UNIVERSITÉ PARIS - PANTHÉON-ASSAS

Année universitaire 2022-23

Master 2 Sécurité et défense

LE CONTROLE DES ACTIVITÉS DE RENSEIGNEMENT

Mémoire préparé sous la direction du Professeur Bertrand WARUSFEL

présenté et soutenu publiquement
pour l'obtention du Master 2 Sécurité et défense
mention droit public – finalité recherche

par
Luc PONCEOT

JURY :

Président : Monsieur Bertrand WARUSFEL
Professeur à l'Université Paris 8 – Vincennes – Saint-Denis

Assesseur : Monsieur Jérôme MILLET
Administrateur d'État au Ministère de l'intérieur

LE CONTROLE DES ACTIVITÉS DE RENSEIGNEMENT

Table des abréviations

CESE	Comité économique social et environnemental
CJA	Code de justice administrative
CPCE	Code des postes et des communications électroniques
CJCE	Cour de justice de la Communauté européenne
CJUE	Cour de justice de l'Union Européenne
CNCIS	Commission nationale de contrôle des interceptions de sécurité
CNCTR	Commission nationale de contrôle des techniques de renseignement
Cour EDH	Cour européenne des droits de l'homme
CEDH	Convention européenne des droits de l'homme
CSI	Code de la sécurité intérieure
CVFS	Commission de vérification des fonds spéciaux
DCPJ	Direction nationale de la police judiciaire
DDHC	Déclaration des droits de l'homme et du citoyen
DGSE	Direction générale de la sécurité extérieure
DGSI	Direction générale de la sécurité intérieure
CNIL	Commission nationale de l'informatique et des libertés
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
LPM	Loi de programmation militaire
NSA	National security agency
s.	Suivant
UE	Union Européenne
v.	Voir

SOMMAIRE

INTRODUCTION GÉNÉRALE

« *L'information, c'est tout, à la guerre, comme pendant la paix, dans la politique, comme dans la finance », Joseph Fouché (1759-1820).*

« Je m'appelle Edward Joseph Snowden. Avant, je travaillais pour le gouvernement mais aujourd'hui, je suis au service de tous. », Edward Snowden.

Cette phrase, tirée de l'ouvrage d'Edward Snowden, *mémoires vives,* paru en 2019, choque. Comment expliquer que le gouvernement ne soit pas tourné vers le service de tous, c'est-à-dire de l'intérêt général. Dans cet ouvrage, l'auteur, alors officier au sein de la CIA, explique qu'elles ont été les raisons l'ayant poussé à dénoncer la mise en place d'une surveillance de masse par la NSA. L'une d'entre elles visait à mettre fin aux atteintes portées par les services de renseignement aux droits et libertés (garanties par la Constitution) de 340 millions d'Américains. L'histoire de ce lanceur d'alerte a amené à se questionner sur l'impact des services de renseignement sur les libertés et droits de chacun.

1. Souvent considérées comme la chasse gardée de barbouzes, les activités de renseignement étaient placées dans un vide juridique. Cependant, elles n'ont pas échappé à des critiques notamment à la suite de la divulgation de ratés[1] ou à l'action de lanceurs d'alerte[2]. Ce vide ne pouvait plus persister à l'heure d'une judiciarisation générale de notre société et de la volonté de plus en plus grande de protéger les libertés de chacun. En France, cette évolution est caractérisée, pour beaucoup, par la loi du 24 juillet 2015 (même si cette évolution a été plus progressive en

[1] En 1965, l'affaire Ben Barka a bousculé le fonctionnement des services de renseignement. Le Président de Gaulle a alors rattaché le SDECE au ministère de la Défense, car le Premier ministre était trop détaché des questions de renseignement, voire pire, il utilisait les services à des fins privées. Le leader tiers mondiste marocain avait été enlevé boulevard Saint-Germain par une équipe composée de policiers, d'agents secrets et de truands. V. notamment l'ouvrage de Bernard Violet, *L'affaire Ben Barka*, Fayard, 1991.

[2] En 2013, Edward Snowden (agent de la CIA) rend public l'existence d'une surveillance de masse mondiale d'internet et des moyens de communication par la NSA. v. notamment l'article publié dans Le Monde, *Révélations Snowden, un séisme planétaire*, 21 octobre 2013.

réalité). Ce texte vient encadrer le recours aux techniques de renseignement les plus liberticides. Il est codifié au sein du livre VIII du code de sécurité intérieure. Grâce à cette loi, la France vient rattraper son retard sur les autres pays européens. Cette judiciarisation tardive s'explique notamment pour deux raisons. La première tient à l'importance des activités de renseignement pour la sécurité nationale (peur d'enrayer ces activités primordiales à la sécurité). La seconde, non sans lien avec la première, tient au secret auquel doit être soumis les activités de renseignement (en multipliant les contrôles, le risque de fuite est aussi multiplié).

2. ***Définition de l'activité de renseignement***. Depuis l'existence des sociétés modernes, les États se sont donné les moyens d'anticiper les menaces auxquelles ils pourraient faire face. Sherman Kent définissait le renseignement (*intelligence* en anglais) comme : « *la connaissance dont nos civils et militaires haut placés doivent disposer pour assurer la protection de la Nation* »[3]. Cette définition régalienne est quelque peu réductrice, car elle fait uniquement référence aux activités étatiques. Aujourd'hui, ce n'est un secret pour personne que des sociétés privées réalisent des activités de renseignement industriel. Selon une approche plus actuelle, régalienne et pragmatique, elles renvoient à l'ensemble des activités exercées par les services de renseignement.

3. En droit positif français, peu de textes offrent une définition de la notion. Il a fallu attendre le Livre blanc pour la défense et la sécurité de 2008[4] afin qu'une définition apparaisse. Selon ce dernier le renseignement a : « *pour objet de permettre aux plus hautes autorités de l'État, à notre diplomatie, comme aux armées et au dispositif de sécurité intérieure et de sécurité civile, d'anticiper et, à cette fin, de disposer d'une autonomie d'appréciation, de décision et d'action* ». Cette définition centrée sur la finalité renvoie à celle donnée par Sherman Kent. L'activité de renseignement permet donc d'aider le décideur politique ou militaire dans la prise de décision. En affirmant la présence d'une politique publique de renseignement, l'article L811-1 du CSI vient définir le rôle des activités de renseignement à savoir de concourir : « *à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation* ». Jusqu'ici, les définitions données sont centrées sur la finalité des activités de renseignement qui

[3] Sherman Kent, *Strategic intelligence for American World Policy*, Princeton University Press, 1949.
[4] *Livre blanc sur la défense et la sécurité*, 2008, page 133.

est, par conséquent, de protéger et de promouvoir les intérêts fondamentaux de la Nation, notamment en aidant à la décision du pouvoir politique.

4. Concernant le contenu de ces activités, l'article L811-2 du CSI précise que les missions « *des services de renseignements spécialisés* » sont « *en France et à l'étranger, la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et de ces menaces* ». À la lumière de cette disposition, les services de renseignement ont donc à charge la « *recherche, la collecte, l'exploitation et la mise à disposition* » d'informations concernant des risques susceptibles d'affecter la vie de la Nation. C'est ce que Sherman Kent appelait le cycle du renseignement. Ce dernier est important à comprendre et retenir, car des contrôles, plus ou moins efficaces, ont été mis en place à chaque étape (ou presque) de ce cycle.

5. Les activités de renseignement sont exercées par les « *services spécialisés de renseignement* »[5] ainsi que les services « *relevant des ministres de la défense, de l'intérieur et de la justice ainsi que des ministres chargés de l'économie, du budget ou des douanes* »[6] ajoutés par voie réglementaire après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR).

Le code de la sécurité intérieure renvoie donc indirectement aux services de la communauté du renseignement ainsi qu'aux services dits du « *second cercle* ». Selon le décret du 28 septembre 2015*,* les services de la communauté du renseignement (c'est-à-dire les services spécialisés au sens du CSI) sont : la Direction générale de la sécurité intérieure (DGSI) ; la Direction générale de la sécurité extérieure (DGSE) ; la Direction de la protection et de la sécurité de la défense (DPSD) ; la Direction du renseignement militaire (DRM) ; Tracfin et la Direction nationale du renseignement et des enquêtes douanières (DNRED).

[5] Article L811-2 du CSI.
[6] Article L811-4 du CSI.

Les services du second cercle sont autorisés à recourir aux techniques de renseignement (ou à certaines d'entre elles) contenues dans le livre VIII du code de sécurité intérieure. Depuis 2015, ce nombre de services n'a jamais cessé d'augmenter en raison des vagues successives de décrets additionnels. Figure notamment parmi ces derniers certains services spécialisés de la police judiciaire. Par exemple, le *décret du 29 novembre 2021* ajoute la possibilité pour la Direction centrale de la police judiciaire (DCPJ) de recourir à certaines techniques du livre VIII. Les principaux services du second cercle sont : la direction du renseignement de la Préfecture de police de Paris ; le service central du renseignement territorial ; la sous-direction de l'anticipation opérationnelle de la Gendarmerie nationale et le service national du renseignement pénitentiaire.

6. ***Distinction entre renseignement administratif et renseignement judiciaire***. Il est primordial de ne pas confondre les deux. Le renseignement administratif relève d'une mission de police administrative, alors que le renseignement judiciaire relève d'une mission de police judiciaire. Cette distinction aux premiers abords est simple, mais peut vite devenir ambiguë. En effet, certains services de police judiciaire font partie des services dits du second cercle[7], autrement dit, ils peuvent recourir à certaines techniques prévues dans le livre VIII du CSI. De plus, les enquêtes judiciaires sont de plus en plus souvent enclenchées à la suite de renseignements, c'est ce qui est appelé « *le renseignement pré-judiciaire* ». La qualification juridique de ce dernier fait débat… Certains considérant le renseignement préjudiciaire comme relevant d'une mission de police administrative alors que d'autres considèrent que le renseignement préjudiciaire relève d'une mission de police judiciaire. Cette évolution pratique affine la frontière entre renseignement administratif et renseignement judiciaire.

7. En matière de terrorisme et de crimes organisés, la distinction est encore plus complexe[8]. Comme l'explique Benoist Hurel[9], dans ce type de criminalité, la frontière entre les indices permettant d'identifier une menace (fondent l'action du renseignement administratif) et les indices susceptibles de caractériser des actes préparatoires (fondent l'enquête judiciaire) est devenue quasi

[7] Depuis la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
[8] V. notamment le compte-rendu du rendez-vous de la recherche du 21 mai 2019 portant sur le renseignement au service de l'enquête (IHEMI), page 4.
[9] Magistrat membre du Conseil supérieur de la magistrature, ayant effectué la majeure partie de sa carrière au sein de différents parquets.

inexistante. Pour faciliter cette articulation, le Conseil constitutionnel a donné priorité au judiciaire sur l'administratif[10], et ce, en raison de la règle obligeant les autorités administratives à informer le procureur de la République en cas d'informations sur la commission éventuelle d'une infraction. Autrement dit, lorsqu'un service spécialisé aura la connaissance par son activité d'une infraction (sachant que la commission d'acte préparatoire est une infraction) alors il devra en informer le parquet qui décidera (ou non) d'enclencher le processus judiciaire. Ce transfert de l'autorité administrative à l'autorité judiciaire amène une difficulté pratique considérable concernant le « *blanchissement* » du renseignement, c'est-à-dire comment utiliser le renseignement dans l'enquête judiciaire[11].

