle effectif était assuré par l'Élysée, fonction partagée entre le cabinet du Président, l'état-major particulier et le secrétariat général de l'Élysée, selon les époques. La fin de

[6] On suivra avec commodité les cinq années et demi de réforme en se reportant à la frise figurant en p. 23.

[7] *Cf.* les références précises en fin de volume.

[8] *Cf.* sur ce point : S. Laurent, « Chaban à trois temps (1943-1944, 1957-1958, 1969-1972) : le renseignement dans la politique », dans : Bernard Lachaise, Gilles Le Béguec et Jean-François Sirinelli (dir.), *Jacques Chaban-Delmas en politique,* Paris, Presses universitaires de France, 2007, p. 163-176.

[9] Le dispositif de 1959 avait été réformé et modernisé en profondeur en 1989 sous l'impulsion d'un conseiller du Premier ministre, le préfet Rémy Pautrat, ancien directeur de la DST.

cette anomalie politico-administrative a signifié également que l'Élysée entendait établir définitivement son rôle en matière d'orientation et d'exploitation du renseignement : ainsi, si le renseignement relève nominalement d'une politique gouvernementale assurée par le fait que les six agences dépendent directement de trois ministres et que le Premier ministre, selon l'article 21 de la Constitution, conduit la politique du gouvernement, la nouvelle fonction stratégique devenait dès lors dans les faits d'abord une politique présidentielle. Mettre fin à l'anomalie a été aussi un acte politique, une façon de faire coïncider la lettre avec l'esprit présidentialiste de la Constitution de 1958.

- Naturellement absent du *Livre blanc* 2008 consacré à la défense, le renseignement intérieur a été pourtant également profondément réorganisé par la création au 1er juillet 2008 de la Direction centrale du renseignement intérieur (DCRI), organisme succédant à la DST et dépendant de la Direction générale de la police nationale (DGPN) du ministère de l'Intérieur. La DCRI, chargée de la défense des « intérêts fondamentaux de la nation » au sens du code pénal, était le résultat de la fusion de la DST et d'une partie des renseignements généraux (DCRG) afin de créer une direction spécialisée sur le contre-terrorisme, le contre-espionnage et la contre-ingérence. L'autre partie des effectifs de la DCRG demeurait dans les départements afin de poursuivre la collecte du renseignement intérieur dans le cadre de la sous-direction de l'information générale (SDIG), rattachée désormais à la sécurité publique. Le rattachement de la gendarmerie, force militaro-civile de renseignement territorial, au ministère de l'Intérieur au 1er janvier 2009, a été une composante, plus discrète mais bien réelle, de la réforme du renseignement, en raison de l'ancienneté et l'ampleur de son maillage, dans un esprit de rationalisation des forces de l'ordre et de renseignement.

- La réforme a été complétée par la loi de programmation militaire du 29 juillet 2009, traduisant matériellement la promotion du renseignement en garantissant des moyens conséquents aux services du ministère de la Défense, notamment par la création de 700 emplois pour les trois services, ce qui représentait à l'époque une croissance de 10 %, ainsi que l'engagement d'investissements lourds en matière technique.

- L'année 2010 a vu l'accomplissement de la réforme des statuts des personnels et de la formation. L'Académie du renseignement, rattachée au Premier ministre, a ouvert en septembre 2010 afin d'assurer la formation initiale et continue des cadres supérieurs des services. Par ailleurs, le décret du 30 décembre 2010 a

profondément transformé le statut des personnels de la DGSE avec une double perspective : aligner le statut des fonctionnaires de catégorie A du service extérieur (les « délégués ») sur celui des attachés de la fonction publique d'État afin, notamment, de favoriser les mobilités entre les différentes administrations et d'autre part offrir des débouchés à la DGSE à la sortie de l'ENA.

Il faut cependant relever les disparités de la réforme, sources de déséquilibres structurels qui n'ont pas été entièrement corrigés depuis. Le renseignement extérieur a été conforté dans la diversité de ses moyens, dans son fonctionnement et dans ses moyens budgétaires. Or, sur le plan de ces moyens, la LPM 2009 a exclusivement concerné les trois agences relevant du ministère de la Défense et la LOPPSI de 2011 n'a pas apporté à la DCRI et à la SDIG les mêmes engagements budgétaires et d'emplois que la LPM. Effet de la réforme de l'État, les moyens budgétaires de la jeune DCRI ont même légèrement décru jusqu'aux effets attendus des annonces faites en 2013 *(cf. infra)*. Il y a eu donc d'emblée un très fort déséquilibre entre DGSE, DRM et DPSD d'une part et DCRI, DNRED, TRACFIN de l'autre. La nouvelle DCRI qui représente à elle seule un tiers des effectifs des six agences a été de fait le parent pauvre de la réforme globale. Par ailleurs, la réforme n'a pas concerné le statut juridique des six services et l'encadrement juridique de leurs pratiques, se contentant de renforcer leurs protections juridiques (renforcement de la protection de l'anonymat des agents, principe des lieux classifiés). La question de l'impact des pratiques des services sur les libertés publiques a été totalement absente de la réflexion. Enfin, la valorisation auprès du public de la fonction du renseignement, la réflexion sur les savoirs professionnels utiles aux analystes, sur les parcours de la formation initiale assurés *de facto* par l'enseignement supérieur public, en un mot tout ce qui touche à la dimension culturelle du renseignement n'a pas été envisagé un seul instant. La **réforme** a été exclusivement **politique, se traduisant** principalement **sur un plan organisationnel et budgétaire.**

1.3. LE RÔLE NOUVEAU ET BÉNÉFIQUE DU PARLEMENT : LA POURSUITE DE LA RÉFORME APRÈS 2012

Après l'alternance politique de 2012, d'autres modifications ont été introduites, moins mises en avant politiquement mais sans remise en cause de la forte valorisation du renseignement. Dans cette nouvelle configuration politique, il faut

relever toutefois que la nouvelle majorité a pu s'appuyer sur une abondante et sérieuse expertise politique publiée en 2011 et 2012, alors qu'elle était dans l'opposition[10]. Ceci explique en grande partie que la poursuite de la réforme soit d'initiative parlementaire. L'action du président de la commission des lois Jean-Jacques Urvoas, rendue publique au travers de deux rapports au printemps 2013, a été déterminante. Le travail de ce dernier a rendu légitime pour la première fois la parole parlementaire sur ce domaine très réservé, après des décennies d'auto-censure de la part des élus[11]. L'une des mesures les plus fortes proposée par le rapport Urvoas de mai 2013 était de mettre en place un contrôle parlementaire de légalité et de proportionnalité. Le rapport proposait d'accorder des outils juridiques exorbitants du droit commun aux services de renseignement, mais en les soumettant a une commission unique de contrôle, la Commission de contrôle des activités de renseignement (CCAR).

Si la totalité des préconisations Urvoas n'a pas été à ce jour retenue, il faut souligner plusieurs points importants de la réforme post-2012 :

- la création – annoncée par l'Élysée – le 10 juin 2013 d'une inspection spécialisée pour les organes de renseignement au sein des corps d'inspection de l'administration, des armées et de la police ;

- annoncée quelques jours après par le ministre de l'Intérieur, le projet d'émancipation de la DCRI par rapport à la tutelle de la DGPN pour former, sous la responsabilité directe du ministre, une direction générale de la sécurité intérieure (DGSI). Il faut relever qu'il s'agissait d'une revendication précoce de la jeune DCRI. Le ministre de l'Intérieur avait annoncé à cette occasion que la DCRI recruterait plus de 430 personnels supplémentaires dans les années à venir. La DGSI a vu le jour avec les décrets des 2 et 7 mai 2014 et le recrutement de 430 personnels, en majorité non policiers sur les cinq ans à venir, a été annoncé.

La LPM 2014, votée en décembre 2013 a complété certaines dispositions esquissées lors de la précédente loi de programmation et a ajouté d'autres éléments nouveaux préconisés dans le rapport Urvoas. Ainsi la LPM 2014 a-t-elle repris une recommandation de ce rapport, en élargissant le champ d'activité de la DPR afin de modifier ses compétences : désormais selon l'article 12 de la loi, la

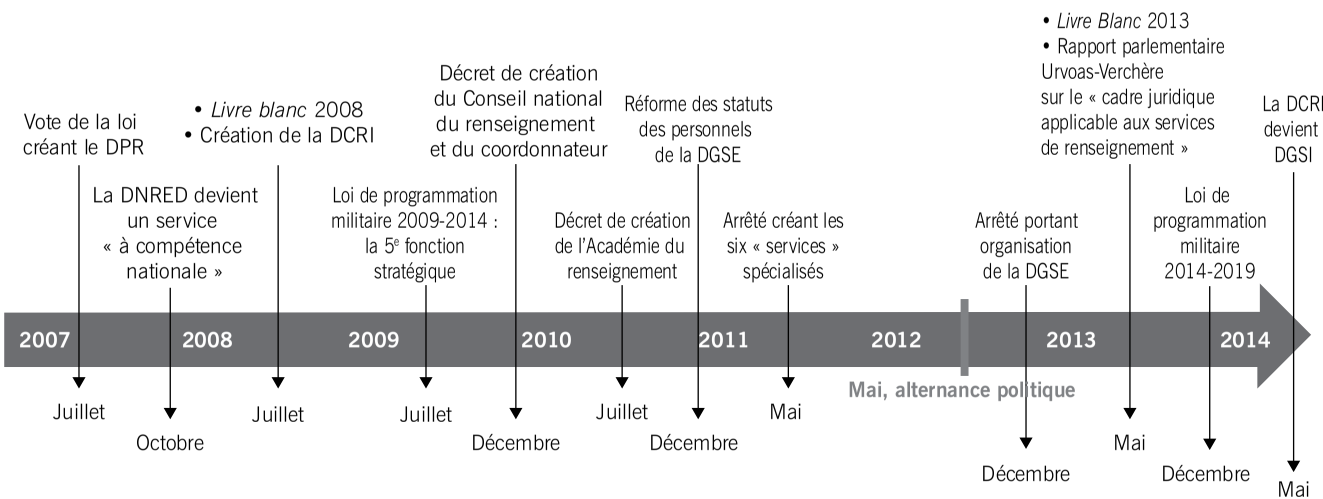
[10] *Cf.* les diverses publications du député Jean-Jacques Urvoas et de Floran Vadillo, citées en fin de publication.

[11] *Cf.* notre étude : « Les parlementaires face à l'État secret et au renseignement sous les IVe et Ve République : de l'ignorance à la politisation », *Les Cahiers de la sécurité,* n° 13, juillet-septembre 2010, p. 134-144.

Délégation « exerce le contrôle parlementaire de l'action du Gouvernement en matière de renseignement » et peut, pour ce faire, obtenir notamment communication de documents élaborés par le CNR. L'article 12 marque une évolution d'importance : le « suivi » inscrit dans la loi de 2007 est abandonné au profit d'un « contrôle » qui renvoie ainsi explicitement à l'action habituelle de contrôle parlementaire des administrations classiques. En outre, la commission de vérification des fonds spéciaux est absorbée par la DPR (article 13). L'inflexion est très nette : il reste cependant à voir ce que feront les parlementaires de la DPR et s'ils sauront utiliser les nouvelles prérogatives dont ils disposent, qui supposent des compétences spécifiques sur des sujets techniques, l'abandon d'un réflexe ancien d'auto-censure et un certain courage dans la capacité à exercer le nouveau « contrôle ».

L'autre principale disposition de la nouvelle loi de programmation militaire en matière de renseignement est l'article 20, dont le principe a été vivement contesté par un certain nombre de parlementaires et dans la blogosphère : les six services de renseignement peuvent désormais accéder aux « données techniques de connexion » des internautes, en dehors du cadre de la lutte antiterroriste, ce qui était une disposition introduite en 2006. Désormais l'obtention de ces données peut être exigée des opérateurs de communications électroniques dans le cadre, plus large, des cinq motifs introduits par la loi de 1991, dont celui de « renseignements intéressant la sécurité nationale ». L'esprit de la LPM 2014 demeure dans le droit fil de celle de la LPM 2009 pour ce qui est du renseignement : les services du ministère de la Défense sont préservés budgétairement, leurs outils techniques de collecte renforcés, leurs moyens d'actions juridiques garantis, sans que les effets sur les libertés publiques aient été pleinement pris en compte. Le **« double retard »** évoqué plus haut persiste et peut-être même **s'accroît.**

Les réformes de structure de renseignement de 2007 à 2014



1.4. UN « AGRÉGAT INCONSTITUÉ DE PEUPLES DÉSUNIS » TIENT LIEU DE « COMMUNAUTÉ DU RENSEIGNEMENT »

Le terme de « communauté du renseignement » est aujourd'hui couramment employé par les directeurs des services[12] et par les pouvoirs publics[13]. Cet anglicisme postule une cohérence et une homogénéité entre les six organes de renseignement qui sont loin d'être des réalités. L'expression employée dans le titre ci-dessus, utilisée par Mirabeau pour qualifier la France à l'aube de la Révolution, convient parfaitement pour décrire la mosaïque que forment aujourd'hui ces six agences très hétérogènes, apparues par sédimentation sur plus d'un demi-siècle, sans que jamais le souci de simplification bureaucratique et l'esprit de subsidiarité aient été pris en considération. Il paraît ainsi plus juste de parler d'acteurs du renseignement que d'une « communauté » qui est imaginée sinon imaginaire. Éloignés de toute perspective de rationalisation de leur organisation générale, les « services » dépendent de trois ministères régaliens qui sont souvent eux-mêmes en conflit structurel sur d'autres enjeux. On trouve ainsi :

- au sein du ministère de la Défense : la Direction générale de la sécurité extérieure (créée sous le nom de SDECE en 1945, devenu DGSE en 1982), la Direction de la protection et de la sécurité de la défense (créé sous le nom de Sécurité militaire en 1961, devenue DPSD en 1981), la Direction du renseignement militaire-DRM (créée *ex nihilo* en 1992) ;

- au sein du ministère de l'Intérieur : la Direction centrale du renseignement intérieur (créée sous le nom de DST en 1944, devenue DCRI en 2008) ;

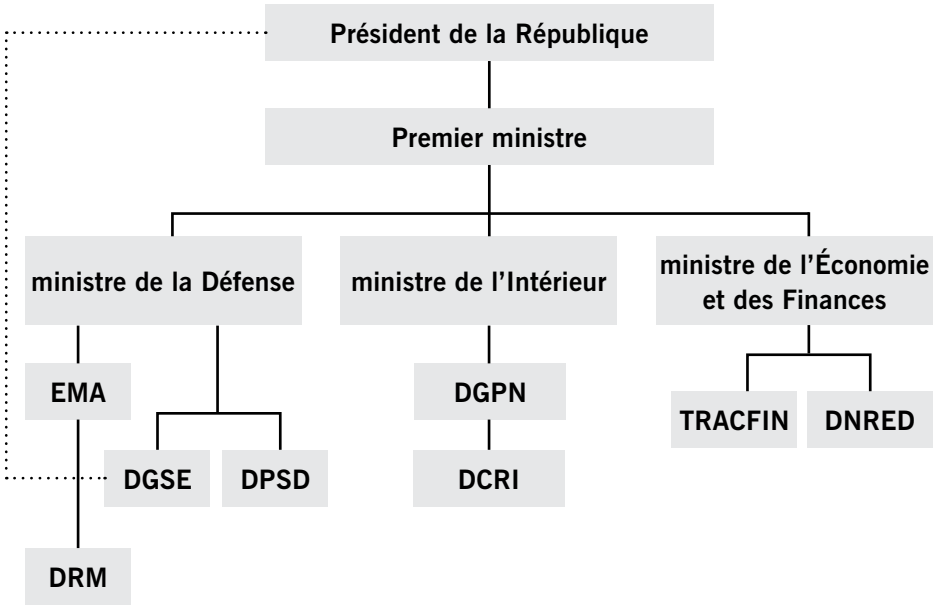
- au sein du ministère de l'Economie et des Finances : la Direction nationale du renseignement et des enquêtes douanières (créé sous le nom de SRFD en 1938, devenu DNRED en 1988) et la cellule de Traitement du renseignement et action contre les circuits financiers clandestins-TRACFIN (créée *ex nihilo* en 1990).

---

[12] *Cf.* notamment : François Mermet, « Quelques réflexions sur la fonction renseignement », *ENA mensuel,* n° 236, novembre 1993. p. 12 ; Pierre Brochand, « Les activités et les défis du service », dans : « Le renseignement », *L'ENA hors les murs,* octobre 2006, n° 365, p. 6 ; Erard Corbin de Mangoux, « Les nouveaux défis du renseignement extérieur », *Les Cahiers de Mars,* n° 198, décembre 2008, p. 24 ; Bernard Squarcini, « Les mutations du renseignement intérieur français », *Questions internationales,* n° 35, janvier-février 2009, p. 46.

[13] *Cf.* l'article 1er du décret n° 2009-1657 du 24 décembre 2009 relatif au Conseil de défense et de sécurité nationale et au Secrétariat général de la défense et de la sécurité nationale.

Vue générale des acteurs du renseignement avant mai 2014



Effet induit de la réforme commencée en 2007, l'arrêté du Premier ministre du 9 mai 2011 a introduit la qualification de « services spécialisés » délivrant ainsi un label précieux, porteur de prérogatives administratives et juridiques particulières pour ces six services de renseignement – la DGSE, la DRM, la DPSD, la DCRI, la DNRED et Tracfin – qui forment *de facto* le « premier cercle », au plus près de l'exécutif. Ceci n'a en rien gommé la diversité entre les services, y compris en leur sein même. Le statut particulier de la DCRI l'illustre. Si elle est presque exclusivement composée de fonctionnaires de police, les autres organes comptent en interne fonctionnaires et agents contractuels, civils et militaires, avec des statuts, des obligations et des capacités d'action différentes. Une d'entre elles seulement – la DCRI – compte des personnels ayant un statut d'officier ou d'agent de police judiciaire. Elle a donc des moyens d'enquête et d'action singuliers sur le territoire français, et supérieurs en l'espèce par rapport aux cinq autres agences, malgré les effets du décret de 2011 attribuant des moyens particuliers d'actions aux six « services spécialisés ». La situation des douaniers de la DNRED est assez proche. Ces différences sont sources de tensions structurelles entre les services, mais sont surtout préjudiciables

à l'efficacité globale du renseignement public. En outre, on constate que l'action des services de police et de gendarmerie dans un contexte judiciaire est beaucoup plus claire et précise, notamment pour ce qui est des pratiques d'enquête, que dans le contexte administratif. Dans ce dernier cadre les fonctionnaires et agents, ainsi que les « sources » sont faiblement (voire pas) protégés et leurs actions non légales les exposent à des poursuites sur le territoire français. De même, cette situation expose ceux qui sont l'objet de leurs enquêtes à des intrusions et/ou des entraves – par définition non légales – à l'exercice de leurs libertés fondamentales, et comme telles, peut ouvrir droit à des poursuites judiciaires.

Le caractère hétérogène des corps socio-professionnels et des moyens administratifs ou juridiques des organes appartenant à la communauté est encore renforcé par la diversité de leurs ressorts géographiques. D'après les textes réglementaires créant les six « services spécialisés », ceux-ci sont nettement délimités entre le territoire national et le domaine étranger :

Les ressorts territoriaux – théoriques – de compétence des six services

	Intérieur	Extérieur
Min. Def.		
• DGSE		
• DRM		
• DPSD		
Min. Intérieur		
• DCRI		
Min. Eco. Fi.		
• DNRED		
• TRACFIN		

Dans les faits, les ressorts d'action des six services sont bien différents en raison d'une part du caractère transfrontalier de nombreuses infractions ou atteintes à la sécurité, mais aussi parce que le travail de renseignement, y compris pour la simple collecte d'information, suppose très souvent de dépasser le cadre frontalier. Dès lors, les textes réglementaires apparaissent bien théoriques par rapport aux

ressorts réels. La réalité des pratiques des organes de renseignement engendre ainsi des chevauchements entre services, aussi bien à l'intérieur qu'à l'extérieur du territoire, voire parfois des tensions sur des enjeux de sécurité importants. La communauté n'est pas seulement hétérogène dans sa composition, elle touche parfois à l'irrationalité dans la délimitation géographique de ses missions.

Les ressorts territoriaux – réels – d'action des six services

	Intérieur	Extérieur
Min. Def.		
• DGSE		
• DRM		
• DPSD		
Min. Intérieur		
• DCRI		
Min. Eco. Fi.		
• DNRED		
• TRACFIN		

1.5. A LA RECHERCHE BUDGÉTAIRE DU « RENSEIGNEMENT » DANS LA LOLF

En ce qui concerne les organes de renseignement, la nouvelle organisation budgétaire de la LOLF (2001/2006) a rendu plus complexe la nomenclature budgétaire mise en place par l'ordonnance de 1959. En effet depuis 2006, la fonction renseignement mise en œuvre par les six services relève *a minima* de trois « missions », cinq « programmes » et… six « actions ». Ainsi l'éclatement empêche t-il des financements entre plusieurs missions **empêche de considérer,** du seul point de vue budgétaire, le renseignement **comme une politique publique,** au sens de l'article 7 de la loi organique. Ce faisant, la **LOLF ne permet pas d'évaluer avec précision l'effort budgétaire national en faveur du renseignement** et en pratique affaiblit la possibilité d'un contrôle effectif par la représentation nationale.

Le découpage du renseignement dans la LOLF

	« Mission » au sens de la LOLF	« Programme » au sens de la LOLF	« Action » au sens de la LOLF	« Services spécialisés » concernés
Min. Défense	« défense »	« environnement et prospective de la politique de défense (144)	« recherche et exploitation du renseignement intéressant la sécurité de la France » (3)	DGSE DPSD
		« préparation et emploi des forces » (178)	« planification des moyens et conduite des opérations » (1)	DRM
Min. Intérieur	« sécurité »	« police nationale » (176)	« ordre public et protection de la souveraineté » (1)	DCRI
Min. Économie et finances	« gestion des finances publiques et des ressources humaines »	« facilitation et sécurisation des échanges » (302)	« surveillance douanière des flux de personnes et de marchandises et lutte contre la grande fraude douanière » (1)	DNRED
		« conduite et pilotage des politiques économique et financière » (218)	« état-major, médiation et politiques transversales » (1) + « support et soutien » (5)	TRACFIN
Premier Ministre	« direction de l'action du gouvernement »	« coordination du travail gouvernemental » (129)		« fonds spéciaux » (fonds spéciaux DGSE et GIC)

Source : http://www.performance-publique.budget.gouv.fr/fileadmin/medias/documents/ressources/PLF2013/liste_mpoi_plf2013.pdf. ; www.performance-publique.budget.gouv.fr/.../PAP2010_BG_Securite.publique et Observatoire de la Défense-Orion, Le renseignement en France : quelles perspectives ?*, Paris, Fondation Jean Jaurès, 2012, p.* 69.

Il faut néanmoins s'interroger : que pèse le renseignement et quel est son coût pour le budget de l'État ? Ces questions sont essentielles mais il est difficile d'y répondre, précisément en raison du puzzle budgétaire et de la discrétion évidente des services. En l'état des documents budgétaires, seuls ceux du ministère de la Défense peuvent être exploités avec plus de précision, ainsi que le tableau ci-dessous le montre. D'un point de vue global, le budget des trois services est passé, en crédits de paiements et fonds secrets inclus, de 701,7 M€ en 2006 à 876,4 M€ en 2012, soit une augmentation de près de 20 % dans un contexte de crise économique. **Le renseignement militaire et le renseignement stratégique ont été non seulement préservés, mais ont vu leurs moyens croître considérablement,** notamment après la LPM 2009. Pour ce qui est de la ventilation interne des crédits, on remarquera que pour la DGSE et la DPSD (programme 144), les dépenses d'investissement représentent sur les dernières années une part non négligeable, de l'ordre d'un quart.

Par ailleurs, les courbes du graphique traduisent bien la hiérarchie entre les trois services : le budget de la DPSD est très modeste (pour des effectifs de 1 400 personnels en 2007[14] et qui n'ont cessé de décroître dans une forte proportion), celui de la DRM qui utilise pourtant des capteurs techniques théoriquement coûteux l'est également (pour des effectifs de 1600 personnels en 2012[15]) et celui de la DGSE (pour des effectifs atteignant presque 5 000 personnes en 2012[16]) est beaucoup plus important, trois fois supérieur à celui de la DRM. On relèvera par ailleurs que sur les 12 000 personnels que comptaient les six services selon le *Livre blanc* 2008[17], les trois relevant du ministère de la Défense représentaient plus de 60 % des effectifs.

[14] Bernard Carayon, Rapport n° 83. *Création d'une délégation parlementaire au renseignement,* Paris, Documents législatifs, 2007, p. 10.

[15] Jean-Jacques Urvoas et Patrice Verchère, *Pour un « État secret » au service de notre démocratie. Rapport d'information,* Assemblée nationale, no 1022, 2013, p. 176.

[16] *Ibid.,* p. 182.

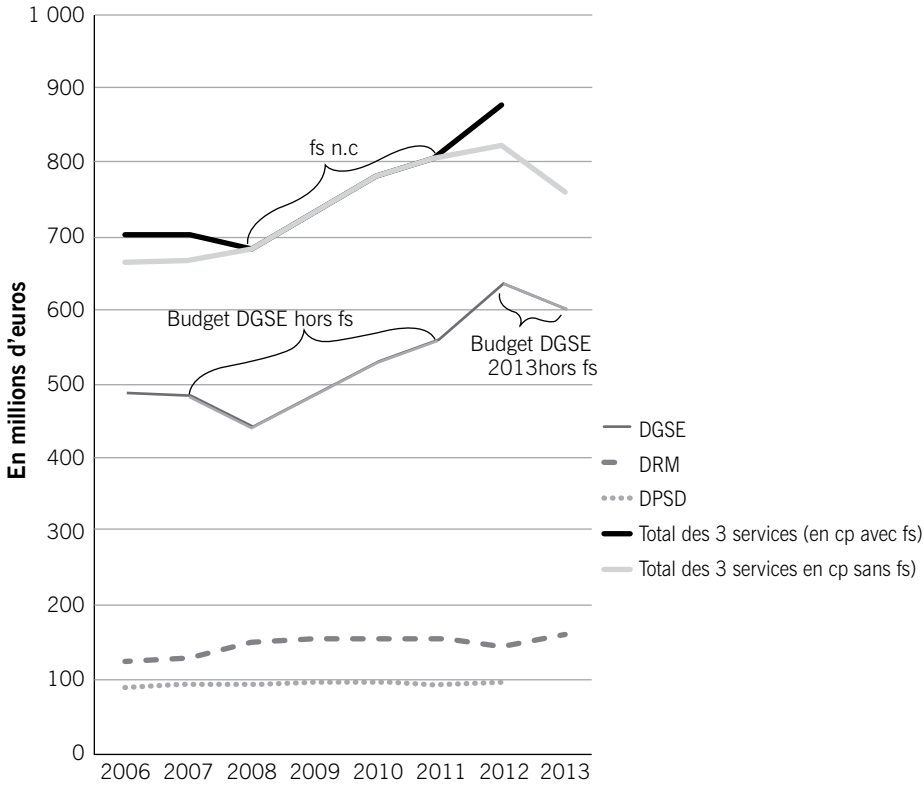
[17] Défense et sécurité nationale. *Livre blanc,* Paris, Odile Jacob-La documentation française, 2008, p. 139.

Budgets des « services » du ministère de la Défense

	2006			2007			2008			2009			2010			2011			2012			2013		
	ae	cp	fs	ae	cp	fs	ae	cp	fs	ae	cp	fs	ae	cp	fs	ae	cp	fs	ae	cp	fs	ae	cp	fs
DGSE	450	449	36,2	429,3	445,4	36,2	425,5	440,1	nc	543,5	480,4	nc	476,5	527,4	nc	543	559	nc	593	578	53,9	644,5	600	nc
Total DGSE (en cp avec fs)			485,2			481,6			440,1			480,4			527,4			559			631,9			600
DRM	129,3	126,6		127,8	129,7		131,5	149,3		156,8	155,4		154,3	156,2		156,4	156,4		147,2	147,2		161,4	161,4	
Total (en cp ss fs)			126,6			129,7			149,3			155,4			156,2			156,4			147,2			161,4
DGSE + DRM			611,8			611,3			589,4			635,8			683,6			715,4			779,1			761,4
DPSD	92,1	89,9		92,5	93,2		93,9	93,8		96,4	96,4		96,6	96,6		93,1	93,1		nc	97,3		nc	nc	
Total DPSD (en cp ss fs)			89,9			93,2			93,8			96,4			96,6			93,1			97,3			nc
Total des 3 services (en cp avec fs)			701,7			704,5			683,2			732,2			780,2			808,5			876,4			nc
Total des 3 services (en cp sans fs)		665,5			668,3			683,2			732,2			780,2			808,5			822,5			761,4	

cp : crédits de paiement
fs : fonds secrets
n.c : non connu
Source : www.performance-publique.budget.gouv.fr

Budgets des « services » du ministère de la Défense



Par ailleurs, la LOLF ne permet pas, pour les différentes « actions » des « programmes », de retrouver le budget de la DCRI, de la DNRED et de TRACFIN. Il est donc possible d'avoir seulement un ordre de grandeur très approximatif du budget des six services que l'on peut estimer à plus d'un milliard d'euros, polarisé essentiellement par le ministère de la Défense, tant en budget qu'en effectifs. Il faut toutefois ajouter que le montant cité relève d'une hypothèse très basse ne tenant pas compte de la possibilité de faire supporter le coût, élevé, des investissements technologiques utiles notamment à la DGSE et à la DRM par d'autres programmes et notamment ceux conduits par la Direction générale de l'armement (DGA). On

peut ainsi relever dans le programme 146 « équipement des forces » les sous-actions 07-39 et 07-40 qui correspondent à « Renseigner, surveiller, acquérir et reconnaître », c'est-à-dire aux capteurs techniques : ces deux lignes représentaient plus de 220 M€ en 2012 et 335 M€ en 2013. Encore est-il réaliste de penser que d'autres dépenses techniques sont masquées dans la LOLF par les services qui ne peuvent pas rendre public des programmes sensibles. Au final, il apparaît réaliste d'avancer **au minimum un budget global d'1,5 milliard d'euros** pour l'ensemble des six services. Cette somme, qui n'est qu'un ordre de grandeur est une **hypothèse très basse**[18], car elle ne tient que très partiellement compte du coût de recherche et de développement de la technologie utilisée par les services. Cette estimation, modérée par rapport au budget de la Défense, est pour autant importante en valeur absolue. Elle est susceptible d'évoluer à la hausse car le coût du renseignement d'origine technologique est croissant pour tous les pays.

1.6. LES FINALITÉS DU RENSEIGNEMENT POUR L'ÉTAT : STOCKER OU JUDICIARISER ?

En l'absence d'un texte de loi précisant, comme c'est le cas dans la plupart des démocraties libérales, la finalité des services[19] auxquels ces moyens financiers importants sont consentis et des outils juridiques exorbitants du droit commun sont concédés, la question de la finalité du renseignement doit être clairement posée. Les services de « renseignement » sont fondés sur la collecte, théoriquement raisonnée, d'informations, quelle qu'en soit la nature, pour en faire un renseignement transmis hiérarchiquement aux autorités administratives de tutelle. Si aucun des textes réglementaires ne fait allusion à la transmission horizontale à l'autorité judiciaire des renseignements correspondant à des infractions, la plupart des objets de recherche des services renvoient potentiellement à certaines incriminations pénales. Or, les organes de renseignement s'inscrivent dans une logique temporelle singulière qui les éloigne souvent de la répression à court ou même à moyen terme. Si l'on exclut la DRM qui n'a pas à connaître du renseignement collecté sur le territoire français, les cinq autres services sont *de facto* compétents sur le territoire national et s'inscrivent, par nature, dans une logique de stockage de l'information, souvent

[18] Dans son dernier rapport, et pour la première fois, la DPR a avancé pour l'année 2012 un chiffre d'« environ » 2,1 Mds€ (Délégation parlementaire au renseignement, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2013,* Assemblée nationale n° 1886, Sénat n° 462, 16 avril 2014, p. 15).

[19] A l'exception notable de Tracfin dont le rôle est précisé dans l'article 5 de la loi du 12 juillet 1990.

à long terme. Dans cet esprit une « cible », y compris lorsqu'elle commet une infraction ou présente un danger pour des « intérêts fondamentaux », doit être placée sous observation et le déclenchement d'une action répressive représente souvent le terme de tout un canal d'informations qui peut d'ailleurs être de portée bien plus vaste. C'est la raison pour laquelle il y a souvent réticence de la part des organes de renseignement à aller vers l'autorité judiciaire. Certaines affaires judiciaires médiatisées ont d'ailleurs montré que des juges d'instruction avaient retrouvé, en la possession de certains fonctionnaires des services, des documents que les premiers estimaient utiles à leur investigation. Il y a incontestablement une différence de philosophie avec l'institution judiciaire qui est comptable du déclenchement de l'action publique. Il semble qu'en matière antiterroriste, la DCRI-DGSI ait l'habitude, au moins depuis 1986, de travailler en bonne entente avec le parquet antiterroriste avec des résultats notables et évidents. Il reste que l'antiterrorisme n'est pas la seule mission des services et que dans de nombreux autres cas, la décision d'avertir ou non le procureur de la République relève de la seule appréciation des services. Certes, la « judiciarisation du renseignement » est un processus complexe et de nombreuses « affaires » judiciaires médiatisées ont montré la complexité de ce processus. Malgré ceci, la question du passage du cadre de la police administrative à celui de la police judiciaire renvoie à une question de fond. On peut penser que ce n'est pas tout à fait un hasard si le pouvoir exécutif a pris soin depuis soixante ans, dans les divers textes réglementaires ayant créé et organisé les services, de ne pas mentionner la nature du lien avec l'autorité judiciaire, sinon même son existence.

CHAPITRE II

UN RISQUE D'INCOHÉRENCE ?