8. L'importance de cette distinction s'explique en raison de la différence de régime applicable en fonction qu'il s'agisse de renseignement judiciaire (police judiciaire) ou de renseignement administratif (police administrative). Le renseignement judiciaire est encadré par le code de procédure pénale[12] et est contrôlé par le juge judiciaire. Le renseignement administratif est lui encadré - en partie - par le livre VIII du CSI et fait l'objet de divers contrôles (notamment administratif avec la CNCTR ainsi que juridictionnel avec le Conseil d'État).

9. ***Définition de la notion de contrôle***. Elle renvoie, en droit, à la surveillance et à la vérification du respect des règles applicables (régime) à une notion ou une activité donnée. Le contrôle peut prendre diverses formes (juridictionnel, politique, administratif, hiérarchique). L'ensemble de ces contrôles va être scruté afin d'identifier leurs points forts ainsi que leurs points faibles. Depuis plusieurs décennies, les autorités administratives indépendantes (ou autorités publiques indépendantes) se multiplient, leur rôle est souvent de réaliser un contrôle spécifique. Les activités de renseignement ne font pas exception à cette tendance générale.

10. ***Les activités de renseignement et les libertés concernées***. Le premier article du livre VIII du CSI (article L801-1) dispose que la loi de 2015 vise à protéger la vie privée « *dans toutes ses*

[10] Décision constitutionnelle du 23 juillet 2015 (n° 2015-713 DC).
[11] Concernant les techniques pour intégrer un renseignement dans une procédure judiciaire v. notamment pages 4 et 5 du compte rendu du rendez-vous de la recherche du 21 mai 2019 portant sur le renseignement au service de l'enquête (IHEMI).
[12] Articles 706-73 à 706-106 du code de procédure pénale pour la délinquance et criminalité organisée par exemple.

composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile ». Le droit à la vie privée est un droit protégé par la loi (article 9 du Code civil), par la Convention européenne des droits de l'homme (article 8) et jouit d'une protection constitutionnelle[13]. Ce droit permet, dans sa conception originelle, de protéger les individus d'une intrusion (par une personne privée ou l'État) dans leur intimité. Le Conseil constitutionnel définit la vie privée (et la rattache à l'article 2 de la Déclaration des droits de l'homme et du citoyen) comme « *la sphère d'intimité de chacun* »[14].

La mention de ce droit au début du livre consacré au renseignement s'explique par la dichotomie entre les activités de renseignement et le droit au respect de la vie privée. Les premières ne peuvent pas exister sans violation du second. C'est pourquoi les violations de la vie privée doivent être strictement justifiées. Cependant, comme tous les principes et libertés à valeur constitutionnelle, une conciliation doit être faite entre eux[15].

11. Les activités de renseignement concourent également à la sécurité nationale. Pour rappel, la sécurité est un droit fondamental au sens de l'article L111-1 du CSI. Selon ce dernier, la sécurité est « *une des conditions de l'exercice des libertés individuelles et collectives* ».

12. ***Le contrôle du renseignement en France avant 2015***. Avant d'entrer dans le vif du sujet, il est important de faire un rappel de ce qu'était le contrôle des activités de renseignement avant 2015. Par le passé, les activités de renseignement faisaient l'œuvre uniquement d'un encadrement médiatique (opinion publique), ce qui explique pourquoi de nombreux scandales ont éclaté. Or, pour les raisons évoquées précédemment, l'état du droit a évolué.

13. Dès 1991, la Commission nationale de contrôle des interceptions de sécurité (CNCIS) a été créée par la loi relative au secret des correspondances émises par voie de télécommunications. Ce texte fut pris après la condamnation de l'État français par la Cour européenne des droits de l'homme[16].

---

[13] Décision constitutionnelle du 2 mars 2004 (n° 2004-492 DC).
[14] Décision constitutionnelle du 23 juillet 2015 (n° 2015-713 DC).
[15] Décision constitutionnelle du 23 juillet 2015 (n° 2015-713 DC).
[16] CEDH, *Kruslin et Huvig contre France*, 24 avril 1990

Cette autorité administrative indépendante était chargée de contrôler a posteriori la décision d'autorisation du Premier ministre permettant l'interception des correspondances émises par voie de télécommunications. D'une manière générale, cette loi créa un véritable cadre juridique pour ce type d'interception réalisée à l'occasion de missions de police administrative. Elle vient limiter le recours à cette technique aux seuls cas où cette dernière intéresse *« la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées* ». La CNCIS était donc chargée de contrôler l'application de ce régime spécifique. Cependant, elle pouvait uniquement émettre des recommandations au Premier ministre.

De plus, l'article 24 de cette loi crée une infraction qui vient punir l'agent dépositaire de l'autorité publique qui aurait ordonné ou réalisé une interception des correspondances électroniques en dehors des cadres prévus par la loi. La CNCIS pouvait, dans le cadre de son contrôle a posteriori, informer le procureur de la République sur la présence d'une éventuelle infraction.

Certes, le contrôle de cette autorité administrative indépendante ne portait que sur une technique spécifique de renseignement, mais cette loi pose les prémices d'un futur encadrement plus général.

14. La loi du 9 octobre 2007 est venue créer la Délégation parlementaire au renseignement (DPR). Pour rappel, une délégation, à la différence des commissions, est composée de membres de chaque chambre. La DPR est constituée de quatre députés et de quatre sénateurs. Le président de la Commission des affaires étrangères, de la défense et des forces armées (Sénat) ainsi que le président de la Commission de la défense nationale et des forces armées (Assemblée nationale) siègent de plein droit au sein de cette délégation. Les autres membres sont nommés par les présidents de chambre « *de manière à assurer une représentation pluraliste* ».

Son objet est affirmé au troisièmement de l'unique article, sa mission est « *de suivre l'activité générale et les moyens des services spécialisés à cet effet placés sous l'autorité des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget* ». Autrement dit, depuis 2015, elle est chargée d'évaluer la politique publique du renseignement. Cette délégation

a vu ses pouvoirs augmentés petit à petit[17], mais reste cantonnée à un contrôle porté sur les moyens dont sont dotés les services de renseignement. Cette loi de 2007 vient créer un contrôle politique potentiel sur les activités de renseignement. Sa portée est donc importante et pourra à terme devenir considérable.

15. ***Les apports de la loi du 24 juillet 2015***. Cette loi va venir encadrer le contrôle et le recours aux techniques de renseignement considérées comme les plus liberticides. Par conséquent, le contrôle administratif instauré par cette dernière ne couvre pas la totalité des activités de renseignement.

16. La loi du 24 juillet 2015 vient limiter à des cas précis le recours aux techniques de renseignement prévues au livre VIII. L'article L811-3 du CSI présente les motifs pouvant justifier la mise en place de l'une d'entre elles. Ces derniers sont : « *l'indépendance nationale, l'intégrité du territoire et la défense nationale* », « *les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère* », « *les intérêts économiques, industriels et scientifiques majeurs de la France* », « *la prévention du terrorisme* », ainsi que « *la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L212-1, des violences collectives de nature à porter gravement atteinte à la paix publique, la prévention de la criminalité et de la délinquance organisées et la prévention de la prolifération des armes de destruction massive* ». En d'autres termes, seul un (ou plusieurs) de ces motifs peut justifier légalement la mise en place d'une technique de renseignement.

17. Dorénavant, la mise en place d'une technique de renseignement (prévue au livre VIII) est autorisée par le Premier ministre après avis (non conforme) de la CNCTR. La demande d'autorisation peut émaner uniquement du ministre de l'Intérieur, du ministre de la Défense, du ministre de l'Économie et du Budget, ainsi que du garde des Sceaux. Cette demande doit répondre à un certain formalisme[18]. L'autorisation est délivrée pour une durée maximale de quatre mois.

[17] Notamment par la loi de programmation militaire (LPM) pour 2014-2019.
[18] V. Article L821-3 du CSI.

Cette dernière comprend aussi une forme particulière, notamment lorsque le Premier ministre ne suit pas l'avis de la CNCTR (le cas échéant, il devra préciser pourquoi).

18. Cette loi vient remplacer la CNCIS par la CNCTR. Cette dernière est aussi une autorité administrative indépendante. Elle est composée de neuf membres (deux conseillers d'État, deux magistrats de la Cour de cassation, quatre parlementaires et un membre spécialisé en moyens de communication) et peut se réunir en deux formations (une plénière et l'autre restreinte). Son rôle est double : réaliser un contrôle a priori (par l'émission d'un avis non conforme pour chaque autorisation) et un contrôle a posteriori (dans l'application des autorisations). L'ensemble de ses membres sont habilités secret-défense. Cette habilitation est capitale à deux égards. D'une part, elle va permettre aux membres de la CNCTR d'accéder aux informations classifiées dont ils ont besoin pour réaliser leur contrôle. D'autre part, elle permet de rendre pénalement responsables ses membres en cas de divulgation d'informations classifiées. Pour rappel, l'article 413-10 du Code pénal punit de sept ans d'emprisonnement et de 100 000 euros d'amende toute personne habilitée qui viendrait détruire, détourner, soustraire ou reproduire une information classifiée ou donner l'accès de cette dernière à une personne non habilitée.

19. Encore plus innovante fut la création d'une formation spécialisée au sein du Conseil d'État. Ladite loi vient ajouter un nouveau chapitre relatif au contentieux lié aux techniques de renseignement et aux fichiers intéressants la sûreté de l'État au sein du code de justice administrative[19]. Cette formation spécialisée sera compétente notamment pour statuer sur les recours faits par la CNCTR ou par tout administré concernant la légalité de l'autorisation du Premier ministre de recourir à une technique de renseignement prévue au livre VIII du CSI.

À la lumière des membres de la CNCTR, les conseillers d'État qui siègent dans cette formation spécialisée jouissent aussi d'une habilitation secret-défense. Là encore, le but de cette habilitation est de permettre à ses membres d'accéder aux informations classifiées qui concernent le dossier afin de réaliser un véritable contrôle. Ce point explique pourquoi la procédure contentieuse devant cette formation spécialisée est problématique, notamment en ce qui concerne le respect des droits du requérant. Cette dernière sera abordée par la suite.

[19] V. Articles L773-1 à L773-8 du CJA.