2.1. AUPRÈS DU CHEF DE L'ÉTAT : EFFICACE COORDINATION, MAIS ABSENCE DE COLLÉGIALITÉ

Le premier coordonnateur du renseignement, l'ambassadeur Bernard Bajolet[20], indiquait clairement le 31 mars 2009 devant la commission des affaires étrangères du Sénat que sa fonction le situait « à mi-chemin entre une fonction de simple liaison et de direction générale des services »[21]. De fait, il apparaît clairement que la fonction de coordonnateur s'est installée rapidement dans la superstructure publique, assurant avec efficacité la coordination entre les six services, selon les nombreux témoignages publics de leurs différents directeurs, ce qui a été confirmé par les entretiens accordés dans le cadre de cette étude[22]. Il semble que la fonction de coordination ait contribué à installer un climat de confiance entre des services dont nous avons vu la diversité de nature et de moyens. Cette innovation dans le fonctionnement de l'État, a été accompagnée par la fragile existence du Conseil national du renseignement, créé par la volonté présidentielle en octobre 2008 : en effet, cette formation collégiale, composante du CDSN, n'a jamais été réunie par son créateur, mais par son successeur, pour la première et unique fois à ce jour en juin 2013. Est-ce parce qu'une structure collégiale en matière de renseignement n'est pas envisageable en France et qu'il faut se contenter d'un unique responsable, dans un souci de préservation du secret, autant que de rareté des compétences ? L'exemple du *Joint Intelligence Committee (JIC)* créé en 1936 au sein du *Cabinet Office* du Premier ministre britannique atteste du contraire : le *JIC,* peuplé de nombreux analystes, fonctionne encore soixante-dix ans plus tard. Il en est de même pour le *National Security Council* créé en 1947 au bénéfice du Président des États-Unis auquel il est directement attaché. Ces deux structures collégiales de conseil existent encore aujourd'hui.

[20] Actuellement directeur général de la DGSE.
[21] Compte rendu de la Commission des affaires étrangères, Assemblée Nationale, 31 mars 2009, n° 47, p. 6.
[22] Cités en référence en fin de volume.

2.2. LA BALKANISATION EN MATIÈRE D'ORGANISATION DU RENSEIGNEMENT

Une autre question d'efficacité est posée par le fait qu'un certain nombre d'organes de renseignement n'ont pas été mentionnés dans l'arrêté du 9 mai 2011 et ne sont pas reconnus comme des « services spécialisés », alors que leur fonction relève incontestablement d'une mission de renseignement. La Direction du renseignement de la préfecture de police (DRPP) et la sous-direction de l'information générale (SDIG) de la Direction centrale de la sécurité publique et la gendarmerie qui font *de facto* partie d'un « second cercle » collecteur d'information et producteur de renseignement n'ont pas les prérogatives administratives et juridiques particulières des six grands services. La distance entre le « premier cercle » articulé directement avec les ministres de tutelle et l'Élysée par le biais du coordonnateur et le « second cercle » est considérable. Au-delà de l'aspect symbolique qui n'est pas anecdotique car il nourrit notamment les tensions entre services, ceci créé une hiérarchie qui peut être entendue par le second cercle comme une hiérarchie d'intérêt, préjudiciable au fonctionnement global du renseignement public.

D'autre part, la volonté de créer des agences spécialisées ayant le monopole de la collecte et du traitement sur des secteurs spécifiques n'a pas toujours été respectée dans les faits. Ainsi, la Direction du renseignement militaire, créée en 1992 par fusion des organes des différentes armées, devait avoir le monopole en matière de « renseignement d'intérêt militaire » (RIM). Cependant les trois armées ont créé depuis des centres de renseignement qui assurent collecte et traitement du renseignement[23] : l'esprit du texte n'a pas été respecté dans la mesure où c'est à la DRM d'orienter la recherche du renseignement et de recevoir le résultat de la collecte. On relèvera qu'en 2008 le directeur de la DRM estimait que 7 800 militaires participaient à la collecte et au traitement du RIM au bénéfice de la direction dont seulement la moitié figuraient dans ses effectifs[24]. Ceci signifie non seulement que les membres de la « communauté du renseignement » sont plus nombreux que les 12 000 avancés par le *Livre blanc* de 2008 ou les 13 000 indiqués par la DPR[25], mais aussi que la maîtrise complète de l'effort RIM au sein du ministère de la Défense est complexe à délimiter dans la mesure où une partie des moyens de recherche humains du RIM est assurée à son bénéfice, mais pas sous son autorité directe.

[23] *Cf.* « Entretien avec le général Gomart. Le renseignement militaire aujourd'hui », *Stratégique,* janvier 2014, n° 105, p. 177-188.

[24] *Cf.* Michel Masson, « Les défis du renseignement militaire », *Sécurité globale,* n° 4, été 2008, p. 10.

[25] Délégation parlementaire au renseignement, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2013,* Assemblée nationale no 1886, Sénat n° 462, 16 avril 2014, p. 15.

2.3. UN ÉCHEVEAU COMPLEXE DE DROITS ET DE NORMES JURIDIQUES CONCURRENTS

Aujourd'hui les activités des organes de renseignement relèvent autant du code de la défense que du code de sécurité intérieure, du code des douanes, du code monétaire et financier et du code pénal, et certaines de leurs pratiques touchent aussi directement à la limitation de certaines libertés publiques essentielles, en particulier à la liberté individuelle, au travers notamment de la liberté d'aller et venir et du droit au respect de la vie privée. On retrouve sur le terrain du droit la tension évoquée plus haut[26] entre pratiques de sécurité et garanties des libertés, la dialectique entre deux ensembles juridiques par nature différents et même antagonistes. Malgré les vagues successives de décentralisation, la France demeure un pays de culture jacobine, dominé par un État unitaire sans contre-pouvoir parlementaire véritable : ce contexte général renforce au plus près du « domaine très réservé », la situation juridique des organes de renseignement qui s'inscrivent dans un cadre réglementaire dépendant de l'exécutif, bien loin du domaine de la loi débattue publiquement.

Cette situation déjà complexe naturellement l'est rendue plus encore par l'apparition de droits externes, communautaire et européen, dont l'influence sur le droit français ne cesse de croître. Ainsi en se référant en partie aux articles de la Convention européenne des droits de l'homme de 1950[27] – ratifiée par la France en 1974 – plusieurs assemblées européennes, dont la France fait partie, ont élaboré un certain nombre de principes et de « bonnes pratiques » relatives au statut et à l'action des services de renseignement dans les régimes démocratiques. Les différentes recommandations et résolutions ont abouti dans la décennie 2000 à fixer trois principes cardinaux[28] : (1) la création de services de renseignement doit être l'aboutissement d'un processus législatif, c'est-à-dire d'un texte normatif porté à la connaissance de la représentation nationale, (2) ils ne peuvent porter atteinte aux libertés ou les limiter qu'avec proportionnalité, (3) enfin les services doivent être soumis à un contrôle externe parlementaire et juridictionnel. Ces textes, bien qu'ils s'appuient sur la jurisprudence de la Cour européenne des droits de l'homme, demeurent de nature et de portée politiques. Ils ont néanmoins largement inspiré les nouveaux pays membres de l'UE après 1991 qui s'y sont tous conformés. À ces textes préconisant des « bonnes pratiques » – qui ne correspondent pas à la situation française – s'ajoute la jurisprudence de la CEDH qui a plusieurs fois

[26] *Cf.* en page 14.

[27] On notera son appellation originale et complète : « Convention de sauvegarde des droits de l'homme et des libertés fondamentales ».

[28] On trouvera en annexe 1 en page 73 une liste de ces principaux textes.

condamné la France, notamment pour le non-respect de l'article 8 de la Convention : ainsi fut-elle par exemple condamnée en 1991 pour son système non légal d'écoutes téléphoniques.

En outre, en matière de libertés fondamentales, il y a dans tous les pays occidentaux un avant et un après 2001, dans la mesure où des législations nouvelles en ciblant la menace réelle du terrorisme international djihadiste ont fortement affaibli ou transformé les garanties classiques pesant sur les libertés. La France n'échappe pas à la règle : par les lois de 2001 (« relative à la sécurité quotidienne »), 2004 (dite « Perben II »), 2006 (« relative à la lutte contre le terrorisme »), l'évolution de la procédure pénale et des moyens de surveillance ont eu un effet direct sur l'état des libertés en affaiblissant les garanties classiques fondatrices de l'État de droit. Dans un autre contexte, les pratiques d'espionnage massif des États-Unis et de ses quatre alliés – dont la Grande-Bretagne, membre de l'UE – connues depuis 2001[29], et plus encore par la vague de documents publiés par Edward Snowden depuis juin 2013, constituent des atteintes supplémentaires aux libertés.

Du point de vue des services de renseignement, la dialectique sécurité-libertés peut être observée en matière d'écoutes et d'interceptions de communication, de protection des données ou encore de classification.

Au titre de l'article 22 de la loi de 1991[30], les six services peuvent demander aux opérateurs des informations concernant les données techniques de communication, soit les numéros de lignes, soit les factures détaillées (« fadettes ») qui permettent d'identifier les numéros appelés et appelants, enfin les éléments permettant de localiser les lignes à un moment donné. Afin de reconstituer la cartographie des réseaux des personnes suspectes, ce type d'information est particulièrement précieux pour les « services ». On le mesure, en observant par exemple entre août 2011 et juillet 2012, que près de 197 000 demandes de ces données techniques ont été présentées à la CNCIS (qui en en a refusé 7 %)[31]. Avec ce chiffre, on prend également conscience de l'ampleur des mesures de police administrative intrusives et limitatives pour les libertés. Dans le processus d'autorisation des interceptions de

---

[29] *Cf.* Sur « Echelon », ancêtre de « Prism », les rapports du Parlement français (Arthur Paecht, *Echelon : mythe ou réalité ? Rapport d'information,* Paris, Assemblée nationale, 11 octobre 2000, 90 p.) et du Parlement européen (Gerhard Schmid, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, système d'interception ECHELON* (2001/2098 (INI), Rapport A5-0264/2001, Parlement européen, 11 juillet 2001, 210 p.)

[30] Désormais article L. 244-2 du code de la sécurité intérieure.

[31] *Cf.* CNCIS, *Vingtième rapport d'activité 2011-2012 de la Commission nationale de contrôle des interceptions de sécurité,* Paris, La Documentation française, p. 65-66.

sécurité qui touche au principe d'inviolabilité de la correspondance et dans celui de l'article L. 244-2 sur les données techniques de communication, la CNCIS décide en fonction de plusieurs principes : outre la conformité aux cinq motifs de la loi de 1991, elle prend également en compte les critères de présomption d'implication directe et personnelle, de subsidiarité et de proportionnalité. Elle est donc une structure non judiciaire[32] qui décide – dans un cadre administratif – du degré d'intrusion autorisé aux services. Ce faisant la CNCIS est une autorité administrative indépendante qui est *de facto* protectrice des libertés des citoyens. L'interception de données liées aux communications électroniques avait été autorisée dans le cadre antiterroriste par une loi de 2006. Le vote de la LPM 2014 a étendu ces interceptions pour les services de renseignement hors du cadre antiterroriste en les soumettant aux motifs utilisés depuis 1991 pour les écoutes téléphoniques administratives. C'est une « personnalité qualifiée » dépendant du Premier ministre et non la CNCIS qui accorde l'autorisation ou la refuse. Pour les données techniques, il y a eu là un alignement des règles du régime de police administrative sur celle prévalant dans un cadre antiterroriste.

Le principe du secret des correspondances est reconnu par d'anciens et très nombreux textes internationaux et notamment parmi ceux qui ont structuré une part du droit international public : la Déclaration universelle des droits de l'homme (1948), la Convention européenne des droits de l'Homme (1950), le Pacte international relatif aux droits civils et politiques (1966), mais aussi par des textes de moindre ampleur, plus techniques, à l'image de la Constitution de l'Union internationale des télécommunications (1992), ou encore les directives de 1997 et de 2002 de l'Union européenne sur le secteur des télécommunications.

Les textes relatifs à la protection des données sont plus tardifs et moins nombreux, mais pas moins clairs. La convention 108 du Conseil de l'Europe signée en 1981 assure avec beaucoup de précision la protection des données, mais c'est un texte d'origine politique de portée juridique moins forte que la Convention de 1950, bien que la convention 108 ait été à l'origine (tout comme la loi française de 1978) de la directive UE 1995/46/CE du 24 octobre 1995 qui, elle, est un cadre contraignant pour les pays membres de l'UE. Par rapport aux directives de l'UE qui ne s'appliquent qu'aux États membres, 46 pays, dont les États-Unis et la Russie, ont à ce jour ratifié la convention 108 qui est donc un socle international important pour les libertés. Quant à la directive de 1995, qui est en cours de révision parallèlement et de façon convergente avec la convention 108, elle pose le principe de l'existence d'une

[32] Son délégué général est toutefois un magistrat de l'ordre judiciaire.

autorité de contrôle et d'un droit d'accès aux données pour les citoyens[33]. Enfin, il faut mentionner que la Charte des droits fondamentaux de l'UE, entrée en vigueur en 2009, a la même valeur que les traités de l'Union : or, elle garantit dans ses premiers articles, autant la liberté de communication que la protection des données.

Les administrations sont naturellement amenées à protéger une partie de l'information qu'elles recueillent et produisent. Elles disposent pour cela d'un principe établi par le code pénal qui les contraint à assurer le « secret de la défense nationale » en procédant à des mesures de classification de tous supports et formes d'informations. La définition de ce secret de « défense nationale » est large depuis l'ordonnance de 1959. À l'heure où les menaces pour les intérêts de l'État se diversifient, il importe de ne pas affaiblir le principe de la classification et le champ large défini en 1959. Dans ce cadre particulier, trois enjeux manifestes apparaissent : l'opportunité de la classification, son niveau, enfin sa durée. La capacité importante du pouvoir réglementaire de restreindre l'accès à l'information des citoyens (principe garanti par l'article 1er de la loi n° 78-17 du 6 janvier 1978) ne doit pas être un outil détourné de sa finalité. D'ailleurs, l'instruction générale interministérielle (IGI) « 1300 »[34] relative à la protection du secret de la défense nationale du 30 novembre 2011 rappelle dans son introduction qu'il faut « limiter […] la production de documents classifiés à ce qui est strictement nécessaire ». Dans cet esprit, il importe de classifier, à bon escient, des documents touchant effectivement au secret de la défense nationale et non des informations d'une autre nature, pratique avérée dans le passé par certains avis de la CCSDN[35]. Ainsi que l'écrivait cette commission : « Le secret de la défense nationale est d'autant mieux respecté et crédible qu'il en est fait usage de façon restrictive et à bon escient »[36]. Il importe de relever qu'un mauvais usage de la classification, faite pourtant pour protéger l'État peut même le fragiliser dans la mesure où la responsabilité pénale d'un ministre pourrait être engagée. Les pratiques de sur-classification peuvent également jouer sur les niveaux de classification, chacun d'entre eux étant par ailleurs porteur d'une durée différente. En Allemagne, l'ordonnance sur la classification[37] a entériné le principe de la déclassification automatique, avec des durées modulées en fonction du niveau.

---

[33] Toutefois après le rappel des principes fondamentaux sur la protection des données, la Convention rappelle qu'il est possible aux États membres d'y déroger « pour un motif d'intérêt public important » (art. 8-4) et par la loi, pour des raisons touchant à la « sûreté de l'État, la défense ou la sécurité publique » (art. 13).

[34] Actuellement en cours de refonte.

[35] *Cf.* notamment : *Rapport de la commission consultative du secret de la défense nationale 1998-2004,* Paris, La Documentation française, 2005, p. 111.

[36] *Cf. Rapport de la commission consultative du secret de la défense nationale 1998-2004,* Paris, La Documentation française, 2005, p. 111.

[37] 2006, modifiée en 2010.

Sur l'ensemble de ces aspects juridiques, la dispersion des règles de droits, la prévalence du cadre de police administrative d'une part et le rôle croissant du droit externe de l'autre exposent de façon croissante l'État à l'« insécurité juridique »[38], selon la formule du Conseil d'État, prenant la forme soit de censures du Conseil Constitutionnel par le biais de recours parlementaires[39], soit à de questions prioritaires de constitutionnalité[40], soit enfin l'exposant à une condamnation par la Cour de Strasbourg.

2.4. FACE À LA « NOUVELLE FRONTIÈRE » DU CYBERESPACE, LES ATOUTS DE LA CO-PRODUCTION PUBLIC-PRIVÉ

Qualifié parfois de « 5e dimension », le cyberespace abolit les repères traditionnels des États : nulle territorialité, souveraineté très floue, inexistence d'un droit propre et gouvernance multi-acteurs dont les États ne sont qu'une composante parmi d'autres… autant de caractéristiques gênant la mise en place d'une stratégie claire. Or, cet « espace » ou cette dimension nouvelle présente un double intérêt : pour les organes de renseignement, il est un lieu de collecte de l'information, qu'elle soit librement accessible ou qu'elle ne le soit pas, et il est également un terrain d'affrontements.

Le cyberespace est en fait un immense agrégat constitué en partie de « données » relatives aux individus. Face aux captations étrangères, privées ou publiques, dont elles sont l'objet, les données des citoyens français sont un réel enjeu de souveraineté nationale qui n'est pas toujours bien identifié, ce qui amoindrit la capacité à les protéger. Or, dans le cadre de l'UE, les accords signés avec les États-Unis en 2000 (« Safe Harbour ») et 2010 (« Swift 2 ») ont débouché sur la livraison de volumes gigantesques de données. Ceci pose d'importantes questions en matière de souveraineté numérique.

Cet espace est aussi saturé de données économiques, à commencer par celles de nos entreprises. Des informations sur leurs clients aux documents comptables en passant

---

[38] *Cf.* le très classique : Conseil d'État, *Rapport public 2006. Sécurité juridique et complexité du droit,* Paris, La Documentation française, 2006, 411 p.