20. Dans sa décision du 23 juillet 2015, le Conseil constitutionnel a partiellement censuré la loi du 24 juillet 2015. Les dispositions relatives à la procédure dite d'urgence opérationnelle ont été censurées car portant une atteinte disproportionnée au droit du respect de la vie privée et au secret des correspondances. Cette procédure prévoyait la possibilité pour un service de renseignement de mettre en place une technique sans l'autorisation du Premier ministre en cas de menace imminente ou de risques trop élevés. La censure du Conseil portera uniquement sur ce point, le reste du dispositif ayant été jugé (presque en totalité) comme conforme à la Constitution (ce qui limite la possibilité de QPC dans le futur…).

21. L'article 27 de la présente loi prévoyait une évaluation parlementaire au maximum cinq après son entrée en vigueur. Cette évaluation a donné lieu à des modifications du texte originel. Ces modifications sont le fruit de problèmes pratiques ou de problèmes juridiques. Ces évolutions seront étudiées dans la suite de cette étude.

22. ***Délimitation du sujet***. Les activités de renseignement privées, c'est-à-dire la recherche par des opérateurs économiques privés d'informations visant à se démarquer (ou rattraper) d'autres opérateurs, ne seront pas étudiées. Par conséquent, cette étude s'intéressera uniquement aux activités de renseignement étatiques. De plus, sera traité uniquement le cas français, même si des comparaisons avec d'autres États, notamment européens, pourront avoir lieu.

23. ***L'efficacité nécessaire des différents contrôles***. Au cours de l'histoire récente de la France, les exemples d'excès concernant les activités de renseignement sont nombreux. Montesquieu disait à propos du pouvoir : « *C'est une expérience éternelle que tout homme qui a du pouvoir est porté à en abuser; il va jusqu'à ce qu'il trouve des limites* ». En passant par *l'affaire du Canard enchaîné* ou encore *l'affaire des écoutes de l'Élysée*, cette maxime n'a pu qu'être confirmée.

Les services de renseignements, par les pouvoirs qui leur sont confiés, peuvent avoir un apport néfaste sur une société démocratique. Le passé montre que ces services peuvent être utilisés à des fins contraires à l'intérêt général, c'est-à-dire dans un autre but que celui de préserver les intérêts fondamentaux de la Nation. La loi du 24 juillet 2015 réalise un bond en avant primordial dans le respect de l'État de droit. Il paraissait injustifiable que les activités de renseignement ne

fassent l'objet d'aucun cadre légal, alors que les autres démocraties occidentales avaient sauté le pas depuis plusieurs années.

24. Certes, l'encadrement légal des activités de renseignement est une avancée pour l'État de droit, cependant ce dernier doit faire l'objet d'un contrôle efficace, indépendant et accessible. Ce contrôle fait face à une difficulté structurelle, il faut assurer un contrôle effectif sans remettre en cause l'efficacité des services de renseignement, qui comme le montre le nombre d'attentats déjoués ces dernières années, est inhérente au maintien d'une légalité républicaine et d'une sécurité minimale. L'ambiguïté réside dans le fait que les activités de renseignement peuvent être liberticides si insuffisamment contrôlées, mais le manque d'efficacité de ces dernières amènerait des externalités nuisibles dans l'exercice des libertés de chacun. Cette idée est notamment consacrée à l'article L. 111-1 du CSI précédemment cité. Par conséquent, un contrôle effectif des activités de renseignement permet d'assurer un équilibre. Or, la loi de 2015 comportait de nombreuses lacunes. La première touchait l'effectivité directe du contrôle administratif réalisé par la CNCTR. D'autres portaient notamment sur le contrôle a posteriori. Le législateur a tenté en modifiant à plusieurs reprises ladite loi de résorber ces failles.

25. ***Problématique.*** D'une façon générale, la loi du 24 juillet 2015 comprenait de nombreuses zones d'ombres, et était incomplète. L'action du législateur était donc nécessaire. Cette action a été rendue obligatoire par les exigences posées par les juridictions européennes. Il est donc capital de se demander si les dernières évolutions juridiques ont permis de dissiper les lacunes relatives au contrôle des activités de renseignement.

26. ***Plan***. Le cadre juridique créé par la loi du 24 juillet 2015 a connu de nombreuses modifications. Deux remarques peuvent être retenues. D'une part, les diverses modifications viennent renforcer un contrôle, notamment a priori, souvent critiqué par les juges européens (***titre I***). D'autre part, malgré ces évolutions, des lacunes persistent dans l'effectivité ou la contenance des procédures de contrôle mis en place par le droit français (***titre II***).

TITRE I : UN RENFORCEMENT NÉCESSAIRE DU CONTRÔLE IMPULSÉ PAR LA JURISPRUDENCE EUROPÉENNE

27. ***Annonce.*** Les évolutions de la loi du 24 juillet 2015 découlent principalement de jurisprudences rendues par les juges européens. Le droit du renseignement fut le terreau d'un dialogue important entre, à la fois, les juges français, la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme (***chapitre 1***). Ce dialogue a poussé le législateur français à augmenter les prérogatives de la CNCTR, afin d'en faire un véritable garde-fou. De plus, par son action, d'autres contrôles se sont révérés importants (***chapitre 2***).

<u>CHAPITRE 1</u> : LE DROIT DU RENSEIGNEMENT : UN EXEMPLE DU DIALOGUE DES JUGES

28. ***Annonce.*** Malgré l'instauration d'un encadrement des activités de renseignement ainsi que la mise en place de plusieurs contrôles, les juges européens s'inscrivent, comme souvent, dans une approche libérale et veillent à ce que les États membres, tant du Conseil de l'Europe que de l'Union européenne, garantissent une protection suffisante de la vie privée (***section 1***). Même si ce dialogue amène le législateur à faire évoluer l'état du droit, il amène parfois des conflits entre les juges nationaux et les juges européens. En la matière, un désaccord subsiste entre le Conseil d'État et la Cour de justice de l'UE au sujet de l'obligation générale et indifférenciée de conservation des données faites aux fournisseurs de réseau (***section 2***).

<u>Section 1 :</u> Les juges européens : réels garants des libertés en matière de renseignement

29. ***Rappels.*** Depuis 1974 avec la ratification de la Convention européenne des droits de l'homme (CEDH), la France s'est engagée à respecter le contenu de ce texte (et ses protocoles additionnels) ainsi que les jurisprudences rendues par la Cour européenne des droits de l'homme (Cour EDH). De plus, la France, en tant que membre de l'Union européenne, doit respecter, d'une part, le droit primaire et le droit dérivé de l'UE, et d'autre part, la jurisprudence de la Cour de justice de l'UE[20].

[20] V. débat autour de la primauté du droit européen sur le droit national, y compris constitutionnel. V. aussi CJUE*, Internationale Handelsgesellschaft,* 1970.

30. ***Annonce.*** Les juges européens, surtout la Cour de Strasbourg, sont réputés pour leur interprétation libérale et positive des textes. La Cour EDH veille au respect de l'ensemble des droits et des libertés contenus dans la CEDH, notamment la vie privée garantie par son article 8. Les juges européens ont développé des exigences minimales en matière de renseignement. Ces dernières doivent être respectées par le législateur étatique et par les services de renseignement sous peine d'une condamnation de l'État (***paragraphe 1***). Au-delà de ces exigences minimales, la Cour EDH se prononce, lorsqu'elle est saisie, sur le cadre juridique étatique général qui entoure les activités de renseignement. Par ailleurs, un recours a été réalisé contre le cadre juridique français mis en place par la loi du 24 février 2015 (***paragraphe 2***).

Paragraphe 1 : Les exigences minimales demandées par les textes et les juges européens

31. ***L'article 8 de la CEDH***. Après avoir énoncé le droit à la vie privée, il prévoit en son deuxième alinéa que les pouvoirs publics puissent porter atteinte à ce droit (qui n'est donc pas absolu) dans certaines conditions. Ce dernier dispose : « *Il ne peut y avoir ingérence d'une autorité publique (…) que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». Plusieurs remarques doivent donc être émises dès maintenant. D'une part, les rédacteurs du texte ont bien pris en compte, dès 1950, que les autorités publiques avaient besoin, pour l'intérêt général, de porter atteinte à l'article 8 alinéa 1. D'autre part, le texte vient conditionner ces atteintes. Ces dernières doivent être prévues par la loi (principe de légalité) et être justifiées notamment par la défense de la sécurité nationale, de la sûreté publique, du bien-être économique du pays, de l'ordre, à la prévention des infractions pénales. Les motifs permettant de porter atteinte au principe énoncé sont donc vastes. Enfin, la France ne respectait donc (directement) pas la CEDH avant 2015, car les techniques utilisées par les services de renseignement ne trouvaient, mis à part pour la surveillance des correspondances émises par télécommunication depuis 1991[21], aucun fondement légal avant 2015.

[21] Pour rappel, cet encadrement restreint fait suite à la condamnation de la France par la Cour EDH. v. CEDH, *Kruslin et Huvig contre France*, 24 avril 1990.

32. ***La jurisprudence de la Cour EDH***. Les arrêts concernant les activités de renseignement, rendus par la Cour européenne des droits de l'homme, ont été relativement nombreux ces dernières décennies. Or, dès 1978, dans un arrêt qui concernait l'Allemagne[22], la Cour fut saisie d'un contentieux relatif à la surveillance, par les pouvoirs publics, de la correspondance et des communications électroniques. En l'espèce, les requérants (avocats) contestaient la conformité à la convention de dispositions légales permettant aux pouvoirs publics allemands de procéder à des surveillances de communications électroniques ou de correspondances. La question était donc de savoir si le dispositif prévu par l'Allemagne entrait dans l'exception posée à l'alinéa 2 de l'article 8. La Cour constate une non-violation de l'article 8 par l'État allemand. Elle constate que l'atteinte est prévue légalement (principe de légalité respecté) et que la loi a « *bien pour but de sauvegarder la sécurité nationale et/ou d'assurer la défense de l'ordre et la prévention des infractions pénales* ».

En 1987, dans une affaire concernant la Suède[23], la Cour est venue préciser le contenu de l'obligation de légalité énoncée par l'alinéa 2 de l'article 8. D'une part, la loi prévoyant la possibilité d'atteinte doit « *être accessible à l'intéressé* », autrement dit, l'ensemble des citoyens doivent avoir connaissance de cette possibilité d'intrusion ; c'est ce qu'appelle la Cour l'exigence de prévisibilité. D'autre part, la Cour précise que « *la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée* ». En d'autres termes, la Cour pose une exigence de précision : le citoyen doit savoir dans quel contexte les pouvoirs publics pourront porter atteinte à sa vie privée. Plus récemment, la Cour a estimé, dans une affaire concernant le Royaume-Uni[24], que la loi britannique violait l'article 8 car elle ne précisait pas l'étendue et les modalités d'exercice du pouvoir d'appréciation considérable laissé aux pouvoirs publics en matière d'interception de communications, ce qui n'apportait pas une protection suffisante contre les abus de pouvoir[25].