[39] Ainsi en décembre 2013, plusieurs dizaines d'élus de la majorité et de l'opposition ont essayé en vain, de déposer un recours auprès du Conseil Constitutionnel contre l'article 20 de la loi de programmation militaire. Leur initiative avait échoué à une dizaine de voix du nombre requis de 60.

[40] C'est par ce biais que le Conseil Constitutionnel a censuré en 2011 un article de la précédente loi de programmation militaire sur les lieux classifiés.

par des données plus stratégiques encore, la vogue du « partage de l'information » et la réalité de l'hyperconnexion font des entreprises des maisons de verre pour ceux qui maîtrisent les outils intrusifs dans le cyber. Ce n'est pas seulement le patrimoine informationnel qui doit être protégé mais souvent des données liées aux investissements et à la stratégie, c'est-à-dire au développement et à la pérennité de l'entreprise. Des cyberattaques d'origines plus ou moins privées à l'espionnage économique conduit par un certain nombre d'États maîtrisant les moyens techniques, il y a là un enjeu majeur de sécurité.

Les capacités cybernétiques françaises publiques sont actuellement entre les mains de quatre ensembles : l'ANSSI qui dépend directement du Premier ministre, l'État-major des armées (EMA) qui a créé la fonction d'officier général à la cyber-défense en 2011, la Direction générale de l'armement (DGA) et enfin les « services spécialisés ». La première a une mission purement défensive de sécurité des systèmes d'informations nationaux ; l'EMA est une structure militaire à vocation opérationnelle qui assure à la fois la sécurité des moyens cyber des armées, mais peut également mener « des actions informatiques d'accompagnement des actions militaires »[41], c'est-à-dire du cyber offensif en parallèle de l'action militaire ; la DGA travaille en recherche-développement sur les moyens informatiques de souveraineté en matière défensive et offensive[42] ; enfin parmi les « services spécialisés », la DGSE est composée d'une direction technique. Le cadre du cyber étatique est donc fortement militarisé en France. Or ceci n'est pas la règle dans le monde : en 2012, selon l'*United Nations Institute for Disarmament Research,* sur 114 États ayant des programmes et des organisations dévolues à la cybersécurité, 67 relevaient de structures civiles et 47 seulement des armées[43].

Dans le cadre de l'organisation française, trois enjeux apparaissent particulièrement saillants :

- pour ce qui est de la composante cyber dans les opérations militaires, l'état-major considère logiquement que le cadre juridique de référence est celui du conflit armé concerné ;

---

[41] Déclaration du contre-amiral Coustillière, officier général en charge de la cyberdéfense : *Compte rendu de la Commission de la défense nationale et des forces armées,* Assemblée nationale, 12 juin 2013, n° 79, p. 3.

[42] *Cf.* les déclarations de l'ingénieur en chef de l'armement Guillaume Poupard, directeur de la DGA-MI : *Compte rendu de la Commission de la Défense nationale et des forces armées,* Assemblée nationale, 10 juillet 2013, no 85, p. 5. Il est depuis mars 2014 directeur de l'ANSSI.

[43] UNIDIR, *The Cyber Index. International Security Trends and Realities,* United Nations, New York and Geneva, 2013, p. 1.

- le directeur de la DGSE avait indiqué en février 2013 devant une commission de l'Assemblée nationale que son service avait « un important dispositif d'interception des flux Internet »[44]. Il est heureusement possible techniquement de séparer les communications des citoyens français de celles des citoyens étrangers et donc de respecter le secret des correspondances garanti par le droit français, principe dont l'importance a été rappelée par le Premier ministre le 22 février 2014 lors de la visite effectuée à l'ANSSI au cours de laquelle il a déclaré : « Notre objectif est de garantir l'inviolabilité des correspondances, vieux principe républicain qu'il faut réaffirmer et réactualiser dans le monde numérique ». En revanche, le cadre légal français des interceptions des communications étrangères sur son territoire n'est pas connu à ce jour. Rendues publiques depuis l'été 2013, les pratiques des États-Unis en matière d'interruption des communications ont inquiété l'opinion, y compris parmi ses « alliés ». Ceci a rendu l'opinion particulièrement sensible désormais à tout ce qui concerne ses « données » et à leurs modes de protection, tout en engendrant questions et confusions ;

- par ailleurs, il existe également ce qui, depuis le *Livre Blanc* 2008, est appelé la « lutte informatique offensive »[45] (LIO). Les armes informatiques sont mises en œuvre, selon le sénateur Bockel, par les « services spécialisés »[46], c'est-à-dire selon l'arrêté de mai 2011, par les services de renseignement. Or, seule la DGSE a les moyens techniques de le faire, depuis que la France a fait le choix d'une « agence intégrée », c'est-à-dire d'une agence technique intégrée au service de renseignement extérieur. D'autres pays ont procédé différemment à l'exemple de la Grande-Bretagne ou des États-Unis qui ont des agences techniques séparées (GCHQ et NSA), alimentant ensuite en données les analystes au sein des agences pour produire le renseignement. Dans le cas de la France, ni les moyens de la Lutte informatique offensive (LIO), ni son cadre d'emploi ne sont connus, pas plus que son cadre juridique. Jean-Claude Mallet, conseiller spécial du ministre de la Défense, a évoqué devant le Parlement cette question en des termes précis : « Dans ce cadre, le ministère de la Défense réfléchit à des capacités informatiques offensives, dont les autorités publiques, au plus haut niveau de l'État, pourraient décider de l'emploi – en l'occurrence, un emploi proportionné, discret et le plus

[44] *Compte rendu de la Commission de la Défense nationale et des forces armées,* Assemblée nationale, 20 février 2013, n° 56, p. 3.

[45] *Défense et sécurité nationale. Livre blanc. Les débats,* Paris, Odile Jacob-La Documentation française, 2008, p. 207.

[46] Jean Marie Bockel, *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense,* 18 juillet 2012, Sénat, n° 681, p. 89.

efficace possible, en appui des actions militaires »[47]. La discrétion parfaitement compréhensible des autorités s'explique par le fait que le cyber pourrait être conçu et inséré dans une perspective de dissuasion, ainsi que l'indique le sénateur Bockel : « La France dispose de capacités offensives. Si nous n'avons pas à mettre sur la place publique le dispositif opérationnel qui est le nôtre, qui est un vrai dispositif de dissuasion, nous pourrions néanmoins avoir une doctrine d'emploi »[48]. Or, en ce qui concerne le cadre d'emploi, le *Livre blanc* de 2008 rappelait qu'il devait être « compatible avec les principes juridiques du droit français »[49].

Le domaine cybernétique est par ailleurs un lieu particulier où les besoins en matière de sécurité pour les intérêts nationaux sont tels que des industries de souveraineté, par ailleurs excellentes à l'export dans le domaine de la cybersécurité et de la cyberdéfense, se sont développées, telles Airbus Defence and Space, Thales, Atos ou encore Sogeti pour les plus importantes. En matière de softwares, il existe tout un secteur de sociétés françaises, principalement des PME travaillant principalement dans le domaine des logiciels de souveraineté, ainsi que du traitement des données et de l'information. Il s'agit en fait de technologies duales dans lesquelles la France a, de façon continue, un savoir mondialement reconnu. Sur ce segment, il faut se féliciter que la proximité naturelle avec l'État soit forte, surtout depuis l'accent mis sur le cyber en 2008, encore accentué par le *Livre blanc* de 2013, les trois plans de reconquête en matière de *Big Data, Cloud computing* et *Cybersécurité* (annoncés en 2013 par le ministre de l'Industrie parmi les 34 plans de reconquête de la « Nouvelle France industrielle ») et confirmé par l'annonce du pacte Défense Cyber par le ministre de la Défense en février 2014[50]. Ce secteur a renforcé sa structuration par la création en septembre 2013 du Conseil des industries de confiance et de sécurité (CICS) et l'implication des pouvoirs publics au plus haut niveau, matérialisé par l'installation à Matignon un mois plus tard du « Comité de la filière des industries de sécurité » (CoFIS) pour un secteur réalisant 10 Mds€ de chiffre d'affaires et pesant 50 000 emplois qualifiés. La complémentarité public-privé a été confirmée sur un autre plan par la création d'une réserve citoyenne « cyberdéfense » après 2012. Par rapport à ses principaux partenaires, la France bénéficie de nombreux atouts : un État désormais mobilisé par les questions de cybersécurité, un enseignement supérieur public formant des mathématiciens et informaticiens de niveau mondial, un secteur privé du numérique en forte expansion et une industrie informatique de qualité. En

[47] Bruno Sido et Jean-Yves Le Déaut, *Le risque numérique: en prendre conscience pour mieux le maîtriser ?,* Assemblée nationale n° 1221-Sénat n° 721, 3 juillet 2013, OPECST, p. 54.

[48] *Ibid.,* p. 22.

[49] Défense et sécurité nationale.., *op. cit.,* p. 208.

[50] *Cf. Pacte Défense Cyber : 50 mesures pour changer d'échelle,* Paris, ministère de la Défense-Dicod, 2014, 22 p.

effet, la France dispose d'un secteur informatique soutenant la concurrence à l'export si l'on considère l'informatique industrielle et l'informatique embarquée. À l'image naguère du secteur nucléaire et de certaines industries duales, le numérique – dans sa dimension sécurité et défense – doit s'inscrire désormais dans une perspective économique de co-production. Dans la mesure où il s'agit d'un secteur stratégique pour l'État, pour la protection des entreprises et celle des citoyens, ce secteur nécessite de très forts investissements en recherche fondamentale, en études amont et en R&D. Pour ce faire, il doit mobiliser des fonds publics et privés importants. Or, le développement du secteur ne s'appuie que très marginalement sur les 71 pôles de compétitivité actuellement existants. De même les sommes mobilisées par l'État, notamment les études amont de la DGA pour le cyber qui irriguent le secteur privé et permettent le développement de nombreuses PME, sont encore relativement modestes, 107 millions d'euros en autorisations d'engagement en 2014, selon un récent rapport parlementaire, alors qu'il faudrait le double ou le triple.

CHAPITRE III

RECOMMANDATIONS : RATIONALISER POUR UNE PLUS GRANDE EFFICACITÉ ET RENFORCER LA PROTECTION DES CITOYENS

À la suite du bilan effectué dans les deux premières parties de ce rapport, nous proposons ici 48 recommandations ordonnées en suivant le cadre de la partie précédente et s'inscrivant dans six grandes lignes directrices :

1 - Atténuer la loi d'airain du fonctionnement de la « communauté du renseignement »

2 - Rationaliser pour gagner en efficacité et en reconnaissance publique

3 - Clarifier et moderniser les règles de droit dont les services relèvent

4 - Clarifier les règles et les pratiques dans la « cinquième dimension » au service de la souveraineté

5 - Conduire une réflexion de nature stratégique et prospective sur les activités de renseignement

6 - Engager la réforme culturelle du renseignement.

3.1. ATTÉNUER LA LOI D'AIRAIN DU FONCTIONNEMENT DE LA « COMMUNAUTÉ DU RENSEIGNEMENT »

Ainsi qu'on l'a vu plus haut[51], la structuration tout à fait singulière de l'ensemble formé aujourd'hui par les six organes de renseignement, mais aussi ceux du « second cercle » relève dans le long terme du pouvoir exécutif. Il est vain de penser transformer la structuration des acteurs du renseignement sans prendre en compte cette contrainte politique et institutionnelle majeure depuis 1958, véritable

[51] *Cf.* en page 18.

loi d'airain. La question de l'utilité d'une telle transformation doit d'ailleurs être posée. Cependant quelques transformations et aménagements sont réalistes et souhaitables :

1. En ce qui concerne la marginalisation effective du **Premier ministre en matière de renseignement,** une réflexion doit être engagée **pour identifier ce qui demeure de son ressort réel,** ceci permettant notamment d'achever la réforme de l'ordonnance de 1959. En l'état, il joue un rôle important en matière de collecte de renseignement par des moyens techniques, ayant à sa disposition depuis 1960 le groupement interministériel de contrôle (GIC). Il en assure le contrôle par le biais d'une autorité administrative indépendante qu'il finance, la CNCIS. Sur un autre plan, il importe de préciser quelles sont les compétences précises du SGDSN en matière de renseignement[52].

2. Afin de sortir du pré carré de l'exécutif réglementaire, **l'existence, les missions et les moyens de cinq des six services**[53] **« spécialisés » doivent être inscrits, pour chacun d'entre eux, dans une loi particulière,** se conformant ainsi aux nombreuses recommandations européennes. La **loi devrait notamment mentionner les divers moyens à la disposition des services et notamment les capacités intrusives,** en respectant ainsi le texte et l'esprit de l'article 34 de la Constitution confirmé par la jurisprudence régulière du Conseil Constitutionnel.

3. Le temps est largement venu de **mettre en place un authentique contrôle parlementaire adapté à la singularité des services, sous forme d'une commission permanente de contrôle des activités des services commune aux deux assemblées,** créée par une loi spécifique et non par une loi de programmation militaire dont le périmètre est par nature réduit au ministère de la Défense. Ceci permettrait de se situer dans l'esprit de l'article 24 de la Constitution : « Le Parlement vote la loi. Il contrôle l'action du Gouvernement. Il évalue les politiques publiques ». Cette commission permanente serait caractérisée par une publicité de ses travaux (partielle, tout en étant plus importante que celle de l'actuelle délégation parlementaire au renseignement). Son activité serait bien évidemment bornée par la décision du Conseil Constitutionnel de 2001 interdisant au Parlement de connaître « les opérations en cours »[54]. On notera qu'en Allemagne le contrôle parlementaire du renseignement est inscrit dans la

[52] Ceci étant distinct de l'aide administrative et budgétaire de support qu'il offre à l'équipe du coordonnateur.
[53] On rappelle que Tracfin est le seul des six services créé par la loi (loi n° 90-614 du 12 juillet 1990).
[54] Décision n° 2001-456 du 27 décembre 2001.

Constitution (art. 45. d. 1). Il est intéressant de relever également que dans ce pays où le système politique repose sur une très forte culture parlementaire – à la différence de la France – le contrôle exercé par le *Bundestag* se fait à double détente : le gouvernement doit adresser à la commission compétente (« PKG ») un rapport sur les services et celle-ci peut ensuite interroger les membres des services. Il s'agit donc en fait d'un contrôle de l'usage fait par le gouvernement des services mais également d'un contrôle des services eux-mêmes. Ce type de nuance est important car il permet de comprendre que les élus allemands ont eu aussi le souci de protéger les services à l'égard de la politisation ou d'un éventuel usage politique.

4. La création en 1998 de la Commission consultative du secret de la défense nationale (CCSDN) a été une réforme très importante de portée libérale : en créant un processus permettant aux juges d'instruction de pouvoir connaître les documents classifiés par l'administration, elle a établi un sas entre les pouvoirs exécutif et judiciaire. Le principe de la séparation des pouvoirs étant en fait un principe de distinction mais aussi de collaboration des pouvoirs, dans le même esprit, la CCSDN pourrait être utilisée afin d'établir un sas entre les pouvoirs exécutif et législatif. Bien qu'il y ait eu depuis plus d'une décennie de nombreux cas de figure (conflits armés, missions parlementaires) dans lesquels l'exécutif a donné ponctuellement communication de documents classifiés à certains parlementaires[55], à l'heure actuelle, les élus ne peuvent pas avoir accès à des documents classifiés dans le cadre de leurs enquêtes. Il serait possible **d'autoriser les seules commissions d'enquête parlementaire à solliciter la CCSDN pour la déclassification de certains documents**[56]**,** l'avis de la commission demeurant consultatif.

3.2. RATIONALISER POUR GAGNER EN EFFICACITÉ ET EN RECONNAISSANCE PUBLIQUE

Associé à la contrainte institutionnelle qui vient d'être évoquée, l'héritage historique des services français, marqué par l'irrationalité, pèse lourdement, en particulier la stratification historique des nombreux organes de renseignement, si l'on tient

[55] *Cf.* Marc Guillaume, « Parlement et secret », *Pouvoirs,* 2001, n° 97, p. 78-79.

[56] Il faudrait pour ce faire réformer l'article 6 alinéa 2 de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

compte du fait qu'il ne s'agit pas seulement des six « services spécialisés » définis en 2011, mais de l'ensemble de ceux qui contribuent de fait à l'élaboration du renseignement.

5. Tout d'abord, il importe **d'élargir la délimitation administrative de la « communauté » au-delà du « premier cercle »** afin de prendre en compte les autres composantes de l'administration du ministère de l'Intérieur produisant du renseignement (DRPP, SDIG, Gendarmerie) et assurer ainsi un meilleur partage et une meilleure circulation de l'information au bénéfice de la mise en œuvre de la politique gouvernementale.

En matière de renseignement, nous avons vu que la LOLF – contrairement à son principe directeur – n'avait pas créé de clarté en matière de renseignement, bien au contraire. Certaines réformes simples pourraient être entreprises sans mettre en danger la confidentialité.

6. Il est peu réaliste en l'état de l'éclatement administratif de penser à une réorganisation budgétaire, néanmoins **une fusion des programmes 144 et 178 du ministère de la Défense** permettrait d'avoir une orientation plus rationnelle des choix budgétaires des trois organes de renseignement qui en dépendent.

7. Le caractère interministériel du renseignement étant évident, il serait utile **d'élaborer un document de politique transversale** prévu dans le cadre normal de LOLF **pour le renseignement,** comme c'est le cas par exemple pour « l'action extérieure de l'État » ou la « défense et la sécurité nationale », **permettant notamment d'aboutir à un chiffrage global.**

8. De façon non exclusive de la précédente mesure, une réforme budgétaire paraît également facilement réalisable : sur le modèle du *Single Intelligence Account* britannique et du *National Intelligence Program* aux États-Unis, il faudrait **créer deux agrégats budgétaires afin de mesurer l'effort national annuel en matière de renseignement,** l'un correspondant au budget du « premier cercle », celui des six services, l'autre pour le « second cercle ». Pour des raisons de confidentialité, le détail de chacun de ces agrégats ne serait pas rendu public, mais serait communiqué aux commissions spécialisées des assemblées.

9. Dans le même esprit, il faudrait que lors de l'examen du projet de loi de finances, les rapporteurs spécialisés puissent avoir connaissance d'un agrégat unique

permettant d'évaluer la part des investissements dans le domaine des capteurs techniques. Seuls les rapporteurs devraient avoir connaissance de cet agrégat qu'ils ne pourraient rendre public.

10. À l'occasion de la transformation de la **DCRI en DGSI, il est dès lors possible** de faire figurer, comme pour la DGSE et la DPSD, l'action du ministère de l'Intérieur en matière de contre-espionnage, contre-terrorisme et contre-ingérence sur **un programme budgétaire particulier.**

3.3. CLARIFIER ET MODERNISER LES RÈGLES DE DROIT DONT LES SERVICES RELÈVENT

Plusieurs modifications juridiques d'ampleur et de portée différentes permettraient de mettre un terme au « double retard » évoqué au début de ce rapport et de permettre de maintenir autant la sécurité du périmètre secret de l'État que de mieux garantir les libertés des citoyens.

La modernisation du cadre normatif du renseignement

11. Il faut **inscrire dans la Constitution,** aux côtés de la « défense nationale » et de la « sécurité », **la mission de « renseignement »** publique – à l'instar de l'Allemagne dans les articles 45 d. et 87 de la *Grundgesetz* de 1949 – afin, dans un contexte d'imprécision juridique due à l'ordonnance de 1959, de permettre de faire de la cinquième fonction stratégique une réelle politique publique. Cette évolution présenterait un triple avantage : sur un plan symbolique qui n'est pas anecdotique et dissiperait certains préjugés ; elle permettrait par ailleurs de jeter les bases d'une politique publique ; enfin elle présenterait aussi l'avantage de protéger les « services ».

12. Cette disposition permettrait **d'engager un débat** sur la finalité du renseignement pour l'État **afin de préciser la relation avec l'autorité judiciaire.**

13. Dans le même ordre d'idées, il serait souhaitable **d'achever la refonte et l'adaptation de l'ordonnance de 1959,** fondatrice pour la V^e^ République, en clarifiant, notamment dans le code de la défense, ce qui relève de la « défense nationale » et de la « sécurité nationale ».

14. Il paraît important de **modifier l'article 241-3 du code de la sécurité intérieure** introduit par la loi de 1991 qui laisse planer une grande ambiguïté sur le fait que les communications hertziennes individuelles (utilisant les lignes de téléphones portables) ne relèveraient ni de ce code, ni du code de procédure pénale. Avec sagesse en 1998, la CNCIS – reprenant d'ailleurs l'exposé des motifs de la loi qui craignait une condamnation de la CEDH[57] – avait estimé qu'il fallait réintégrer les interceptions individuelles pratiquées dans le domaine hertzien dans le champ de la loi. Bien que dans la pratique la CNCIS ait levé l'ambiguïté en s'appuyant sur les travaux préparatoires à la loi de 1991, **il faut donner à cette bonne pratique la force d'une protection par la loi.**

15. Cette modification permettrait de **dissiper le flou de la notion de « défense des intérêts nationaux »** mentionnée dans le même article. Une telle évolution est souhaitable dans la mesure où cette la notion peut être interprétée de façon si large que son usage devient fortement attentatoire aux libertés publiques. Ce caractère incertain, nourrissant de vifs débats judiciaires, a pu être constaté, notamment dans les échanges entre avocats et magistrats dans le cadre d'un procès ayant eu lieu en février 2014 devant la 17e chambre correctionnelle du TGI de Paris.

16. Dans le même esprit, **certaines composantes de la notion d'« intérêts fondamentaux de la Nation »** (art. 410-1) créée en 1992 dans le nouveau code pénal devraient être précisées. Dans la longue liste détaillée qu'il comporte, si certains termes sont parfaitement clairs, d'autres sont si larges – en fait bien vagues – qu'ils sont susceptibles de multiples interprétations, certaines en défaveur des libertés[58].

Le renforcement nécessaire des libertés individuelles : garanties et indicateurs

17. Dans le droit français, la protection de la vie privée dont la protection des données est une composante, relève du domaine de la loi (lois des 17 juillet 1970 et du 7 janvier 1978). Afin de renforcer le **droit à la protection des données personnelles, il faut l'inscrire dans le préambule de la Constitution.**

---

[57] *Cf. Septième rapport d'activité 1998 de la Commission nationale de contrôle des interceptions de sécurité,* Paris, La Documentation française, 1999, p. 35.

[58] *Cf.* l'annexe 2.

18. Le gouvernement français doit jouer un **rôle permanent auprès de la Commission européenne en vue d'accélérer l'adaptation de la directive** UE 1995/46/CE **sur la protection des données personnelles** afin de rattraper le retard pris depuis l'automne 2013.

19. Ce renforcement des libertés concerne également les membres des organes de renseignement. La nécessité est grande de **renforcer la protection juridique des fonctionnaires et des agents des services de renseignement dans le cadre de leurs missions** en étendant aux fonctionnaires et agents de la DRPP et de la Gendarmerie les dispositions de l'article 27 de la LOPPSI votée en 2011 (art. 2371-1 du code de la défense) donnant possibilité, sous certaines conditions, de faire usage d'une « identité d'emprunt ou d'une fausse qualité ». Les agents de la SDIG opérant en milieu ouvert, il ne paraît pas opportun de leur étendre cette protection.

20. Les « sources » qui concourent à la réalisation d'une mission de sécurité en collaborant avec les services de renseignement **doivent être juridiquement protégées** en leur conférant, en cas de besoin et à titre temporaire uniquement et ce sous l'autorité du chef de mission, différents types de protection offerts dans un cadre judiciaire : l'anonymat (en s'inspirant du code monétaire et financier[59]) ou la protection du témoin sous X (sur la base des règles du code de procédure pénale[60]).

21. Les rapports parlementaires Urvoas et Cavard du printemps 2013 ont tous deux estimé que les 1840 interceptions de sécurité autorisées étaient insuffisantes et qu'il appartenait au gouvernement d'en augmenter « significativement »[61] le nombre. Dans le vingtième rapport de la CNCIS pour la période 2011-2012, la commission avait au contraire estimé que ce chiffre ne devait pas être dépassé. Dans la mesure où les « interceptions de sécurité » sont une atteinte, légale depuis 1991, à la liberté individuelle, il importe que l'ampleur et le volume soient portés à la connaissance de la représentation nationale : il faut donc inviter le gouvernement à informer les commissions des lois **de l'Assemblée nationale et du Sénat,** ainsi que la future commission parlementaire, **de toute décision d'augmentation du nombre de ces interceptions.**

---

[59] *Cf.* article L 561-24 al. 1.

[60] *Cf.* les articles 706-58 et 706-59.

[61] Christophe Cavard et Jean-Jacques Urvoas, *Suivi et surveillance des mouvements radicaux armés. Commission d'enquête,* Assemblée nationale, n° 1956, 2013, p. 49.

22. Il faut **encourager la CNCIS à publier** dans son rapport **annuel les indications chiffrées sur les demandes d'interception de sécurité non pas seulement par ministère mais pour chaque service** en les croisant avec les cinq motifs légaux définis en 1991.

23. Dans le même esprit, il faudrait **inviter la future personnalité qualifiée,** désignée au terme de l'article 20 de la LPM 2014 **à publier des agrégats statistiques annuels.**

24. Les « flux internet » lorsqu'ils caractérisent les échanges de courriels ou la voix sur IP, sont une correspondance et relèvent donc de la loi de 1991 dont la CNCIS est l'autorité de contrôle. Il importe donc de rappeler, ne serait-ce que pour dissiper les idées de surveillance généralisée, qu'aucune interception de communication entre deux personnes ne peut être pratiquée en dehors du cadre de cette loi.

25. La loi de 1978 « informatique et libertés » d'intention libérale qui plaça la France en avance en Europe fut en son temps une source d'inspiration pour plusieurs pays européens ainsi que pour l'UE (pour la directive de 1995). Elle demeure aujourd'hui un élément particulièrement important du dispositif de protection des libertés en France. Mais l'organisme de contrôle qui en est issu, la **CNIL,** doit être confortée, ses pouvoirs renforcés et ses moyens accrus. Il paraît très important qu'elle puisse jouer son rôle de vigie des libertés publiques en poursuivant une activité d'information du public en publiant **deux indicateurs : un agrégat annuel par ministère des pratiques d'interconnexion de fichiers**[62] **et un état annuel non détaillé du nombre de fichiers et de traitements automatisés de données à la disposition des services de renseignement,** qu'ils soient « spécialisés » ou appartiennent au « second cercle ». Ces deux indications statistiques ne fragiliseraient pas le travail des services et contribueraient à **dissiper les nombreux fantasmes,** notamment celui de leur omniscience et de leur omnipotence. Il s'agirait d'une étape importante en vue d'instaurer un climat de confiance entre les citoyens et les « services ». Le groupe de travail sur les fichiers présidé par Alain Bauer avait fait en 2007 une œuvre pionnière et très utile dans cet esprit et dans un cadre plus large puisqu'il s'agissait de recenser l'ensemble des fichiers (au

[62] Il importe de préciser qu'en soi les pratiques d'interconnexion sont parfois nécessaires à l'activité de certaines administrations et qu'elles ne sont pas systématiquement attentatoires aux libertés publiques.

nombre de 33) utilisés par la police et de gendarmerie[63]. Ce type de mesure permettrait de faire reculer les préjugés et d'instaurer une relation de confiance. Dans cet esprit, Facebook et Google, afin de restaurer la confiance envers leurs usagers après le scandale Prism, ont publié en ligne les chiffres des requêtes des différents gouvernements concernant les données des utilisateurs. La vogue des « rapports de transparence » s'étend aujourd'hui à de nombreux fournisseurs d'accès et opérateurs de téléphone dans le monde. L'État ne peut ignorer ce mouvement.

26. Enfin une réflexion doit être engagée sur la **possibilité d'établir pour la CNIL les moyens de s'assurer qu'il n'y a pas de détournement des finalités** (qui est une infraction pénale[64]) **dans l'usage des fichiers** des services de renseignements, dans le cadre du décret n°2007-914 du 15 mai 2007 qui limite considérablement les pouvoirs de l'autorité administrative indépendante (à l'encontre de l'esprit et du texte de la loi de 1978).

27. Il paraît utile de réfléchir à la création d'un **Observatoire public de la classification (OPC) rattaché au SGDSN** qui pourrait s'inspirer du principe du *National Declassification Center* (NDC) créé en 2009 aux États-Unis. Toutefois, à la différence du NDC, l'observatoire français ne procéderait pas à la déclassification des documents, prérogative qui doit demeurer entre les mains de l'autorité ayant classifié. Cet observatoire aurait pour tâche de tenir un état statistique annuel du nombre de documents classifiés par ministère. L'OPC, rattaché au Premier ministre, serait composé d'une équipe très réduite, à l'image de la CCSDN ou de la CNCIS, avec des niveaux d'habilitation élevés. L'activité d'observation serait conduite par des juges administratifs détachés à l'OPC qui pourraient procéder à des sondages dans les différentes administrations afin de s'assurer que les documents ont été classifiés pour des motifs relevant effectivement du secret de la défense nationale et avec le niveau de classification approprié. Ils s'assureraient enfin que chaque ministère conserve à jour un document de synthèse établissant la liste des documents classifiés, le nom de l'autorité ayant procédé à la classification ainsi que la date de cette opération. Ainsi pourrait-il produire un état statistique annuel qui favoriserait la dissipation des préjugés et rapprocherait les citoyens avec leurs administrations, ce qui est depuis plus d'une dizaine d'années un objectif constamment affirmé dans le cadre de la réforme de l'État.

---

[63] *Cf.* Alain Bauer et Christophe Soullez, *Fichiers de police et de gendarmerie. Comment améliorer leur contrôle et leur gestion ?,* Paris, La Documentation française, 2007, 145 p.

[64] *Cf.* L'article 226-21 du code pénal.

28. Dans le même esprit, il faudrait confier à l'OPC le soin de **s'assurer de la mise en œuvre effective de l'article 46** de l'IGI 1300, **prévoyant** que **« la révision du besoin et du niveau de classification des informations ou supports** doit être effectuée rigoureusement **selon une périodicité inférieure ou égale à dix ans,** précisément définie par chaque ministre pour le département dont il a la charge ».

29. Il importe de faire évoluer le principe de l'instruction interministérielle « 1300 » du SGDSN sur le point particulier de la durée d'un document classifié : **un texte réglementaire de portée interministérielle devrait mentionner des durées automatiques de déclassification selon les trois niveaux existants** en les faisant correspondre aux délais que la loi sur les archives publiques de 2008 fixe pour l'ouverture des archives (25, 50 et 75 ans). La correspondance entre la règlementation en matière de protection du secret et le droit des archives publiques permettrait ainsi de mettre un terme à l'existence d'une catégorie de documents administratifs hors du droit commun, tout en préservant un secret indispensable. Cette correspondance ne ferait d'ailleurs que revenir à ce que disait l'instruction 1 300 dans la version en vigueur de 2003 à 2011…

3.4. CLARIFIER LES RÈGLES ET LES PRATIQUES DANS LA « CINQUIÈME DIMENSION » AU SERVICE DE LA SOUVERAINETÉ

Un des progrès incontestable des deux derniers siècles a été l'émergence d'un droit des conflits armés qui a rendu réelle l'idée de « guerre réglée », mais la cinquième dimension est un monde naturellement déréglé où les affrontements sont quotidiens et intenses… Dans ce cadre très incertain qu'est le monde cybernétique, l'effort de réflexion préalable est d'une importance majeure afin d'adopter ensuite des mesures pratiques adaptées au plan national, comme dans des négociations internationales. Cet effort doit être l'occasion de former une communauté épistémique rassemblant ingénieurs réseaux et télécom, militaires, fonctionnaires de police mais aussi le monde académique spécialisé sur les questions de sécurité, relevant aussi bien des sciences exactes que des sciences sociales. La transversalité est, sur cette dimension très particulière, absolument indispensable.

Mieux comprendre le « nouveau monde »

30. L'effort de réflexion doit porter en premier lieu sur la compréhension de ce qu'est le cyberespace : comme d'autres États, la France en est encore au stade des « grandes découvertes » avec des cartes aléatoires et des boussoles incertaines. En effet, la diversité des acteurs est grande et la compréhension de leurs stratégies souvent obscure. Il faut donc **mener des recherches de fond** en mobilisant principalement les ressources de la recherche publique en sciences sociales **sur la cartographie des acteurs du cyberespace** afin **d'identifier les lieux réels de pouvoir et de décision** pour pouvoir ensuite **alimenter une réflexion sur les stratégies des différents acteurs.** L'enjeu est de faciliter le positionnement la France dans les négociations « multi-acteurs » qui sont bien différentes des négociations « multilatérales » classiques.

31. La France doit poursuivre ses efforts à l'international pour **faire prévaloir l'esprit de la Charte des Nations Unies en matière cybernétique,** notamment sur les enjeux importants : comment caractériser une action hostile en matière cybernétique : est-ce une « agression armée » ? Un « recours à la force » ? Une action criminelle ? Quels sont les contours de la légitime défense ?

32. Quelle est la contrepartie de l'abandon de souveraineté (numérique) que représente la migration des données européennes ? A l'heure où la directive UE sur les données est en cours de refonte, la France doit adopter en Europe une attitude résolue afin d'amener l'UE à **faire un examen précis des bénéfices pour l'UE et pour la France des accords « Safe Harbour » et « Swift 2 » signés avec les États-Unis.**

Mesures pratiques réglementaires et juridiques

33. Il est possible de **renforcer la cyber-sécurité** des « opérateurs d'importance vitale » **(OIV) par une centralisation effective de leurs processus de protection** au niveau gouvernemental (SGDSN-ANSSI).

34. La LPM 2014-2019 a franchi un cap important en matière de sécurité, en disposant par son article 22 que les OIV ont une obligation de déclaration d'incident affectant leur système d'information. Ce qui est en jeu est en fait plus que la défaillance d'une entreprise particulière. Dans ce cadre il faut donc

assurer un contrôle de l'obligation de déclaration d'incident des OIV auprès de l'ANSSI.

35. Le **code pénal** est un outil solide de lutte contre la cybercriminalité, mais il n'est pas parfaitement adapté. Il faudrait **le modifier afin de faire du vol de données informatiques qui est en pratique une copie de données sans soustraction à son propriétaire, un vol authentique.**

36. Il faut **rendre publique une évaluation statistique annuelle des attaques cybernétiques** dont les administrations et acteurs publics sont l'objet **par un chiffre global** et ventilé par types d'attaques. Il paraît à ce stade important de ne pas être plus précis afin de ne pas accroître les faiblesses.