---

[22] Arrêt *Klass et autres contre Allemagne*, 6 septembre 1978.
[23] Arrêt *Leander contre Suède*, 26 mars 1987.
[24] Arrêt *Liberty et autres contre Royaume-Uni*, 1er juillet 2008.
[25] Plus précisément, la loi n'apportait aucune précision sur la procédure applicable à l'examen, à la diffusion, à la conservation et la destruction des données interceptées. L'exigence de légalité n'était donc pas remplie.

Petit à petit, la Cour EDH a développé une jurisprudence poussée en matière d'encadrement des activités de renseignement, tout en rappelant que ces dernières sont nécessaires à la sauvegarde de la sécurité nationale. La Cour adapte sa jurisprudence aux nombreuses évolutions techniques qui traversent les activités de renseignement.

33. ***La jurisprudence de la CJUE***. Pour rappel, à l'origine, l'Union européenne n'avait pas vocation à protéger les libertés individuelles (sauf les libertés économiques). Cependant, pour donner suite à la demande des juges étatiques[26], la CJUE a progressivement protégé les droits des citoyens européens. Ce mouvement a atteint son paroxysme en 2000 avec la création de la Charte des droits fondamentaux. Cette dernière, depuis 2007, fait partie du droit primaire de l'UE, et doit par conséquent, être respectée par les États membres et les institutions européennes. En ce qui concerne les activités de renseignement, l'article 7 de ladite charte protège le droit à la vie privée et l'article 8 les données personnelles.

Le contentieux de la Cour de justice en matière d'activité de renseignement est moins fourni que celui de la Cour européenne des droits de l'homme. Les arrêts de la Cour du Luxembourg portent sur des points précis. Dans le second volet de l'affaire Kadi[27], la Cour de justice avance qu'il ne peut pas lui être opposé le secret ou la confidentialité de certaines informations et que c'est à elle de procéder à la conciliation des impératifs sécuritaires avec les droits fondamentaux dans le cadre du contrôle juridictionnel qu'elle exerce. Par cet arrêt, la Cour de justice vient protéger les droits procéduraux des ressortissants européens. En 2016, le juge de l'UE est venu interdire dans un arrêt capital l'obligation généralisée et indifférenciée, faite aux opérateurs téléphoniques, de collecter et de conserver les données relatives au trafic et aux données de localisation[28]. Ce point a été âprement critiqué par les services de renseignements et a amené un conflit avec certains juges européens, dont les juges français (*v. supra*).

[26] V. *affaire Solange* entre la Cour constitutionnelle allemande et la CJCE (*Solange et Solange II*).
[27] Arrêt du 18 juillet 2013 dit *Kadi II*.
[28] Arrêt du 16 décembre 2016, *Tele2 Sverige*.

34. Par leurs décisions, les juges européens se portent comme de réels protecteurs des libertés de chaque ressortissant européen. Elles permettent une amélioration des législations internes en matière d'encadrement du renseignement. Même si leur action est parfois qualifiée d'enlisant par les services de renseignement, elle participe à légitimer leur action. De plus, cette action permet à chaque État européen d'avoir un régime (minimal) commun, ce qui permet une coopération entre les services européens.

Paragraphe 2 : Un contrôle complet réalisé par la Cour EDH sur le régime juridique encadrant les activités de renseignement

35. ***Rappels***. La juridiction de Strasbourg est connue pour son interprétation extensive et libérale de la CEDH. Depuis la ratification de cette dernière par la France, les décisions rendues par la Cour EDH ont amené le législateur français à réaliser de nombreuses réformes. Par exemple, la condamnation de la France dans l'arrêt Kruslin et Huvig a amené les premiers encadrements pour le recours à certaines techniques de renseignement. Autre exemple, le développement, par la Cour EDH, de l'exigence du droit à un avocat pendant la garde à vue a amené le législateur français à repenser le régime de la garde à vue[29].

En ce qui concerne le régime juridique assujetti aux activités de renseignement, la Cour n'hésite pas à réaliser un contrôle sur l'entièreté du régime. Ce contrôle peut autant être réalisé sur le fondement du droit à la vie privée (article 8 de la CEDH) que sur les droits de la défense (article 6 de la CEDH), voire sur celui de la liberté d'expression (article 10 de la CEDH). Plusieurs régimes ont déjà été passés au crible par la Cour. Pendant ses contrôles, elle en profite pour préciser ses exigences concernant des points précis, c'est le cas notamment pour les échanges de renseignement entre services ne relevant pas du même État.

36. ***Le cas britannique : l'arrêt Big Brother Watch.*** Dans un arrêt récent en date du 25 mai 2021[30], la Cour EDH a pu se prononcer sur le régime mis en place par le Royaume-Uni concernant

[29] V. à ce titre : Cour EDH, *arrêt Salduz c. Turquie* (27 novembre 2008) et *Brusco c. France* (14 octobre 2010), ainsi que la QPC, Daniel W. et autre, 30 juillet 2010.
[30] Cour EDH, *Big Brother Watch contre Royaume-Uni*, 25 mai 2021.

l'encadrement des activités de renseignement. Par cet arrêt, la Cour rappelle que l'État peut porter des atteintes aux droits et libertés des administrés (sauf en ce qui concerne l'interdiction de la torture et des traitements inhumains et dégradants) afin de garantir la sécurité nationale, à la condition que ces atteintes soient autorisées et définies par des critères au préalable. Ici, la Cour ne fait que rappeler ce que prévoit la convention, notamment à son article 8 paragraphe 2.

Après avoir rappelé ce principe, la juridiction de Strasbourg réalise un contrôle entier sur le régime juridique britannique. Ici, le texte principal attaqué par les requérants était le *Regulation of Investigatory Powers Act* (RIPA), entré en vigueur en 2000. Les requérants estimaient ce texte contraire aux articles 8 et 10 de la convention. La « *RIPA* » est la loi qui encadre les interceptions de masse des communications. De plus, étaient également attaqués, le régime de réception des renseignements venant de l'étranger ainsi que le régime réglementant l'accès par les pouvoirs publics aux données conservées par les fournisseurs de services de communication[31].

37. ***L'arrêt Big Brother Watch : le contrôle de l'encadrement des techniques relatives à la surveillance généralisée***. La Cour vient sanctionner le Royaume-Uni pour violation des articles 8 et 10 de la convention. Elle retient que la loi britannique ne répond pas aux exigences de « *qualité de la loi* », autrement dit que la loi était trop opaque. En effet, la Cour s'est estimée préoccupée, d'une part, en raison de « *l'absence de supervision sur la sélection des canaux de transmission visés par les interceptions, sur les sélecteurs utilisés pour le filtrage des communications interceptées et sur le processus de sélection par les analystes des communications interceptées à examiner* ». D'autre part, la Cour s'est inquiétée concernant « *l'absence de garanties réelles applicables à la recherche et à la sélection pour examen des données de communication associées* »[32]. Elle se montre, par le présent arrêt, exigeante concernant les garanties que doivent apporter les régimes de chaque État concernant les interceptions généralisées. Elle estime qu'en l'espèce le régime britannique ne « *renfermait pas suffisamment de garanties « de bout en bout » pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus, en dépit des garde-fous qu'il comportait, dont certains ont été jugés solides* ». Par la présente position, la Cour exige la présence d'une réelle protection afin d'éviter une dérive, mais elle ne s'oppose pas à ces

[31] V. point 266 de l'arrêt.
[32] V. point 276 de l'arrêt.

procédés visant la surveillance de masse des données. Il était reproché au cas britannique de ne pas subordonner le recours auxdites techniques à une autorisation conférée par un organe indépendant. Par conséquent, pour recourir à des procédés de surveillance de masse, les États doivent amener en contrepartie des « *garanties de bout en bout* ». De plus, la mise en place de ces mesures doit être nécessaire et proportionnée. Et ce n'est pas tout, en plus des exigences précitées, la Cour rappelle que la loi doit comprendre six critères[33] afin d'éviter les abus de pouvoir. La loi doit prévoir pour quels types d'infractions les techniques peuvent être mises en place, définir le type de personnes concernées par les interceptions, fixer la limite concernant la durée de la mesure, prévoir la procédure à suivre pour l'examen, encadrer « *l'utilisation et la conservation des données recueillies* », préciser « *les précautions à prendre pour la communication des données à d'autres parties* », et enfin prévoir « *les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites* ». Ici encore, elle estime que la loi britannique n'apporte pas les garanties énoncées.

38. ***L'arrêt Big Brother Watch : le contrôle des échanges de renseignements***. La Cour précise les exigences demandées concernant le partage de renseignements entre services relevant d'États différents. Encore une fois, elle ne s'oppose pas à ces échanges, mais exige que le droit des États concernés doive apporter des garanties et que ces transferts doivent faire l'objet d'un contrôle indépendant. Plus précisément, la Cour distingue les renseignements entrants et les renseignements sortants. Pour les premiers, l'État doit prévoir un fondement légal aux demandes de renseignements et l'État destinataire doit mettre en place des garanties suffisantes concernant la conservation, le traitement, le transfert et la destruction des renseignements reçus, et ce afin d'éviter d'éventuels contournements. Pour les seconds, le droit interne doit prévoir la possibilité et les cas dans lesquels les transferts de renseignements à un État tiers peuvent avoir lieu. Enfin, l'État expéditeur doit veiller à ce que l'État destinataire ait bien mis en place les garanties suffisantes afin d'éviter les abus. La Cour réalise finalement le même raisonnement que pour les violations par ricochet de l'article 2. En l'espèce, le droit britannique amène les garanties nécessaires.

39. ***Le régime français face à la prochaine décision de la Cour EDH***. Le 19 avril 2017, plusieurs requérants ont réalisé un recours contre la loi du 24 juillet 2015. Parmi ces requérants se

[33] V. point 274 de l'arrêt.

trouvent notamment des journalistes, des associations de défense des droits et des avocats[34]. Ils arguent que la loi du 24 juillet 2015 ne satisfait pas aux exigences d'une base légale suffisante, notamment car elle ne définit pas la notion d' « *informations ou documents* ». Plus largement, les requérants avancent que le dispositif de surveillance mis en place par ladite loi n'est pas proportionné (« *car la loi excède ce qui est strictement nécessaire à la préservation des institutions démocratiques* »[35]). Enfin, ils estiment que l'encadrement mis en place n'offre pas de garanties suffisantes quant au respect de la confidentialité des échanges entre avocats ou entre avocats et clients.

La Cour EDH devrait se prononcer sur ces requêtes dans un futur proche. À la lumière de ce qu'elle a fait pour le régime britannique en 2021, elle devrait passer au crible l'ensemble du dispositif d'encadrement français amené par la loi du 24 juillet 2015, en prenant en compte ses modifications ultérieures. Il existe plusieurs failles dans ce dispositif législatif qui pourraient entraîner la condamnation de la France (l'absence de contrôle sur les échanges internationaux de renseignements, la procédure devant la formation spécialisée, etc.). Ces failles seront traitées par la suite (v. infra).