37. En ce qui concerne l'interception des flux Internet, la loi de 1991 constitue une base juridiquement très solide. Un débat doit donc être engagé sur la différence d'application de la loi entre les citoyens français et les autres et afin de trouver des critères compatibles avec les moyens techniques. Un échange doit donc avoir lieu **entre représentants de la DGSE, juristes, magistrats judiciaires et administratifs. Au terme de ce débat non public, une information devrait être donnée aux commissions parlementaires** compétentes sur les enjeux de libertés publiques et de défense.

38. Il faut **inviter l'état-major des armées à informer les commissions compétentes des assemblées des grandes lignes du « concept » et de la « doctrine » interarmées de cyberdéfense** adoptées en juillet 2011 et janvier 2012. Ceci permettrait notamment de conforter les moyens budgétaires dans un environnement où ils seront à l'avenir soumis à décrue.

39. De même, il faudrait **clarifier auprès d'elle les règles d'emploi du cyber-offensif** – ainsi que cela avait été clairement préconisé dans le *Livre blanc* de 2008. Il importerait notamment de délimiter particulièrement soigneusement où s'arrête la capacité défensive et où commence l'action offensive dans la mesure où les règles juridiques sont, par nature, différentes.

Ces deux recommandations permettraient au demeurant de se conformer avec le cinquième des sept « axes d'effort » de la stratégie nationale de cybersécurité de l'ANSSI (2011) qui prévoyait « d'adapter » le droit au monde cyber.

40. Pour la LIO, il paraît difficilement imaginable que l'article 35 de la Constitution sur la discussion au Parlement s'applique et que la France invoque le chapitre VII de la Charte des Nations Unies, car il ne peut s'agit que d'une guerre secrète. Un effort a été initié en vue d'adapter le droit pénal à la conduite des opérations militaires et a été traduit dans la LPM 2014 qui modifie un certain nombre de dispositions des codes de procédure pénale, de la justice militaire et de la défense... On pourrait penser que l'offensif relève de la capacité donnée à la DGSE « d'entraver, hors du territoire national » par l'article 2 du décret n° 82-306 du 2 avril 1982 qui l'a fondé. Encore faut-il noter dans ce texte que cette capacité d'entrave doit être dirigée contre des tentatives « d'espionnage ». Sans écorner le choix de la stratégie dissuasive qui semble avoir été fait, **une réflexion doit également être engagée dans un cadre non public sur le cadre juridique du cyber-offensif.**

L'indispensable engagement dans une co-production publique et privée de souveraineté en matière de confiance et de sécurité

41. Face à la domination de matériels et de logiciels étatsuniens sur le marché mondial, il y a urgence à **engager une politique de long terme afin de renforcer la souveraineté cybernétique et numérique.**

Dans l'esprit de co-production évoqué plus haut, le secteur privé pourrait en tirer profit. Développer une industrie numérique de souveraineté passe avant tout par le renforcement du secteur informatique en France sur l'ensemble du spectre, hardware et software. Le hardware est particulièrement important et notamment en ce qui concerne les *clouds* et les routeurs dominés par les États-Unis (Cisco) et la Chine (Huawei et STE). La recherche d'une souveraineté numérique réelle repose sur l'hébergement sécurisé des données par des *clouds* souverains, par des routeurs de cœur de réseau, par des processeurs nationaux d'une part, et d'autre part, par des capacités de sécurité renforcées avec des firewalls, des sondes souveraines pour la chaîne de détection d'attaques, enfin par des capacités cryptologiques, domaine dans lequel la France a, dans la durée, des compétences d'excellence. En matière de sécurisation des données, la solution des *clouds* souverains doit également être fortement encouragée : lancés en 2012 avec l'aide de la Caisse des Dépôts, ils ont fait l'objet d'investissements limités – deux *clouds* à 75 M€ chacun – si on les rapporte à l'enjeu essentiel

qu'ils représentent. Il importe cependant de ne pas décourager le financement des *clouds* privés pour peu qu'ils soient situés sur le territoire français. Une autre piste sur laquelle il faut investir est celle de la cryptologie sur le trafic en temps réel qui n'est pas exclusive des *clouds*.

42. Le financement de la recherche publique en matière de cybersécurité et de confiance qui passe principalement par la DGA et les appels à projet de l'Agence nationale de la recherche, **doit être augmenté de façon notable.**

3.5. CONDUIRE UNE RÉFLEXION DE NATURE STRATÉGIQUE ET PROSPECTIVE SUR LES ACTIVITÉS DE RENSEIGNEMENT

43. C'est l'appréhension des menaces, des risques et des atteintes qui rend légitime les services afin qu'ils puissent servir d'aide à la décision pour le pouvoir exécutif. Le bouleversement stratégique post-1991, qui a permis de valoriser le renseignement, a fait évoluer la réflexion sur les dangers : on est ainsi passé dans la décennie 1991-2001 d'un monde incertain[65] à un monde désormais certain que le danger était quasiment exclusivement terroriste. La France n'a pas échappé à ce mouvement de fond qui lui a permis de renforcer une législation antiterroriste *ad hoc* et d'adopter un discours public valorisant désormais presque exclusivement la menace terroriste, l'absence d'agression terroriste sur le territoire français étant la preuve implicite de l'efficacité des services de renseignement. La logique des services étant d'anticipation et de non-publicité, il n'est pas possible d'évaluer plus de dix ans après la nécessité de continuer à valoriser le « tout-antiterrorisme ». Pourtant, l'affaire Prism a révélé en 2013 que parmi les « alliés » luttant quotidiennement contre la menace terroriste, la compétition économique ne cessait de s'accentuer, menant à des actions d'ingérence et d'espionnage. Dans ce cadre nouveau, **il est à souhaiter que les divers lieux et structures de réflexion stratégique permettent de contribuer – au bénéfice du pouvoir exécutif – à la réflexion sur la nature des menaces en aidant à discriminer les formes les plus aigües** (espionnage, ingérence, terrorisme), qui pour ne pas être toujours nouvelles, pourraient néanmoins s'avérer cruciales. De même, il paraît peut-être utile de ne plus systématiquement

[65] Ainsi que l'atteste très nettement le *Livre Blanc* de 1994.

privilégier les menaces portées par les acteurs non-étatiques. Par ailleurs, un certain nombre d'enjeux particuliers devraient être pris en compte de façon spécifique : la croissance exponentielle de l'information ouverte ou encore l'enjeu cybernétique et numérique constituant en effet des défis pour les services de renseignement. À cet égard, **la recherche française publique sur les questions de sécurité internationale** dans le cadre de la stratégie nationale pour la recherche et l'innovation (SNRI) **doit être mobilisée pour éclairer les choix stratégiques et orienter l'activité des services de renseignement** afin de préparer l'avenir.

Engager la réforme culturelle du renseignement

44. La **vision nettement négative que la population française a du renseignement n'est pas une fatalité.** Si les services suscitent sans difficulté des vocations, l'objectif d'une transformation de son image est de favoriser une disposition favorable à l'égard des services, dans la population dans son ensemble, mais aussi auprès des élus nationaux et de la haute fonction publique. L'objectif principal doit être de **faire disparaître l'assimilation des services à la surveillance de l'opinion.** Ceci paraît tout particulièrement important dans un contexte économique où le budget des services risque de ne pouvoir être sanctuarisé très longtemps. C'est donc un effort d'ensemble qu'il faut mener, celui d'une **véritable réforme culturelle du renseignement.** Il ne peut s'agir d'une perspective de court terme, mais d'un effort inscrit dans la durée qui est la seule échelle réaliste pour transformer les mentalités.

45. Dès lors il importe pour **chaque agence d'accroître la confiance** et, pour ce faire, de penser **une** authentique **politique de communication externe** avec des objectifs proportionnels à ses moyens et sa taille et surtout adaptés à son environnement administratif et juridique singulier.

46. Cette action doit être prolongée à un autre niveau afin **de mettre en place un véritable *public intelligence* dont l'objet doit être de faire connaître au public les grands objectifs stratégiques des services** et d'expliquer ainsi leur participation à la mission de sécurité. Il serait possible dans cet esprit d'élaborer un document public définissant la Stratégie nationale du renseignement (SNR), issu du Plan national d'orientation du renseignement (PNOR) qui n'est logiquement pas rendu public. Les pays anglo-saxons ont procédé de la

sorte sans que cela fragilise leur sécurité. On observe d'ailleurs qu'il existe des précédents en France qui ont été bénéfiques : en 2011, l'ANSSI a publié la Stratégie gouvernementale en matière de sécurité des systèmes d'information et, plus récemment, la publication de la *Synthèse nationale de renseignement déclassifié* du 3 septembre 2013 sur l'usage d'armes chimiques par le gouvernement syrien.

47. La France souffre d'une faiblesse importante qui est l'absence d'une réflexion sur l'analyse, métier qui est pourtant au cœur des services de renseignement. La réforme – de nature administrative – des corps de la DGSE qui a eu lieu en 2010 a été une première étape majeure. Il importe désormais de passer à une seconde étape en **s'interrogeant pour l'ensemble des services sur les savoirs et les disciplines mobilisés dans la formation initiale des analystes, formés essentiellement par l'Université et les IEP.** Les services doivent tisser des liens avec ce monde académique pour évaluer les savoirs dont les analystes ont besoin. Cette réflexion est très poussée dans des pays anglo-saxons et dans d'autres pays européens. Le modèle du concours administratif français n'est peut-être pas le plus approprié pour sélectionner des analystes qui mobiliseront leurs compétences sur le vaste monde. Une réflexion sur la part des sciences sociales (anthropologie, sociologie, histoire principalement) dans la formation des analystes paraît également particulièrement opportun.

48. Il faut également **renforcer** l'organisme de formation qu'est **l'Académie du renseignement en la dotant,** aux côtés du comité pédagogique et du comité d'orientation et d'évaluation, composés uniquement de hauts fonctionnaires représentant les services, **d'un conseil de perfectionnement composé d'universitaires** compétents dans les disciplines et les savoirs participant à la formation des analystes des exploitants, universitaires, dont le métier est de transmettre des savoirs appliqués et fondamentaux. Les missions de ce conseil viseraient à contribuer au choix des intervenants et à assurer un lien avec la recherche universitaire à la fois pour se prononcer sur le contenu des enseignements en fonction des besoins exprimés par les services et pour mener une réflexion sur la possibilité de mobiliser la recherche au profit des services.

CONCLUSION

Depuis leur origine les administrations publiques du renseignement se sont développées de façon autonome au sein de l'État, à l'abri de tout regard extérieur. Cette situation a changé tardivement en France. Ainsi, récemment, sur fond d'une réforme majeure du renseignement, l'auto-censure des élus s'est affaiblie et les enceintes parlementaires se sont enfin saisies d'un enjeu majeur touchant à la sécurité des citoyens, à leurs libertés et à l'équilibre des pouvoirs – en un mot à ce qui constitue la démocratie libérale. Ce rapport est une contribution à un débat qui s'esquisse publiquement à peine en France.

Le lien entre renseignement et sécurité étant principalement d'ordre préventif, les conséquences de l'action des services sont peu visibles, d'où une méconnaissance de l'action des services, renforcée par le recours naturel à la classification de l'information. Le renseignement est pourtant sorti de l'ombre en 2008 par une volonté politique qui a fait d'une ancienne pratique quotidienne et secrète une nouvelle « fonction stratégique » dans le cadre du *Livre blanc.* Mais **ainsi que nous l'avons montré, une « fonction stratégique » ne fait à pas à elle seule une politique publique.** L'impossibilité logique d'assurer la publicité et un contrôle authentique, analogue aux administrations classiques expliquent en partie seulement ce constat. C'est avant tout parce que le renseignement, pris dans son ensemble, est en situation de balkanisation, parce que les normes juridiques sont dispersées et parfois imprécises, parce qu'il n'y a pas de pilotage budgétaire incluant l'ensemble des acteurs du renseignement public au-delà des « services spécialisés ».

Les « services » sont indispensables pour la sécurité des citoyens : il faut les renforcer, mais aussi les contrôler. Leurs modes d'action sont singuliers : il faut les préserver, dans le cadre de la loi votée par le Parlement. Le secret est indispensable pour l'État : face aux désirs de transparence, il faut le garantir, mais aussi le réguler. Les dépenses publiques en matière de renseignement constituent pour la sécurité des citoyens un investissement. C'est pour cette raison que l'effort financier en la matière doit être au moins maintenu dans les années à venir, en dépit d'un contexte qui va affecter très fortement l'ensemble des dépenses publiques.

Pierre Joxe qui fut ministre de l'Intérieur et ministre de la Défense et comme tel, qui eut une connaissance des services policiers et militaires de renseignement, indiquait il y a quelques années cette évidence : « […] les services de renseignement n'administrent pas un service public […] au service des citoyens [ils sont] au service

du pouvoir »[66]. Il faut se rappeler cette évidence pour bien comprendre la singularité des services dans une démocratie libérale. On pourrait toutefois prolonger ce propos en le nuançant et indiquer que s'ils ne sont pas un service public, ils rendent un « service au public » en assurant sa sécurité. De multiples évolutions juridiques sont possibles pour continuer d'accommoder un « État secret », constitué en France à partir du XIX^{e} siècle, aux règles de la démocratie libérale et de l'État de droit. Les situations étrangères ne peuvent pas être transposées en bloc et hors-sol, mais un certain nombre de recommandations formulées ici s'inspirent de mesures précises mises en œuvre dans des pays voisins confrontés aux mêmes enjeux que la France. Enfin, prolonger la réforme organisationnelle et juridique du renseignement par une réforme culturelle permettra d'instaurer de la confiance à l'égard des services en lieu et place des fantasmes et des préjugés.

[66] P. Joxe lors d'un entretien avec FI. Vadillo le 26 septembre 2007, cité dans : F. Vadillo, *Les socialistes et les services de renseignement et de sécurité de 1981 à 2007 : usage et politisation de l'administration du renseignement,* mémoire de Master 2, Université de Bordeaux 3, 2008, p. 29.

REMERCIEMENTS

Tout au long de cette étude dont la réalisation a duré plus de dix mois, j'ai bénéficié de la confiance de l'Institut Montaigne : je souhaite adresser en premier lieu mes remerciements à son Président, M. Claude Bébéar, ainsi qu'à son directeur, M. Laurent Bigorgne et à sa directrice adjointe, Mme Alexia de Monterno.

La disponibilité et l'ouverture d'esprit des 51 personnalités que j'ai pu rencontrer et interroger, parfois à plusieurs reprises, ont été une condition indispensable à la réalisation de ce rapport. Je leur en exprime ma profonde reconnaissance, en particulier aux directeurs des « services spécialisés ».

Ce document a bénéficié de l'expertise inlassable pour la mise en forme de Michel Courty et de la relecture attentive d'« Amby », ainsi que de plusieurs collègues et amis travaillant dans des disciplines différentes : Philippe Claret, Philippe Guillot, Yann Raison du Cleuziou, Pierre Razoux, Amable Sablon du Corail. Que chacun d'entre eux soit vivement remercié.

LISTE DES TABLEAUX, GRAPHES ET FIGURES

LISTE DES SIGLES ET ACRONYMES

CCSDN	Conseil de défense et de sécurité nationale
CNR	Conseil national du renseignement
DCRI	Direction centrale du renseignement intérieur
DGA	Direction générale de l'armement
DGGN	Direction générale de la gendarmerie nationale
DGSE	Direction générale de la sécurité extérieure
DGSI	Direction générale de la sécurité intérieure
DNRED	Direction nationale du renseignement et des enquêtes douanières
DPR	Délégation parlementaire au renseignement
DPSD	Direction de la protection et de la sécurité de la défense
DRM	Direction du renseignement militaire
LIO	Lutte informatique offensive
LOPPSI	Loi d'orientation et de programmation pour la performance de la sécurité intérieure
LPM	Loi de programmation militaire
OIV	Opérateur d'importance vitale
RGPP	Renseignements généraux de la Préfecture de police
RIM	Renseignement d'intérêt militaire
SDIG	Sous-direction de l'information générale
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SIRASCO	Service d'information, de renseignement et d'analyse stratégique de la criminalité organisée
TRACFIN	Traitement du renseignement et action contre les circuits financiers clandestins

ANNEXES

ANNEXE 1 : LES TEXTES EUROPÉENS RELATIFS AUX SERVICES DE RENSEIGNEMENT

- Convention européenne des droits de l'homme, 4 novembre 1950.
- Assemblée parlementaire du conseil de l'Europe, Recommandation n° 1402, 26 avril 1999.
- Parlement européen, Résolution 2001/2098 (INI), 5 septembre 2001.
- Assemblée de l'UEO, Résolution n° 113, 4 décembre 2002.
- Assemblée parlementaire du Conseil de l'Europe, Recommandation n° 1713, 23 juin 2005.
- Commissaire européen pour la justice, la liberté et la sécurité, *Accountability of the Intelligence and Security Agencies and Human Rights, International Symposium,* The Hague, 7 juin 2007.
- Assemblée parlementaire du Conseil de l'Europe, Résolution n° 1838, 6 octobre 2011.

ANNEXE 2 : LA NOTION D'« INTÉRÊTS FONDAMENTAUX DE LA NATION »

Article 410-1 du Code pénal :

« Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel ».