40. ***Remarques générales.*** Le contrôle complet réalisé par la Cour EDH amène plusieurs avantages non négligeables. D'une part, il permet de veiller à ce que le régime d'encadrement des activités de renseignement apporte les garanties suffisantes aux droits et libertés protégés par la convention. Sur ce point, le juge de Strasbourg réalise un contrôle pointu et exigeant, tout en préservant une liberté d'action aux services de renseignement. D'autre part, ce contrôle permet de veiller à ce que l'ensemble des régimes européens aient des garanties minimales, ce qui permet, entre autres, l'échange de renseignement entre services relevant d'États différents. Ce dialogue des juges est donc grandement bénéfique aux droits et libertés de chaque Européen. Cependant, le dialogue mis en place au sujet des activités de renseignement peut amener à un conflit. Ces conflits, non inhérents au domaine étudié, sont cependant d'une ampleur importante dans le domaine des activités de renseignement.

[34] L'ordre des avocats au barreau de Paris et le Conseil national des barreaux font partie des requérants.
[35] Cour EDH, communiqué du 26 avril 2017 (requête n° 49526/15).

Section 2 : Le désaccord entre la France et la Cour de justice au sujet de l'obligation générale et indifférenciée de conservation des données

41. ***Annonce.*** Le dialogue des juges peut - certes - être bénéfique pour la protection des libertés de chaque ressortissant européen. Or, en matière de renseignement, c'est-à-dire dans un domaine régalien, les échauffourées entre le juge européen et les juges nationaux ont atteint leur paroxysme. Dans un contexte où les juridictions internes réaffirment parfois avec maladresse[36] la supériorité du droit constitutionnel interne, ou du moins une partie, sur le droit européen[37]. L'un des plus grands désaccords entre le juge administratif français, représenté par le Conseil d'État, et la Cour de justice prend place dans le cadre des activités de renseignement. Ce désaccord concerne l'obligation générale et indifférenciée de conservation des données faites aux opérateurs téléphoniques et l'accès par les pouvoirs publics à ces données. L'accès aux données est primordial pour les services de renseignement, notamment à l'heure du développement de nouvelles techniques algorithmiques.

Les exigences posées par la Cour de justice en matière de conservation des données sont complexes à cerner et parfois critiquées par les services de renseignements, mais sont d'une certaine manière logiques (***paragraphe 1***). Ces exigences ont été réceptionnées par le Conseil d'État et les pouvoirs publics d'une manière conflictuelle, ce qui a donné lieu à un véritable dialogue entre les deux juridictions en différend (***paragraphe 2***).

Paragraphe 1 : La position actuelle critiquée de la Cour de justice

42. ***Contextualisation.*** Pour rappel, la Charte des droits fondamentaux garantit la protection de la vie privée (article 7) ainsi que celle des données personnelles (article 8). Sur ce texte, la Cour de justice a développé une jurisprudence notamment en ce qui concerne la conservation des

[36] Dans un arrêt du 5 mai 2020, concernant les programmes de rachat de dettes publiques par le SEBC, la Cour constitutionnelle allemande a considéré que la BCE avait agi en dehors de ses compétences (ultra vires). Or, en principe, seule la Cour de justice peut constater qu'un organe de l'UE agit en dehors de ses compétences.

[37] Dans ce cadre, le Conseil constitutionnel a décelé le premier principe inhérent à l'identité constitutionnelle de la France dans sa décision QPC, *société Air France* du 15 octobre 2021.

données personnelles. Dès 2014[38], la Cour du Luxembourg a, par un arrêt rendu en grande chambre, déclaré non conforme au droit primaire de l'Union européenne la directive 2006/24/CE relative à la conservation des données. Cette directive prévoyait notamment une obligation faite aux « *fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications* » de conserver les données de leurs utilisateurs, pour une durée allant de minimum six mois à maximum deux ans, afin de « *garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne* ». Ici, la présente directive définit les données comme « *les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur* » (article 2). De plus, la directive listait l'ensemble des données devant être conservées (article 5)[39]. Cette directive a été déclarée non conforme au droit primaire, car elle portait, d'une part, une ingérence particulièrement grave aux articles 7 et 8 de la Charte des droits fondamentaux, et d'autre part, elle n'était pas suffisamment encadrée.

43. ***Arrêt Tele2 Sverige AB***. Par un arrêt de 2016[40], la Cour de justice va poser une interdiction générale. En effet, selon elle, le droit de l'UE s'oppose à ce que les États membres prévoient, afin de lutter contre la criminalité, une obligation de conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et à la localisation des utilisateurs (« *surveillance de masse* »). En l'espèce, la Cour de justice avait été saisie à titre préjudiciel par des juridictions suédoise et britannique afin de savoir si cette obligation générale et indifférenciée était compatible avec le droit de l'UE. Même si cet arrêt s'inscrit dans la continuité de l'arrêt rendu en 2014, il n'en a pas moins constitué un coup de tonnerre parmi les acteurs du renseignement et de la police judiciaire. En effet, l'accès aux données conservées constitue le fer de lance de leur activité, pour preuve environ 50 000 demandes d'autorisation d'accès à ces données sont autorisées par le Premier ministre chaque année[41]. Malgré cet arrêt rendu par la Cour de justice, plusieurs États membres, dont la France et le Royaume-Uni, ont continué à obliger les fournisseurs à conserver,

[38] Arrêt du 8 avril 2014, *Digital Rights Ireland Ltd*.
[39] Ici, ne sont pas visés les contenus des échanges, mais « *juste* » les données permettant d'identifier les utilisateurs ainsi que leur localisation et l'heure des échanges (ce sont les « métadonnées »).
[40] Arrêt (grande chambre) du 21 décembre 2016, *Tele2 Sverige AB*.
[41] V. Rapport d'activité de la CNCTR pour 2021, p. 33.

de façon générale et indifférenciée, les données de leurs utilisateurs. La pratique de ces États était donc contraire au droit de l'UE…

44. ***Arrêt Quadrature du Net : le contexte***. Face au non-respect par certains États membres de l'interdiction posée par la Cour de justice en 2016, un contentieux, impulsé par les associations protégeant les utilisateurs, est né devant les juridictions internes. Le Conseil d'État fut alors saisi[42] afin d'annuler l'article R. 10-13 du code des postes et communications électroniques (CPCE) et le décret n° 2011-219 du 25 février 2011[43]. Ces deux textes réglementaires fondaient textuellement l'obligation générale et indifférenciée de conservation des données faite aux fournisseurs téléphoniques. Dans un arrêt du 26 juillet 2018[44], le Conseil d'État va sursoir à statuer et poser une question préjudicielle à la Cour de justice. La question principale posée repose sur le fait de savoir si l'obligation générale et indifférenciée de conservation des données imposée sur le fondement de l'article 15 de la directive du 12 juillet 2002[45] n'est pas, notamment au regard des garanties et contrôles de l'utilisation de ces données, une ingérence justifiée par le droit à la sûreté (garanti à l'article 6 de la Charte des droits fondamentaux) et la préservation de la sécurité nationale (« *qui incombe aux seuls États membres en vertu de l'article 4 du TUE* »). Autrement dit, le Conseil d'État demande à la Cour de justice de revoir sa position. Le Conseil d'État a aussi profité de l'occasion pour rappeler l'importance, notamment pour le pouvoir judiciaire, de cette obligation générale de conservation. Il rappelle aussi que cette obligation ne porte pas sur le contenu des communications, et que par conséquent l'atteinte est moindre. À noter qu'une question préjudicielle similaire a aussi été posée par la Cour constitutionnelle belge et une juridiction britannique.

45. ***Arrêt Quadrature du Net : la confirmation***. Sans revenir sur le principe d'interdiction d'une conservation généralisée et indifférenciée des données, la Cour de justice a admis l'importance des objectifs de protection de la sécurité nationale et de lutte contre la criminalité

---

[42] Notamment par l'association French Data Network.
[43] Relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.
[44] Pourvoi n°394922.
[45] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

grave, qui contribuent à la protection des droits et libertés d'autrui. Par cet arrêt, la Cour du Luxembourg est - tout de même - venue préciser le régime applicable à la conservation des données.

Désormais, la Cour de justice considère que la conservation générale et indifférenciée des données relatives à l'identité civile présente une très faible sensibilité et est donc une ingérence faible. L'obligation de conservation de ce type de données peut donc être conférée pour la « *lutte contre la criminalité et prévention des menaces contre la sécurité publique en général*», ainsi que la « *lutte contre la criminalité grave et prévention des menaces graves pour la sécurité publique* » et la « *sauvegarde de la sécurité nationale* ».

Concernant la conservation des adresses IP, la Cour estime que cette conservation entraîne une ingérence grave. Par conséquent, l'obligation générale et indifférenciée de conservation de ce type de données peut uniquement être justifiée par la « *lutte contre la criminalité grave et la prévention des menaces graves pour la sécurité publique* » ainsi que la « *sauvegarde de la sécurité nationale* ».

Enfin, pour la conservation des autres types de données (localisation, données de trafic, etc.), le principe de l'interdiction de l'obligation de conservation générale et indifférenciée demeure. Il n'existe pas d'exception possible quand l'objectif sera de lutter contre les infractions pénales ordinaires. Lorsque l'objet de la conservation sera de « *lutter contre la criminalité grave et de prévenir les menaces graves pour la sécurité publique* », soit les données pourront être conservées selon des critères personnels et géographiques (conservation ciblée) soit les données pourront être conservées dans le cadre de la « *conservation rapide* »[46]. Par exception, lorsque l'objet de la conservation sera la sauvegarde de la sécurité nationale, au vu de l'importance de cet objectif, l'obligation de conservation générale des données pourra être prononcée si trois conditions sont réunies : présence d'une menace grave, actuelle et réelle ou prévisible à la sécurité nationale ; limitation au strict nécessaire de la durée de l'obligation (peut être renouvelée, mais ne doit pas être systématique) ; existence d'un contrôle juridictionnel ou celui d'une AAI dotée d'un pouvoir

[46] Terme issu de la convention de Budapest (2001). Cette dernière fait obligation aux États de prévoir cette conservation rapide pour une durée maximale de 90 jours afin de lutter contre la cybercriminalité, notamment en vue de garantir la conservation de preuves.

contraignant qui vérifiera le respect des deux premières conditions notamment. Cette dernière condition vaut également pour les demandes d'accès des pouvoirs publics aux données conservées.

La Cour de justice a donc décidé de distinguer différents types de données et de leur appliquer, en fonction de l'impact qu'a la conservation de ces dernières sur le droit au respect de la vie privée, un régime de conservation plus ou moins restrictif.