LISTE DES PERSONNES AUDITIONNÉES

- M. Loïc ABRIAL, chargé de mission à la CNCIS
- M. l'Ambassadeur Bernard BAJOLET, directeur général de la DGSE
- M. Bernard BARBIER, conseiller spécial du président-directeur général de Sogeti
- M. Jacques BELLE, ancien président de la Commission consultative du secret de la défense nationale (CCSDN)
- M. Laurent BLOCH, ancien responsable de la sécurité des systèmes d'information de l'INSERM, chercheur à l'IFAS
- M. le Professeur Pierre BODEAU-LIVINEC, professeur de droit international, Université Paris VIII
- M. le général de corps d'armée Jean-Pierre BOSSER, directeur de la DPSD ;
- Dr Yérom-David BROMBERG, maître de conférences en informatique, Université de Bordeaux
- M. Didier BRUGERE, directeur des relations institutionnelles et de l'Intelligence économique, Thales
- Me Bernard CARAYON, ancien député du Tarn
- M. Jean-Baptiste CARPENTIER, directeur de TRACFIN
- M. le colonel de gendarmerie Pierre CASAUBIEILH, commandant le CNEFG
- M. le Vice-amiral Arnaud COUSTILLIERE, officier général à la Cyberdéfense, état-major des armées
- M. le Conseiller d'État Serge DAËL, président de la Commission d'accès aux documents administratifs (CADA)
- M. le député Arnaud DANJEAN, président de la sous-commission « sécurité et défense » au Parlement Européen
- M. Michel DEBACQ, avocat général à la Cour de Cassation
- M. le général Jean-Louis DESVIGNES (2S), vice-président de l'Institut Fredrik R. Bull
- M. Francis DONNAT, directeur des politiques publiques, Google France
- M. le général de corps d'armée Bruno ELIE (2S), ancien directeur de la DRM

- M. le colonel Eric FREYSSINET, chef de la division de lutte contre la cybercriminalité, ministère de l'Intérieur
- M. Émile GABRIÉ, adjoint au chef du service des affaires juridiques de la CNIL
- Enseigne de vaisseau Mélodie GALLANT, état-major des armées-Cyber
- M. Jean-Paul GARCIA, directeur central de la DNRED
- M. Emmanuel de GIVRY, conseiller honoraire à la Cour de Cassation, vice-président de la CNIL
- M. le général de corps d'armée Christophe GOMART, directeur de la DRM
- M. Olivier GUÉRIN, délégué général de la CNCIS
- Dr Philippe GUILLOT, maître de conférences en mathématiques, Université Paris VIII
- M. Hervé GUILLOU, président du Conseil des industries de confiance et de sécurité (CICS)
- M. Philippe HAYEZ, conseiller maître à la Cour des comptes, ancien directeur du renseignement adjoint à la DGSE
- M. Alain JUILLET, Senior Advisor chez Orrick-Rambaud-Martel, ancien directeur du renseignement à la DGSE
- M. le colonel Hervé KEMPF, OTAN, division « défis de sécurité émergents »
- M. le professeur Wolfgang KRIEGER, université de Marburg
- Mme Sophie KWASNY, chef de l'unité de protection des données, Conseil de l'Europe-Strasbourg
- M. le général de corps d'armée aérien Jean-Marc LAURENT (2S), Aeris – Aerospace and Defence
- M. Florian MAGANZA, Senior Policy Analyst-Relations institutionnelles, Google France
- M. David MARTINON, représentant spécial pour la société de l'information, ministère des Affaires étrangères
- M. le général de corps d'armée aérien Michel MASSON, ancien directeur de la DRM
- M. l'inspecteur général de la police nationale Thierry MATTA, directeur adjoint du renseignement intérieur, DCRI

- M. Stanislas de MAUPEOU, directeur consulting cybersécurité et évaluation-Thales
- M. Jean-Yves MONFORT, magistrat, Conseiller à la Cour de Cassation
- Me Olivier MORICE, avocat à la Cour
- M. Alexandre PAPAEMMANUEL, responsable du compte « renseignement », Airbus Defense & Space
- M. Bernard PÊCHEUR, conseiller d'État
- M. Guy RAPAILLE, avocat général près la Cour de Liège, président du comité permanent de contrôle des services de renseignement et de sécurité (Belgique)
- M. Nicolas REVELLO, adjoint au chef du service des contrôles de la CNIL
- Mme Delphine REYRE, directrice des affaires publiques France et Europe du Sud-Facebook
- M. Luc-François SALVADOR, président-directeur général de Sogeti
- M. Benoît TABAKA, Public Policy Manager, Google France
- Dr Hamadoun I. TOURÉ, secrétaire général de l'Union Internationale des Télécommunications, Genève
- Dr Jean-Jacques URVOAS, député du Finistère, président de la Commission des Lois de l'Assemblée nationale
- M. Floran VADILLO, conseiller du président de la Commission des Lois, Assemblée Nationale
- Dr Daniel VENTRE, CNRS, titulaire de la chaire Sogeti-Thales de cybersécurité et de cyberdéfense
- M. Thorsten WETZLING, Senior Research Fellow, Brandenburgisches Institut für Gesellschaft und Sicherheit, Potsdam

SOURCES ET BIBLIOGRAPHIE

1. SOURCES

- Colloque : « Le droit et l'éthique face aux défis de la cyber-conflictualité », Ecole Militaire-Paris, CREC-Chaire Sogeti Thales, 8 octobre 2013.
- 6e Forum international de la cybersécurité, Lille, 21-22 janvier 2014.
- « After Snowden : Using Law and Technology to counter snooping. An expert colloquy to mark data protection day » , Council of Europe-Strasbourg, 28 janvier 2014.
- Forum de la Gouvernance Internet, Conseil économique, social et environnemental, 10 mars 2014.

Documents officiels français :

- *Défense et sécurité nationale. Livre blanc,* Paris, Odile Jacob-La Documentation française, 2008, 350 p.
- Défense et sécurité des systèmes d'information. Stratégie de la France, Paris, ANSSI, 2011, 22 p.
- *Livre blanc. Défense et sécurité nationale,* Paris, ministère de la Défense, 2013, 160 p.
- *La Nouvelle France industrielle*, Paris, ministère du Redressement productif, 2013, 75 p.
- *Pacte Défense Cyber : 50 mesures pour changer d'échelle,* Paris, ministère de la Défense-Dicod, 2014, 22 p.

Rapports des autorités administratives indépendantes :

- CNIL :
  - CNIL, *Rapport d'activité 2011,* Paris, La Documentation française, 2011, 102 p.
  - CNIL, *Rapport d'activité 2012,* Paris, La Documentation française, 2012, 98 p.

- CNCIS :
  - *Vingtième rapport d'activité 2011-2012 de la Commission nationale de contrôle des interceptions de sécurité,* Paris, La Documentation française, 2012, 205 p.
  - *Vingt-et-unième rapport d'activité 2012-2013 de la Commission nationale de contrôle des interceptions de sécurité,* Paris, La Documentation française, 2013, 178 p.
- CCSDN :
  - Rapport *de la commission consultative du secret de la défense nationale,* Paris, La Documentation française, 2001, 67 p.
  - *Rapport de la commission consultative du secret de la défense nationale 1998-2004,* Paris, La Documentation française, 2005, 281 p.
  - *Rapport de la commission consultative du secret de la défense nationale 2001-2003,* Paris, La Documentation française, 2003, 125 p.
  - *Rapport de la commission consultative du secret de la défense nationale 2005-2007,* Paris, La Documentation française, 2007, 178 p.
  - *Rapport de la commission consultative du secret de la défense nationale 2007-2010,* Paris, La Documentation française, 2010, 255 p.

Rapports de Tracfin :

- Tracfin, *Rapport d'activité 2011,* Paris, Ministère de l'économie et des finances, 2012, 120 p.
- Tracfin, *Rapport annuel d'analyse et d'activité 2012,* Paris, Ministère de l'économie et des finances, 2013, 128 p.

Déclarations et documents normatifs européens :

- SEAE, *Communication conjointe au Parlement européen, au conseil, au comité économique et social européen et au comité des régions. Stratégie de cybersécurité de l'Union Européenne : un cyberespace ouvert, sûr et sécurisé,* 7 février 2013, 21 p.
- *Sécurité nationale et jurisprudence européenne,* CEDH-Conseil de l'Europe, 2013, 46 p.

• *Handbook on European data Protection Law, Council of Europe-European Court of Human Rights,* 2014, 210 p.

Documents officiels étrangers :

(ordre chronologique)

• *National Intelligence Machinery,* London, The Stationery Office, 2000, 39 p.

• Office of the Director of National Intelligence, *Intelligence Community Legal Reference Book,* ODNI, Summer 2009, 938 p.

• International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, Washington, The White House, May 2011, 25 p.

• Presidential Policy Directive/PPD-20 on US Cyber Operations Policy, October 16th, 2012, 18 p. (https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf) .

• The President's Review group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World,* 12 December 2013, 304 p.

Rapports parlementaires et auditions des commissions parlementaires sur le renseignement :

(ordre chronologique)

• *Rapport fait au nom de la commission des finances, de l'économie générale et du plan sur le projet de loi de finances pour 2003, annexe n° 36,* Assemblée nationale n° 256, 10 octobre 2002, 40 p. [Bernard Carayon].

• *Rapport fait au nom de la commission des finances, de l'économie générale et du plan sur le projet de loi de finances pour 2006, annexe n° 9,* Assemblée nationale n° 2568, 10 octobre 2005, 47 p. [Bernard Carayon].

• *Rapport fait au nom de la commission des finances, de l'économie générale et du plan sur le projet de loi de finances pour 2007, annexe n° 9,* Assemblée nationale n° 3363, 12 octobre 2006, 48 p. [Bernard Carayon].

• *Rapport fait au nom de la commission des finances, de l'économie générale et du plan sur le projet de loi de finances pour 2008, annexe n° 9,* Assemblée nationale n° 276, 11 octobre 2007, 103 p. [Jean-Michel Fourgous].

- *Rapport fait au nom de la commission des finances, de l'économie générale et du plan sur le projet de loi de finances pour 2009, annexe n° 10,* Assemblée nationale n° 1198, 16 octobre 2008, 85 p. [Jean-Michel Fourgous].
- *Rapport fait au nom de la commission des finances, de l'économie générale et du plan sur le projet de loi de finances pour 2010, annexe n° 10,* Assemblée nationale n° 1967, 14 octobre 2009, 83 p. [Jean-Michel Fourgous].
- *Rapport fait au nom de la commission des finances, de l'économie générale et du plan sur le projet de loi de finances pour 2011, annexe n° 10,* Assemblée nationale n° 2857, 14 octobre 2010, 81 p. [Jean-Michel Fourgous].
- *Rapport fait au nom de la commission des finances, de l'économie générale et du plan sur le projet de loi de finances pour 2012, annexe n° 10,* Assemblée nationale n° 3805, 12 octobre 2011, 83 p. [Jean-Michel Fourgous].
- *Avis présenté au nom de la commission des affaires étrangères, de la défense et des forces armées sur le projet de loi de finances pour 2013, tome V : défense : environnement et prospective de la politique de défense,* Sénat n° 150, 22 novembre 2013, 65 p. [Jeanny Lorgeoux et André Trillard].
- Délégation parlementaire au renseignement, *Rapport d'activité 2008-2009,* Assemblée nationale n° 2170, Sénat n° 181, 17 décembre 2009, 16 p.
- Délégation parlementaire au renseignement, *Rapport relatif à l'activité de la Délégation parlementaire au renseignement pour l'année 2011,* Assemblée nationale n° 83, Sénat n° 672, 17 juillet 2012, 12 p.
- Délégation parlementaire au renseignement, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2012,* Assemblée nationale n° 1012, Sénat n° 557, 30 avril 2013, 21 p.
- Délégation parlementaire au renseignement, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2013,* Assemblée nationale n° 1886, Sénat n° 462, 16 avril 2014, 18 p.
- Jean-Jacques Urvoas et Patrice Verchère, *Pour un « État secret » au service de notre démocratie.* Rapport d'information, n° 1022, 2013, 205 p.
- Christophe Cavard et Jean-Jacques Urvoas, *Suivi et surveillance des mouvements radicaux armés. Commission d'enquête,* Assemblée nationale, n° 1956, 2013, 163 p.
- *Compte rendu de la Commission des affaires étrangères,* Assemblée Nationale, 31 mars 2009, n° 47, 10 p.

- *Compte rendu de la Commission de la Défense nationale et des forces armées,* Assemblée nationale, 20 février 2013, n° 56, 9 p.
- *Compte rendu de la Commission de la Défense nationale et des forces armées,* Assemblée nationale, 12 juin 2013, n° 79, 10 p.
- *Compte rendu de la Commission de la Défense nationale et des forces armées,* Assemblée nationale, 16 juillet 2013, n° 86, 13 p.
- *Compte rendu de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République,* Assemblée nationale, 9 octobre 2013, n° 4, p. 2-10.
- *Compte rendu de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République,* Assemblée nationale, 30 octobre 2013, n° 10, p. 2-12.
- Daniel Reiner, Jacques Gauthier et Gérard Larcher, *Rapport d'information fait au nom de la Commission des Affaires étrangères de la défense et des forces armées sur le renforcement des forces spéciales françaises,* Sénat, 14 mai 2014, n° 525, 82 p.

Rapports parlementaires et auditions des commissions parlementaires sur la SSI et la dimension cybernétique

(ordre chronologique)

- Pierre Lasbordes, *La sécurité des systèmes d'information. Un enjeu majeur pour la France.* Rapport au Premier Ministre, Paris, La Documentation française, 2006, 197 p.
- Roger Romani, *Rapport d'information fait au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense,* 8 juillet 2008, n° 449, Sénat, 59 p.
- Jean Marie Bockel, *Rapport d'information fait au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense,* 18 juillet 2012, Sénat, n° 681, 158 p.
- Bruno Sido et Jean-Yves Le Déaut, *Le risque numérique : en prendre conscience pour mieux le maîtriser ?,* Assemblée nationale n° 1221-Sénat n° 721, 3 juillet 2013, OPECST, 109 p.
- *Compte rendu de la Commission de la Défense nationale et des forces armées,* Assemblée nationale, 10 juillet 2013, n° 85, 13 p. [Guillaume Poupard-DGA].

La parole des services et des responsables politiques

(ordre chronologique)

- Philippe Rondot, « Du bon usage des services spéciaux », *Politique internationale,* n° 29, automne 1985, p. 171-181.
- Pierre Joxe, « Défense et renseignement », *Défense Nationale,* juillet 1991, p. 9-21.
- « Le renseignement aujourd'hui ou les nouveaux moyens de la puissance. Entretien avec Rémy Pautrat », Le Débat, n° 68, janvier-février 1992, p. 150-161.
- François Mermet, « Quelques réflexions sur la fonction renseignement », ENA mensuel, n° 236, novembre 1993, p. 10-12.
- Pierre Lacoste, « Une nouvelle stratégie pour le renseignement ? », *Politique étrangère,* 1997, vol. 62, n° 1, p. 83-97.
- « Le renseignement français face au nouveau contexte international : interview du préfet Bernard Gérard », *Renseignement et opérations spéciales,* n° 4, mars 2000, p. 25-38.
- « Entretien avec Pierre de Bousquet de Florian », *Rue Saint-Guillaume,* n° 140, septembre 2005, p. 41-46.
- Michel Masson, « Les défis du renseignement militaire », *Sécurité globale,* n° 4, été 2008, p. 9-18.
- Daniel Martin, « La réforme des services de renseignement civil français », *Sécurité globale,* n° 4, été 2008, p. 63-73.
- Bernard Squarcini, « Les mutations du renseignement intérieur français », *Questions internationales,* n° 35, janvier-février 2009, p. 45-50.
- Erard Corbin de Mangoux, « Les mutations du renseignement extérieur français », *Questions internationales,* n° 35, janvier-février 2009, p. 29-33.
- Bernard Bajolet, « Quelle coordination pour le renseignement national ? », *Les Cahiers de Mars,* n° 198, décembre 2009, p. 17-19.
- Bernard Squarcini, « Le continuum défense-sécurité », *Les Cahiers de Mars,* n° 198, décembre 2009, p. 20-23.
- Erard Corbin de Mangoux, « Les nouveaux défis du renseignement extérieur », *Les Cahiers de Mars,* n° 198, décembre 2009, p. 24-26.

- Benoît Puga, « Le renseignement d'intérêt militaire : enjeux et perspectives », *Les Cahiers de Mars,* n° 198, décembre 2009, p. 27-29.
- Michel Masson, « L'avenir du renseignement », *Sécurité globale,* 2009, n° 4, p. 7-20.
- Bernard Bajolet, « Renseignement, l'état de la réforme », *Sécurité globale,* été 2010, n° 12, p. 11-16.
- Louise M. Doyon, « Un an plus tard : le point sur le Programme de liaison-recherche du Service canadien du renseignement de sécurité », *Association internationale des études internationales,* février 2010, 6 p. (https://www.csis-scrs.gc.ca/pblctns/cdmctrch/takngstck-fra.asp).
- Contre-amiral Arnaud Coustillière, « La cyberdéfense: un enjeu global et une priorité stratégique pour le ministère de la défense », *Sécurité globale,* printemps 2013, p. 27-32.
- « Le renseignement », *la Tribune du commissaire,* n° 129, décembre 2013, 29 p.
- « Entretien avec le général Gomart. Le renseignement militaire aujourd'hui », *Stratégique*, janvier 2014, n° 105, p. 177-188.
- Bernard Bajolet, « La DGSE, outil de réduction de l'incertitude ? », *Revue Défense nationale,* janvier 2014, n° 766, p. 27-34.