46. ***La définition de la sécurité nationale***. La Cour de justice donne une définition de ce qu'elle entend par la notion de sécurité nationale. Selon elle, la notion renvoie à « *l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme* »[47]. La Cour continue « *or, l'importance de l'objectif de sauvegarde de la sécurité nationale* » (…) « *dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique* »[48]. Il en ressort donc clairement que la lutte contre la criminalité grave ne fait pas partie de la sécurité nationale. Cette définition donnée par la Cour de justice ressemble de près à la définition donnée par le droit français que cela soit par l'article L1111-1 du C.déf[49] ou par ses retranscriptions dans la notion d'intérêts fondamentaux de la Nation[50]. Or, l'article L811-3 du CSI mentionne comme faisant partie des intérêts fondamentaux de la Nation, et donc justifiant la mise en place de techniques de renseignement (y compris l'accès aux données conservées), « *la prévention de la criminalité et de la délinquance organisées* ». Cette différence de ligne, entre la France et l'UE, concernant le contenu de la notion de sécurité nationale,

---

[47] V. point 135 de l'arrêt *Quadrature du Net*.
[48] V. point 136 de l'arrêt *Quadrature du Net*.
[49] « *La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter* (…) ».
[50] V. article 410-1 code pénal : « *Les intérêts fondamentaux de la nation s'entendent (…) 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 ».*

posait et pose encore un problème (v. infra). En toute logique, la France devrait, en raison du principe de supériorité du droit de l'UE[51], adapter les textes sur la définition donnée par le droit de l'UE.

47. ***Arrêt Quadrature du Net : remarques.*** Le régime évoqué par la Cour de justice nécessite plusieurs remarques. D'une part, le régime mis en place par la Cour du Luxembourg permet, pour sauvegarder la sécurité nationale et sous certaines conditions, de mettre en place une obligation générale et indifférenciée de conservation de toutes les données. Le juge européen se montre donc plus souple que dans son arrêt rendu en 2016, il ne s'agit donc pas d'une « *confirmation* » pure et simple de l'arrêt Sverige, comme l'expliquent certains[52] (même si le principe reste l'interdiction générale). Concernant le renseignement administratif, une obligation générale et indifférenciée portant sur l'ensemble des types de données peut donc être mise en place lorsqu'une « *menace grave, actuelle et réelle ou prévisible à la sécurité nationale* » est présente ; autrement dit, pour lutter contre le terrorisme, lorsque cette menace comprend les critères mentionnés, cette obligation peut être mise en place (pas perpétuellement). En revanche, concernant le volet judiciaire, comme l'affirme François Molins[53], cette interdiction de principe risque d'être « *un désastre* » susceptible d' « *entraver très sérieusement* » les enquêtes pénales. En effet, même si les mots de F. Molins sont forts, les enquêteurs n'auront plus accès aux données conservées par les fournisseurs sur une durée d'un an, et pourront plus difficilement obtenir des preuves de la culpabilité (ou de l'innocence) d'un mis en cause.

D'autre part, de façon générale, cette actualisation plus permissive de l'arrêt Sverige paraît être un sage équilibre. En effet, à l'heure des risques d'une surveillance de masse, permettre la conservation généralisée et indifférenciée au seul cas où la sécurité nationale doit être sauvegardée semble être pertinent. Le principal bémol serait la baisse d'efficience des enquêtes pénales. Sur le plan du renseignement administratif, cette limite peut, malgré les critiques venant des acteurs du renseignement, être qualifiée de raisonnée, car il faut l'admettre ces dernières années ont été marquées par une observation générale de pérennisation de mesures exceptionnelles dans

[51] Relevé pour la première fois dans l'arrêt CJUE, *Costa c. Enel*, 1964.
[52] V. *la justice de l'UE s'oppose à la collecte massive des données de connexions Internet et téléphoniques par les États*, Le Monde, 6 octobre 2020.
[53] *Ibid*.

l'ordonnancement juridique[54]. De plus, les contrôles mis en place en 2015 restent récents et n'ont pas encore démontré toute leur efficience. Enfin, est-ce qu'il est légitime de conserver l'ensemble des données de chaque client de fournisseurs, c'est-à-dire des citoyens, pour surveiller une infime partie d'entre eux qui tremperaient dans la criminalité grave et pourraient causer des menaces graves à la sécurité publique ? Avoir un droit trop permissif pourrait être utilisé à mauvais escient dans un futur proche par des dirigeants peu soucieux des libertés de chacun. D'autant plus que cette limitation - au strict minimum - par la Cour de justice de l'obligation indifférenciée et générale de conservation n'empêche pas les services de renseignement de se voir octroyer la permission de recourir à de nouvelles techniques à la pointe de la technologie, voire de mettre en place une conservation ciblée. À titre d'exemple, la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement permet définitivement (cela avait été prévu à titre expérimental jusqu'ici) aux services de renseignements de recourir à des algorithmes de surveillance[55]. À noter que sur ce point, la CNIL explique, dans l'un de ses avis[56], que « *l'utilisation d'une telle technique porte une atteinte particulièrement forte à la vie privée des individus et au droit à la protection des données à caractère personnel* ».

Paragraphe 2 : La réception partielle en droit français

48. ***L'arrêt French Data Network***. Dans un arrêt rendu par l'assemblée contentieuse du Conseil d'État, les conséquences de l'arrêt Quadrature du Net vont être tirées[57]. Le Gouvernement français, en tant que défenseur des règlements attaqués, avançait que l'interprétation de la directive[58] rendue par la CJUE méconnaissait les principes constitutionnels de sauvegarde des intérêts fondamentaux de la Nation ainsi que les objectifs à valeur constitutionnelle de sauvegarde de l'ordre public et de

[54] V. loi SILT (2017) et loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

[55] Cette technique est prévue à l'article L851-3 du CSI. Elle permet de mettre en place des critères (URL par exemple) de surveillance sur les données des utilisateurs de réseaux ouverts par les fournisseurs en temps réel. Autrement dit, elle permet de détecter une connexion susceptible de révéler une menace terroriste. Cette technique renvoie donc directement à ce qu'on peut entendre par surveillance de masse, ce qui explique pourquoi elle peut être utilisée uniquement pour prévenir le terrorisme et qu'elle est soumise à un formalisme très précis.

[56] CNIL, Délibération n°2021-040 du 8 avril 2021, para. 24.

[57] Conseil d'État, assemblée, 21 avril 2021, *French Data Network*, publié au recueil Lebon, n°393099.

[58] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

recherche des auteurs d'infractions, et donc qu'annuler lesdits décrets serait contraire à ces derniers. De plus, à la lumière de ce qu'avait fait la Cour constitutionnelle allemande[59], il demandait au Conseil d'État de constater que la Cour de justice a agi ultra vires, c'est-à-dire en dehors de ses compétences attribuées par le droit primaire de l'UE.

49. Après avoir refusé de constater l'ultra vires, le Conseil d'État va recourir au contrôle d'équivalence qu'il a mis en place une dizaine d'années plus tôt dans l'arrêt Arcelor[60]. Pour rappel dans ce dernier, le Conseil d'État avait présenté deux cas de figure (lorsqu'un décret reprenait une directive précise et inconditionnelle) : soit il existe une équivalence en droit européen au principe constitutionnel invoqué, et par conséquent, le juge contrôle la conformité de l'acte à ce principe équivalent (si acte clair, a contrario il pose une question préjudicielle), soit il n'existe pas d'équivalent, le juge examinera alors la constitutionnalité de l'acte administratif attaqué (revient à un contrôle indirect de constitutionnalité de la directive). Cependant, en l'espèce, contrairement à l'affaire Arcelor, le gouvernement souhaite le maintien d'une disposition ; ce dernier estimant que c'est l'interprétation de la CJUE concernant la directive qui est contraire à des principes constitutionnels. Autrement dit, si le juge administratif décidait de reconnaitre les actes réglementaires attaqués contraires au droit de l'UE, cela reviendrait à priver d'effectivité les exigences constitutionnelles évoquées. Le Conseil d'État, après avoir estimé que le droit européen n'apportait pas une équivalence aux principes constitutionnels invoqués, va retenir que l'obligation de conservation générale et indifférenciée des données est nécessaire à la garantie desdites exigences constitutionnelles. Plus précisément concernant l'obligation de conservation générale et indifférenciée, le CE a estimé cette dernière conforme au droit de l'UE car la France était confrontée à une « *menace grave, réelle, actuelle et prévisible* » concernant sa sécurité nationale[61].

50. Cependant, le Conseil d'État constate, d'une part, que les actes réglementaires ne prévoient pas un réexamen périodique pour vérifier si les caractères liés à la menace sur la sécurité nationale (qui justifient l'obligation générale et indifférenciée de l'ensemble des données) sont encore actuels. D'autre part, il constate que les actes réglementaires attaqués ne limitent pas les finalités

[59] Cour constitutionnelle fédérale allemande, arrêt du 5 mai 2020.
[60] Conseil d'État, assemblée, 8 février 2007, *Société Arcelor*, n°287110, publié au recueil Lebon.
[61] Terrorisme, risque d'ingérence étrangère, augmentation du radicalisme.

de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation. Autrement dit, lesdits actes ne présentent pas les garanties exigées par la Cour de justice, ce qui explique pourquoi le Conseil d'État annule les décisions de refus d'abrogation du Premier ministre et enjoint ce dernier à annuler ou modifier le décret du 25 février 2011 et l'article R. 10-13 du CPCE dans un délai de six mois.

51. Le Conseil d'État devait aussi se pencher sur le régime français concernant l'accès des pouvoirs publics aux données conservées par les fournisseurs. Pour rappel, dans l'arrêt Quadrature du Net, la Cour de justice exige que l'accès par les pouvoirs publics aux données conservées soit soumis à un contrôle juridictionnel ou à celui d'une autorité administrative indépendante dotée d'un pouvoir contraignant. Ici, le Conseil d'État constate que ces exigences ne sont pas respectées. En effet, la CNCTR ne dispose pas d'un pouvoir contraignant dans le cadre de son contrôle a priori et la formation spécialisée du Conseil d'État ne pouvait (à la date de l'arrêt) qu'être saisie après la décision du Premier ministre. Nonobstant une contrariété avec le droit de l'UE, après avoir constaté que le Premier ministre n'avait jamais outrepassé un avis défavorable de la CNCTR, le Conseil d'État ne prononce pas l'annulation des textes visés, mais demande que soit procédé à la mise en conformité du droit national avec les exigences posées par la Cour de justice.

52. ***Arrêt Dwyer : une nouvelle mise en garde pour la France***. Cet arrêt rendu par la grande chambre de la Cour de justice[62] concernait l'Irlande. Cependant, la Cour du Luxembourg profite de ce dernier pour rappeler les principes déjà évoqués dans l'arrêt Quadrature du Net. De plus, elle rejette encore « *l'argumentation selon laquelle les autorités nationales compétentes devraient pouvoir accéder, aux fins de la lutte contre la criminalité grave, aux données »* (…) *« qui ont été conservées »* (…) *« pour faire face à une menace grave pour la sécurité nationale* ». Ce rappel s'adresse indirectement à la France, et peut être qualifié de mise en garde. Ici, la Cour est claire, il est impossible pour les pouvoirs publics d'accéder aux données conservées de manière générale et indifférenciée dans le cadre d'une menace à la sécurité nationale pour une autre raison que cette dernière. Autrement dit, selon la CJUE, une autorité de police judiciaire ou un service de renseignement ne peut pas accéder, dans le cadre de la prévention ou d'une enquête relative à la criminalité grave, aux données conservées de manière générale et indifférenciées (dans leur

[62] CJUE, grande chambre, 5 avril 2022, *Dwyer*.

totalité) dans l'optique de lutter contre une menace pour la sécurité nationale. Là encore, ce point semble logique, à quoi sert-il de limiter la conservation générale et indifférenciée au cas où la sécurité nationale est menacée, si c'est pour que dans un second temps, les services étatiques puissent accéder à ces données pour des raisons sans rapport avec la sécurité nationale. Encore une fois, cet arrêt rappelle que les États peuvent mettre en place des obligations de conservation des données limitées géographiquement et par le nombre de personnes visées, voire mettre en place des obligations générales et indifférenciées de conservation des données concernant les adresses IP.

53. ***Le droit actuel concernant la conservation des données en France.*** Ce dialogue des juges a eu pour conséquence une modification du droit français concernant les obligations de conservation auxquelles sont assujettis les fournisseurs.

Premièrement, la loi du 30 juillet 2021[63] et le décret du 20 octobre 2021[64] viennent modifier respectivement l'article L. 34-1 et l'article R. 10-13 du CPCE. Avant cette modification, l'article L. 34-1, dans son troisième point, prévoyait que l'obligation de destruction des données de chaque utilisateur pouvait être différée « *pour une durée maximale d'un an* ». Cet article était complété par l'article R. 10-13, ce dernier fut annulé par le Conseil d'État dans l'arrêt de 2021 car il mettait en place une obligation générale et indifférenciée de conservation des données.

Aujourd'hui, l'article L. 34-1 est bien plus détaillé. Il prévoit une distinction entre les différents types de données comme la Cour de justice l'exige. Il précise que les « *opérateurs de communications électroniques* » doivent conserver les informations relatives à l'identité civile de l'utilisateur[65] et aux paiements[66] pour les besoins de la procédure pénale et la prévention de la sécurité publique et des atteintes à la sécurité nationale. Selon l'article R. 10-13 ces informations renvoient à la fois au « *nom et prénom, la date et le lieu de naissance pour une personne physique ou la raison sociale, ainsi que les nom, prénom, date et lieu de naissance de la personne agissant en son nom, lorsque le compte est ouvert au nom d'une personne morale* » ainsi que « *la ou les*

[63] LOI n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.
[64] Décret n° 2021-1361 du 20 octobre 2021 relatif aux catégories de données conservées par les opérateurs de communications électroniques, pris en application de l'article L. 34-1 du CPCE.
[65] « Sur une durée de 5 ans à compter de la fin de validité du contrat ».
[66] « Jusqu'à l'expiration d'un délai d'un an à compter de la fin de validité de son contrat ou de la clôture de son compte ».

adresses postales associées, la ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant » et « *le ou les numéros de téléphone* ». Concernant le paiement, les fournisseurs doivent conserver « *le type de paiement utilisé* », « *la référence du paiement* », « *le montant* » ainsi que « *la date, l'heure et le lieu en cas de transaction physique* ».

De plus, pour lutter contre la criminalité et la délinquance grave, pour prévenir des menaces graves contre la sécurité publique ou pour sauvegarder la sécurité nationale, les fournisseurs sont tenus de conserver, pour une durée d'un an[67], les données permettant « *d'identifier la source de la connexion* » ou les données relatives au type d'appareil utilisé. Figurent parmi ces données, toujours selon l'article R. 10-13, « *l'adresse IP attribuée à la source de la connexion et le port associé* », « *le numéro d'identifiant de l'utilisateur* », « *le numéro d'identification du terminal* » ainsi que « *le numéro de téléphone à l'origine de la communication* ».

Enfin, l'article prévoit la possibilité faite au Premier ministre, par décret pris en Conseil d'État, d'enjoindre aux fournisseurs de conserver, pour une durée d'un an, les données relatives aux données de trafic et de localisation lorsque la sécurité nationale fait face à une menace grave, actuelle ou prévisible. Il s'agit donc de la retranscription, par le législateur, de la jurisprudence Quadrature du Net dans l'ordonnancement juridique français. Cette appréciation des caractères de la menace par le Premier ministre, retranscrite dans le décret, sera susceptible d'être contrôlée par juge administratif dans un futur contentieux. Reste à savoir quel type de contrôle sera exercé le cas échéant par le Conseil d'État : contrôle restreint ou contrôle entier ? Encore une fois, l'article R. 10-13 précise le type de données compris. Sont donc comprises « *les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication* », « *les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs »,* « les données techniques permettant d'identifier le ou les destinataires de la communication » ainsi que « *pour les opérations effectuées à l'aide de téléphones mobiles, les données permettant d'identifier la localisation de la communication* ».

Deuxièmement, la loi du 30 juillet 2021 vient également modifier l'article 6 de la loi de 1978 (pour la confiance dans l'économie numérique)[68] pour permettre, dans l'hypothèse d'une

[67] « *À compter de la connexion ou de l'utilisation des équipements terminaux* ».
[68] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

menace grave, actuelle ou prévisible à la sécurité nationale, au Premier ministre d'exiger la conservation générale et indifférenciée des données pour une durée d'un an.

54. ***Conclusion section***. L'arrêt Quadrature du Net a donc bouleversé le régime juridique de conservation des données. Ce dernier était trop permissif. Le régime actuel semble donc allier la performance des services de renseignement avec la protection des clients de fournisseurs, même si forcer de le reconnaitre, les autorités publiques ont vu leurs prérogatives atteintes par cette évolution. Cependant, la France ne reste pas à l'abri d'un nouvel arrêt de la CJUE la concernant. En effet, l'accès aux données conservées de manière générale et indifférenciée dans le cadre exceptionnel d'une menace contre la sécurité nationale n'est pas autorisé dans le cadre de la lutte contre la criminalité grave. Or, la France n'a pas encore réglé ce problème. De plus, il est important de rappeler que le Conseil d'État réalisera un contrôle de légalité sur le décret du Premier ministre obligeant les fournisseurs à procéder à une conservation générale et indifférenciée, voire sur le décret visant à prolonger la mesure. Ce contrôle devrait notamment viser l'appréciation faite par le Premier ministre des caractères de la menace (grave, actuelle et réelle ou prévisible).

55. ***Conclusion de chapitre*****.** D'une manière générale la jurisprudence européenne n'a pas eu seulement des répercussions sur la conservation des données, mais a poussé les États européens, dont la France, à perfectionner leur régime de contrôle des activités de renseignement. Les juges européens s'inscrivent donc dans une optique visant à garantir l'exercice des libertés protégées par les textes, qui forcé de le reconnaître, se heurte parfois avec la vision sécuritaire (pas toujours à juste titre) des États. Le contentieux européen a emmené le législateur français à renforcer les procédures de contrôle, notamment en ce qui concerne le contrôle a priori réalisé par la CNCTR.

CHAPITRE 2 : LE RENFORCEMENT DU CONTRÔLE A PRIORI PAR LE LÉGISLATEUR

56. ***Annonce.*** La loi du 30 juillet 2021[69], relative à la prévention d'actes de terrorisme et au renseignement, vient, malgré son volet principal sécuritaire[70], renforcer le contrôle des activités de renseignement[71]. Sous l'impulsion du droit européen, la CNCTR s'est vu être dotée d'une plus grande importance, notamment dans le contrôle a priori (***section 1***). De plus, l'action du législateur vient augmenter le rôle d'autres organes de contrôle qui exercent un contrôle plus indirect sur les activités de renseignement (***section 2***).

Section 1 : Le renforcement du rôle et des prérogatives de la CNCTR dans le contrôle a priori

57. Depuis sa création par la loi du 24 juillet 2015, la CNCTR rend un avis préalable avant l'autorisation du Premier ministre pour chaque demande de mise en place d'une des techniques prévue par le Livre VIII du CSI. Cet avis est, depuis 2015 jusqu'à aujourd'hui, non obligatoire. À titre d'exemple, la CNCTR a rendu, pendant l'année 2021, 87 588 avis dans le cadre de son contrôle a priori. Le nombre d'avis rendu a connu une augmentation de 10 % entre 2020 et 2021[72]. Cette augmentation est due, en grande partie, à la baisse d'activité des services de renseignement pendant la crise sanitaire.

58. ***Annonce.*** La CNCTR a pu, depuis presque huit ans d'existence, perfectionner son contrôle. De plus, elle a vu l'impact de ses avis renforcé par le législateur sous l'impulsion des jurisprudences européennes. Il convient donc de se demander si la CNCTR est devenue un véritable garde-fou (***paragraphe 1***). Enfin, il est intéressant de comparer les prérogatives dont est dotée la CNCTR par rapport aux autres organes de contrôle des démocraties européennes, afin de savoir si, sur ce point, la France a rattrapé le retard sur ses pairs (***paragraphe 2***).

---

[69] Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.
[70] Rend pérenne notamment des mesures de police administrative prévue par la loi SILT (2017).
[71] Et modifier le régime de conservation des données (v. supra).
[72] V. p. 62, *6ème Rapport d'activité 2021* de la CNCTR.

Paragraphe 1 : La CNCTR : véritable garde de fou

59. ***Le type de contrôle exercé a priori par la CNCTR***. Le contrôle réalisé par cette autorité administrative indépendante est, nonobstant la célérité[73] à laquelle le contrôle doit répondre, relativement complet. L'article L801-1 du CSI charge la CNCTR de s'assurer du respect des principes invoqués dans l'article. Autrement dit, elle est chargée premièrement de veiller à ce que la demande de technique de renseignement poursuive l'un des sept items prévus à l'article L811-3. De plus, elle doit aussi vérifier, toujours selon l'article L801-1, que l'atteinte portée à la vie privée soit, d'une part, prévue par la loi[74], et d'autre part, proportionnée. Enfin, la CNCTR doit veiller à ce que la demande d'autorisation émane d'une autorité légalement compétente (c'est-à-dire soit un service de la communauté du renseignement, soit un service du « *second cercle* »), à ce que la procédure mise en place par le titre II soit respectée et à ce que la demande respecte les missions du service demandeur. Par conséquent, le contrôle réalisé par la CNCTR est un contrôle entier alliant à la fois un contrôle sur le fond, c'est-à-dire sur les raisons de la demande, et un contrôle de la forme.