Rapports d'expertise

(ordre chronologique)

- Alain Bauer et Christophe Soullez, *Fichiers de police et de gendarmerie. Comment améliorer leur contrôle et leur gestion ?,* Paris, La Documentation française, 2007, 145 p.
- *Le défi numérique. Comment renforcer la compétitivité de la France,* mai 2011, Paris, Institut Montaigne, 89 p.
- Marie-Pierre Hamel et David Marguerit, *Analyse des big data. Quels usages, quels défis ?,* Commissariat général à la stratégie et à la prospective, Note d'analyse n° 8, novembre 2013, 12 p.
- Sébastien Laurent, *Promouvoir une authentique communauté épistémique d'analystes du renseignement (CEDAR) : étude comparée (États-Unis, France, Grande-Bretagne),* consultance pour la direction des affaires stratégiques (DAS)-Ministère de la Défense, janvier 2014, 36 p.

L'expertise politique

(ordre chronologique)

- Jean-Michel Bélorgey, *La Police au rapport,* Presses universitaires de Nancy-Ligue des droits de l'homme, « Forum de l'IFRAS », 1991, 198 p.
- Arthur Paecht, *Echelon : mythe ou réalité ? Rapport d'information,* Paris, Assemblée nationale, 11 octobre 2000, 90 p.
- Gerhard Schmid, Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, système d'interception ECHELON (2001/2098 (INI), Rapport A5-0264/2001, Parlement européen, 11 juillet 2001, 210 p.
- Jean-Jacques Urvoas et Floran Vadillo, *Réformer les services de renseignement français,* Paris, Fondation Jean Jaurès, 2011, 82 p.
- Jean-Jacques Urvoas, *Les RG, la SDIG et après ? Rebâtir le renseignement de proximité,* note n° 115, Fondation Jean Jaurès, 012, 30 p.
- Observatoire de la Défense-Orion, *Le renseignement en France : quelles perspectives ?,* Paris, Fondation Jean Jaurès, 2012, 78 p.
- Floran Vadillo, *Une loi relative aux services de renseignement : l'utopie d'une démocratie adulte ?,* Paris, Fondation Jean Jaurès, note n° 130, 17 avril 2012, 20 p.

2. BIBLIOGRAPHIE

(ordre alphabétique)

- Philippe Bezes, *Réinventer l'État. Les réformes de l'administration françaises* (1962-2008), Paris, PUF, « Le lien social », 2009, 519 p.
- Hans Born and Aidan Wills, *Overseeing Intelligence Services. A Toolkit,* Geneva, DCAF, 2012, 200 p.
- Aurore Bouvart, *La réflexion sur la valorisation du renseignement dans la stratégie de défense et de sécurité française à travers les Livres blancs de 1972, 1994 et 2008,* mémoire de M2 « affaires internationales », IEP Bordeaux, sous la direction de S. Laurent, 2013, 233 p. +15 p. d'annexes. Premier prix de M2 de l'IHEDN.

- Caspar Bowden, *The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on European Union citizens' fundamental rights,* European Parliament, Directorate General for Internal Policies/civil Liberties, Justice and Home Affairs, 2013, 36 p.
- Olivier Chopin, Bastien Irondelle et Amélie Malissard, *Étudier le renseignement. État de l'art et perspectives de recherche,* Études de l'IRSEM, 2011, n° 9, 238 p.
- Conseil d'État, *Rapport public 2006. Sécurité juridique et complexité du droit,* Paris, La Documentation française, 2006, 411 p.
- Mireille Delmas-Marty, *Libertés et sûreté dans un monde dangereux,* Paris, Seuil, « La couleur des idées », 2010, 273 p.
- Christiane Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'Internet,* Paris, Dalloz, 2012, 1100 p.
- Olivier Forcade, « Les réformes du renseignement en France en 2007-2012 », *Le Mouvement des idées,* 3, 2e trimestre 2012, p. 161-175.
- Olivier Forcade et Sébastien Laurent, *Secrets d'État. Pouvoirs et renseignement dans le monde contemporain,* Paris, Colin, 2005, 238 p.
- Eric Freyssinet, *La cybercriminalité en mouvement,* Paris, Lavoisier, 2012, 226 p.
- Philippe Hayez, « Renseigner en confiance. La démocratie et les services de renseignement », dans : Hervé Dumez (dir.), *Rendre des comptes : nouvelle exigence sociale,* Paris, Dalloz, 2008, p. 88-104.
- Philippe Hayez, « Fighting Terrorism in a Kantian world », *Intelligencia y Seguridad: revista de analysis y prospectiva,* n° 7, décembre 2009-mai 2010, p. 109-116.
- Philippe Hayez, « Après le terrorisme… : quels enjeux pour les services de renseignement ? », *Cahiers de la sécurité,* n° 13, juillet-septembre 2010, p. 33-38.
- Philippe Hayez, « Le renseignement : son importance, ses transformations », *Cahiers français,* n° 360, février 2011, p. 43-48.
- Philippe Hayez, « Renseignement : The New French Intelligence Policy' », *International Journal of Intelligence and CounterIntelligence,* vol. 23, n° 3, 2010, p. 474-486.

- Philippe Hayez, « Adaptation et transformation du renseignement français depuis les années 1970: des hommes et des femmes comme les autres: les ressources humaines des services de renseignement et de sécurité français de 1970 à 2000 », communication à la journée d'études sur le renseignement organisée par l'IRSEM, 4 mai 2011.
- Olivier Kempf, *Introduction à la cyberstratégie,* Paris, *Economica,* 2012, 176 p.
- Sébastien Laurent, « Les parlementaires face à l'État secret et au renseignement sous les IVe et Ve République: de l'ignorance à la politisation », *Les Cahiers de la sécurité,* n° 13, juillet-septembre 2010, p. 134-144.
- Sébastien Laurent, « Les services spéciaux face aux "nouvelles menaces" de la société ouverte », *Revue de défense nationale,* décembre 2012, n° 755, p. 55-58.
- Sébastien Laurent, « Is there something Wrong with Intelligence in France? The Birth of the Modern Secret State », *Intelligence and National Security,* n° 28-3, 2013, p. 299-312.
- Alex Martin and Peter Wilson, « The Value of Non-Governmental Intelligence: Widening the field », *Intelligence and National Security,* vol. 23, n° 6, December 2008, p. 767-776.
- Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge, Cambridge University Press, 2013, 282 p.
- Frédéric Ocqueteau et Daniel Ventre (dir.), « Contrôles et surveillances dans le cyberespace. Avant-propos », *Problèmes politiques et sociaux,* n° 988, Septembre 2011, p. 4-10.
- Virginie Peltier, « Les enjeux de la protection du secret des correspondances: (bref) bilan et perspectives », dans : CNCIS, *20e rapport d'activité,* Paris, La Documentation française, 2012, p. 23-28.
- Kenneth Roberts, « Bridging the Worlds of Policy and Ideas: How Academic Expertise Can Improve Government's Performance », *Paper presented at the annual meeting of the International Studies Association, Hilton Hawaiian Village, Honolulu, Hawaii,* Mar 05, 2005 <http://www.allacademic.com/meta/p70845_index.html .
- UNIDIR, *The Cyber Index. International security Trends and Realities,* United Nations, New York and Geneva, 2013, 138 p.

- Floran Vadillo, *Les socialistes et les services de renseignement et de sécurité de 1981 à 2007 : usage et politisation de l'administration du renseignement,* mémoire de Master 2 sous la direction de S. Laurent, Université de Bordeaux 3, 2008, 321 p. + 261 p. d'annexes.
- Thorsten Wetzling, « L'Allemagne et le contrôle parlementaire des services de renseignement », IFRI, *Note du Comité d'étude des relations franco-allemandes/ CERFA,* n° 78, octobre 2010, 32 p.
- Philippe Wolf et Luc Vallée, « Cyber-conflits, quelques clés de compréhension », dans : ONDRP-INHESJ, *La criminalité en France,* Rapport 2011, Paris, éditions du CNRS, p. 787-802.

LES PUBLICATIONS DE L'INSTITUT MONTAIGNE

- Rester le leader mondial du tourisme, un enjeu vital pour la France (juin 2014)
- 1 151 milliards d'euros de dépenses publiques : quels résultats ? (février 2014)
- Comment renforcer l'Europe politique (janvier 2014)
- Améliorer l'équité et l'efficacité de l'assurance chômage (décembre 2013)
- Santé : faire le pari de l'innovation (décembre 2013)
- Afrique-France : mettre en œuvre le co-développement Contribution au XXVI[e] sommet Afrique-France (décembre 2013)
- Chômage : inverser la courbe (octobre 2013)
- Mettre la fiscalité au service de la croissance (septembre 2013)
- Vive le long terme ! Les entreprises familiales au service de la croissance et de l'emploi (septembre 2013)
- Habitat : pour une transition énergétique ambitieuse (septembre 2013)
- Commerce extérieur : refuser le déclin Propositions pour renforcer notre présence dans les échanges internationaux (juillet 2013)
- Pour des logements sobres en consommation d'énergie (juillet 2013)
- 10 propositions pour refonder le patronat (juin 2013)
- Accès aux soins : en finir avec la fracture territoriale (mai 2013)
- Nouvelle réglementation européenne des agences de notation : quels bénéfices attendre ? (avril 2013)
- Remettre la formation professionnelle au service de l'emploi et de la compétitivité (mars 2013)
- Faire vivre la promesse laïque (mars 2013)
- Pour un « New Deal » numérique (février 2013)

- Intérêt général : que peut l'entreprise ? (janvier 2013)
- Redonner sens et efficacité à la dépense publique
  15 propositions pour 60 milliards d'économies
  (décembre 2012)
- Les juges et l'économie : une défiance française ?
  (décembre 2012)
- Restaurer la compétitivité de l'économie française
  (novembre 2012)
- Faire de la transition énergétique un levier de compétitivité
  (novembre 2012)
- Réformer la mise en examen
  Un impératif pour renforcer l'État de droit
  (novembre 2012)
- Transport de voyageurs : comment réformer un modèle à bout de souffle ?
  (novembre 2012)
- Comment concilier régulation financière et croissance :
  20 propositions (novembre 2012)
- Taxe professionnelle et finances locales : premier pas vers une réforme globale ?
  (septembre 2012)
- Remettre la notation financière à sa juste place (juillet 2012)
- Réformer par temps de crise (mai 2012)
- Insatisfaction au travail : sortir de l'exception française (avril 2012)
- Vademecum 2007 – 2012 : Objectif Croissance (mars 2012)
- Financement des entreprises : propositions pour la présidentielle (mars 2012)
- Une fiscalité au service de la « social compétitivité » (mars 2012)
- La France au miroir de l'Italie (février 2012)
- Pour des réseaux électriques intelligents (février 2012)
- Un CDI pour tous (novembre 2011)
- Repenser la politique familiale (octobre 2011)

- Formation professionnelle : pour en finir avec les réformes inabouties (octobre 2011)
- Banlieue de la République (septembre 2011)
- De la naissance à la croissance : comment développer nos PME (juin 2011)
- Reconstruire le dialogue social (juin 2011)
- Adapter la formation des ingénieurs à la mondialisation (février 2011)
- « Vous avez le droit de garder le silence… » Comment réformer la garde à vue (décembre 2010)
- Gone for Good? Partis pour de bon ? Les expatriés de l'enseignement supérieur français aux États-Unis (novembre 2010)
- 15 propositions pour l'emploi des jeunes et des seniors (septembre 2010)
- Afrique - France. Réinventer le co-développement (juin 2010)
- Vaincre l'échec à l'école primaire (avril 2010)
- Pour un Eurobond. Une stratégie coordonnée pour sortir de la crise (février 2010)
- Réforme des retraites : vers un big-bang ? (mai 2009)
- Mesurer la qualité des soins (février 2009)
- Ouvrir la politique à la diversité (janvier 2009)
- Engager le citoyen dans la vie associative (novembre 2008)
- Comment rendre la prison (enfin) utile (septembre 2008)
- Infrastructures de transport : lesquelles bâtir, comment les choisir ? (juillet 2008)
- HLM, parc privé Deux pistes pour que tous aient un toit (juin 2008)
- Comment communiquer la réforme (mai 2008)
- Après le Japon, la France… Faire du vieillissement un moteur de croissance (décembre 2007)

- Au nom de l'Islam…
  Quel dialogue avec les minorités musulmanes en Europe ?
  (septembre 2007)
- L'exemple inattendu des Vets
  Comment ressusciter un système public de santé (juin 2007)
- Vademecum 2007-2012
  Moderniser la France (mai 2007)
- Après Erasmus, Amicus
  Pour un service civique universel européen (avril 2007)
- Quelle politique de l'énergie pour l'Union européenne ? (mars 2007)
- Sortir de l'immobilité sociale à la française (novembre 2006)
- Avoir des leaders dans la compétition universitaire mondiale
  (octobre 2006)
- Comment sauver la presse quotidienne d'information (août 2006)
- Pourquoi nos PME ne grandissent pas (juillet 2006)
- Mondialisation : réconcilier la France avec la compétitivité (juin 2006)
- TVA, CSG, IR, cotisations…
  Comment financer la protection sociale (mai 2006)
- Pauvreté, exclusion : ce que peut faire l'entreprise (février 2006)
- Ouvrir les grandes écoles à la diversité (janvier 2006)
- Immobilier de l'État : quoi vendre, pourquoi, comment
  (décembre 2005)
- 15 pistes (parmi d'autres…) pour moderniser la sphère publique
  (novembre 2005)
- Ambition pour l'agriculture, libertés pour les agriculteurs
  (juillet 2005)
- Hôpital : le modèle invisible (juin 2005)
- Un Contrôleur général pour les Finances publiques (février 2005)
- Les oubliés de l'égalité des chances (janvier 2004 - Réédition
  septembre 2005)

Pour les publications antérieures se référer à notre site internet :
www.institutmontaigne.org

INSTITUT
MONTAIGNE

3i France
Adminext
Aegis Media France
Affaires Publiques Consultants
Air France - KLM
Allen&Overy
Allianz
Areva
Association Passerelle
AT Kearney
August & Debouzy Avocats
AXA
Baker & McKenzie
BearingPoint
BNI France et Belgique
BNP Paribas
Bolloré
Bouygues
BPCE
Caisse des Dépôts
Cap Gemini
Carbonnier Lamaze & Rasle
Carrefour
CGI France
Cisco
CNP Assurances
La Compagnie financière Edmond de Rothschild
Crédit Agricole
Cremonini
Davis Polk & Wardwell
De Pardieu Brocas Maffei
Development Institute International
EADS
EDF
Egon Zehnder International
Eurazeo
Eurostar
France Telecom
GDF SUEZ
Générale de Santé
Groupama
Hamer & Cie
Henner
HSBC France
IBM
International SOS
ISRP
Jalma
Jeantet Associés
KPMG SA
Kurt Salmon
La Banque Postale
Lazard Frères
Linedata Services
LIR

SOUTIENNENT L'INSTITUT MONTAIGNE

INSTITUT
MONTAIGNE

LVMH
M6
MACSF
Malakoff Médéric
Mazars
McKinsey & Company
Média Participations
Mercer
Michel Tudel & Associés
Microsoft France
Ngo Cohen Amir-Aslani & Associés
OBEA
Ondra Partners
PAI Partners
Pierre & Vacances
PriceWaterhouseCoopers
Radiall
Raise
Rallye - Casino
Randstad
RATP
RBS France
Redex
Réseau Ferré de France
REXEL
Ricol, Lasteyrie & Associés
Roland Berger Strategy Consultants
Rothschild & Cie
RTE
Sanofi aventis
Santéclair
Schneider Electric Industries SA
Servier Monde
SFR
Sia Partners
Siaci Saint Honoré
SNCF
Sodexo
Sorin Group
Stallergènes
Suez Environnement
Tecnet Participations
The Boston Consulting Group
Tilder
Total
Vallourec
Vedici
Veolia
Vinci
Vivendi
Voyageurs du monde
Wendel
WordAppeal

SOUTIENNENT L'INSTITUT MONTAIGNE

Imprimé en France
Dépôt légal : juin 2014
ISSN : 1771-6756
Achevé d'imprimer en juin 2014

INSTITUT
MONTAIGNE

INSTITUT
MONTAIGNE

IL N'EST DÉSIR PLUS NATUREL QUE LE DÉSIR DE CONNAISSANCE

Pour une véritable politique publique du renseignement

Depuis le *Livre blanc* de la Défense de 2008, le renseignement, devenu la fonction stratégique « connaissance et anticipation », a pris une ampleur considérable. Alors que son champ d'intervention est de plus en plus celui du cyberespace, le renseignement se trouve confronté à de fortes critiques et à des exigences croissantes de transparence. Marquée structurellement par le secret, cette fonction doit – pour être efficace – se tenir à distance de celles-ci tout en s'accompagnant de contrôles sérieux, d'indicateurs pour le public et d'une information spécifique aux parlementaires. Cette étude *Pour une véritable politique publique du renseignement* détaille les évolutions souhaitables qui visent d'une part à rendre le renseignement plus efficace et d'autre part à mieux garantir la protection des citoyens. Ces mutations, favorisant un climat de confiance, permettront également de préserver la légitimité de la dépense publique en la matière qui est un investissement.

Institut Montaigne
38, rue Jean Mermoz - 75008 Paris
Tél. +33 (0)1 58 18 39 29 - Fax +33 (0)1 58 18 39 28
www.institutmontaigne.org - www.desideespourdemain.fr

10 €
ISSN 1771-6756
Juin 2014