Concernant le formalisme que doit respecter le service demandeur, il est explicité aux articles L821-1[75] à L822-4 du CSI. La demande écrite doit contenir à la fois « *la ou les techniques à mettre en œuvre* », « *le service pour lequel elle est présentée* », « *la ou les finalités poursuivies* », « *le ou les motifs des mesures* », « *la durée de validité de l'autorisation* » et enfin « *la ou les personnes, le ou les lieux ou véhicules concernés*[76] ». Cette demande doit émaner du ministre de la Défense, du ministre de l'Intérieur, du ministre de la Justice ou des ministres chargés de l'Économie,

---

[73] L'article L821-3 du CSI précise que l'avis doit être rendu par la CNCTR dans un délai compris entre 24 et 72 heures. « *La demande est communiquée au président ou, à défaut, à l'un des membres de la Commission nationale de contrôle des techniques de renseignement parmi ceux mentionnés aux 2° et 3° de l'article L. 831-1, qui rend un avis au Premier ministre dans un délai de vingt-quatre heures. Si la demande est examinée par la formation restreinte ou par la formation plénière de la commission, le Premier ministre en est informé sans délai et l'avis est rendu dans un délai de soixante-douze heures* ».

[74] Autrement dit, la demande doit porter sur l'une des techniques prévues par le Livre VIII (principe de prévisibilité).

[75] L'article L821-1 est la base légale du contrôle a priori de la CNCTR.

[76] « *Pour l'application du 6°, les personnes dont l'identité n'est pas connue peuvent être désignées par leurs identifiants ou leur qualité et les lieux ou véhicules peuvent être désignés par référence aux personnes faisant l'objet de la demande* ».

du Budget et des Douanes[77]. L'autorisation est donnée, après avis de la CNCTR, par le Premier ministre[78] pour une durée maximale de quatre mois (renouvelable). L'autorisation doit reprendre le formalisme prévu pour la demande.

En plus du contrôle de proportionnalité que doit réaliser la CNCTR, cette dernière doit veiller au respect du principe de subsidiarité lorsqu'elle rend son avis préalable. En effet, ce principe vaut pour les techniques jugées les plus intrusives, elle doit veiller à ce que le résultat recherché par le service ne puisse pas être atteint par une technique de renseignement jugée moins intrusive.

60. ***Ce que le contrôle a priori de la CNCTR ne doit pas être***. Le contrôle du respect des principes de proportionnalité et de subsidiarité ne doit pas mener à un contrôle de l'opportunité de la mesure selon la Délégation parlementaire du renseignement (DPR). Dans son rapport d'activité de 2017[79], la DPR se questionnait sur, selon elle, « *le nombre conséquent d'avis défavorables formulés par la CNCTR* » lorsque la demande concernait la défense et la promotion des « *intérêts économiques, industriels et scientifiques majeurs de la France* » (item 3 de l'article L811-3). Interrogé, le Président de la CNCTR s'était défendu en expliquant que la Commission exerçait un contrôle pragmatique, en se fondant, « *non pas sur ce que l'État aurait défini comme présentant un intérêt majeur, mais sur une appréciation « propre » de ce qu'elle estime comme tel* ». Cette approche avait étonné (en mal) la DPR, pourtant, elle est le signe plutôt sain que la Commission exerce son contrôle indépendamment de ce que les pouvoirs publics peuvent dire.

61. ***Le contrôle a priori en quelques chiffres***. En 2021, la CNCTR a rendu 398 avis défavorables[80], et ce hors demande d'accès aux données de connexion en temps différé. Ce chiffre représente 1,1 % des avis rendus par la CNCTR, ce dernier étant en hausse de 0,2 point par rapport à 2020. Cette légère hausse serait liée à la reprise de l'activité des services de renseignements alors gelée durant la crise sanitaire. En effet, de façon générale, le taux d'avis défavorables est en baisse

---

[77] «*Chaque ministre ne peut déléguer cette attribution individuellement qu'à des collaborateurs directs habilités au secret de la défense nationale*».
[78] « *Le Premier ministre ne peut déléguer cette attribution individuellement qu'à des collaborateurs directs habilités au secret de la défense nationale* ».
[79] V. p. 54 rapport DPR pour l'année 2017.
[80] V. rapport d'activité de la CNCTR pour l'année 2021, p. 67.

depuis 2015. Concernant les demandes d'accès aux données de connexion en temps différé (ce qui représente la technique la plus utilisée), la CNCTR a rendu 237 avis défavorables, soit 0,45 % des avis rendus sur cette technique. Ce chiffre est en hausse de 0,3 point par rapport à celui constaté en 2020. Ce nombre d'avis défavorables montre que la CNCTR réalise un contrôle bien réel. Enfin, comme pour les années précédentes, le Premier ministre n'a outrepassé aucun avis défavorable. Cela démontre un respect par les pouvoirs publics des préconisations rendues par la Commission, et donc d'un régime de contrôle sain.

62. ***La loi du 30 juillet 2021 : un avis rendu a priori quasiment obligatoire***. La loi du 30 juillet 2021 est venue modifier l'article L821-1 du CSI. Désormais, ce dernier prévoit que lorsque la CNCTR délivre un avis défavorable et que le Premier ministre décide de passer outre, le Conseil d'État est « *immédiatement saisi par le président de la commission*[81] ». La formation spécialisée devra alors se prononcer dans un délai de vingt-quatre heures. L'élément capital est que durant la période pendant laquelle le Conseil d'État se prononce, la décision d'autorisation, dans le cas où le Premier ministre décide de ne pas suivre l'avis de la commission, ne peut pas être exécutée (le contraire aurait été compliqué à justifier…)[82].

Cependant, la loi préserve une exception : la décision d'autorisation peut être exécutée avant le prononcé de la décision du juge administratif lorsqu'un « *cas d'urgence dûment justifiée* » se présente[83]. Cette possibilité d'outrepasser l'avis de la Commission en cas d'urgence a été interdite pour la technique des algorithmes de surveillance (article L851-3 du CSI). Cette exception d'urgence a aussi été restreinte à la défense et promotion de l'indépendance nationale, de l'intégré du territoire et de la défense nationale, à la prévention du terrorisme et à la prévention des atteintes à la forme républicaine des institutions pour les techniques prévues aux articles L853-1 (captation de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé), L853-2 (le recueil et la captation de données informatiques par des dispositifs techniques) et L853-3 (introduction dans un lieu privé afin d'y mettre en place un dispositif de captation) du CSI.

---

[81] « *ou, à défaut, par l'un des membres de la commission parmi ceux mentionnés aux 2° et 3° de l'article L831-1 du présent code* ».

[82] Cette procédure était déjà prévue dans l'hypothèse où une demande d'autorisation d'introduction dans un lieu privé à usage d'habitation faisait l'objet d'un avis défavorable (v. article L853-3 CSI). Cette procédure a donc été généralisée à l'ensemble des techniques de renseignement.

[83] Cette procédure d'urgence n'est pas applicable lorsque la demande d'autorisation concerne un parlementaire, un magistrat, un avocat ou un journaliste (v. article L821-7 CSI).

En parallèle de l'introduction de l'exception d' « *urgence dûment justifiée* », la loi du 30 juillet 2021 vient supprimer l'article L821-5 du CSI. Ce dernier prévoyait une procédure d' « *urgence absolue* »[84] qui permettait au Premier ministre de délivrer, de manière exceptionnelle, l'autorisation de recourir à une technique de renseignement avant que la CNCTR rende son avis. Cette suppression paraît logique à deux égards. D'une part, cette procédure n'avait été utilisée qu'une seule fois par le Premier ministre. Et d'autre part, l'idée est reprise au sein de l'article L821-1 du CSI, ce qui laisse à penser qu'elle a juste été introduite dans un autre article.

63. ***Remarques sur les nouveautés apportées dans le cadre du contrôle a priori***. La loi du 30 juillet 2021 met en place, d'une certaine manière, un double contrôle a priori. En effet, en cas d'avis défavorable de la CNCTR, la formation spécialisée du Conseil d'État est saisie pour faire un deuxième contrôle (si le Premier ministre décide d'outrepasser cet avis). Dans l'avis du Conseil d'État concernant le projet de loi de la loi du 30 juillet 2021[85], ce dernier explique que le contrôle instauré « *combine un mécanisme d'avis conforme d'une autorité administrative indépendante avec celui d'un contrôle préalable et effectif d'une juridiction lorsque le Premier ministre passe outre l'avis défavorable de la CNCTR*». Plusieurs constats peuvent être faits.

Le premier vise à comprendre pourquoi le législateur n'a pas souhaité rendre obligatoires les avis de la CNCTR. Même si le Premier ministre ne peut plus passer outre (sauf exception), il n'en demeure pas moins que le Conseil d'État a finalement le dernier mot, et peut décider de ne pas suivre l'avis défavorable rendu par la CNCTR. Plusieurs raisons peuvent venir à l'esprit, la première concerne la volonté pour le législateur de mettre en place une sorte de double contrôle afin de renforcer la légitimité d'un refus par la CNCTR, qui ferait peu le poids face au Premier ministre. Or, la CNCTR est composée en partie de parlementaires, ce qui lui confère une légitimité démocratique. De plus, elle est aussi composée de conseillers d'État, ce qui lui confère une légitimité technocratique, ces constats peuvent d'une certaine manière rendre absurde la saisine du Conseil d'État, s'apparentant ici à une perte de temps. Une seconde possibilité serait de donner du

[84] Cette procédure était uniquement possible que pour trois finalités : l'indépendance nationale, l'intégrité du territoire et la défense nationale ; la prévention du terrorisme ainsi que la prévention des atteintes a la forme républicaine des institutions.
[85] Avis du 12 mai 2021 sur une lettre rectificative au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

« *grain à moudre* » à la formation spécialisée du Conseil d'État, qui il est vrai n'est pas d'une grande activité jusqu'ici. Or, au vu des rares cas où le Premier ministre décide d'outrepasser l'avis de la CNCTR, cette hypothèse ne tient pas. L'hypothèse la plus logique serait d'ordre contentieuse, en effet, le juge administratif peut donner des injonctions à l'administration (articles L911-1 et s. du CJA), ce qui lui permet d'obliger le service concerné à ne pas mettre en place la mesure ou à l'arrêté d'office (si recours à la procédure d'urgence). Cela étant dit, il aurait été tout à fait plausible que le législateur confère à la CNCTR la possibilité de rendre des avis obligatoires (et un pouvoir d'injonction) car la Cour de justice n'exige aucunement la présence d'un double contrôle (contrôle juridictionnel ou d'une AAI dotée d'un pouvoir contraignant).

Le second porte sur le type de contrôle que le Conseil d'État est susceptible d'exercer sur la décision d'autorisation. Ce contrôle est-il comparable à celui fait par la CNCTR ? Voire, est-ce que le Conseil d'État contrôle aussi les motifs amenant l'avis défavorable rendu par la CNCTR ? Ni l'avis du Conseil d'État relatif au projet de loi ni les débats parlementaires ne permettent de préciser la nature du contrôle exercé par la formation spécialisée… Il paraît logique que ce dernier contrôle, à la lumière de la CNCTR, la demande d'autorisation, ce qui amène à se poser la question de l'opportunité réelle de ce double contrôle (si c'est pour réaliser un contrôle similaire à celui de la CNCTR). Il faudra donc attendre les futurs retours pour se forger une véritable idée de l'opportunité et de l'efficacité de ce double contrôle, et donc de savoir s'il n'aurait pas été plus préférable de « *simplement* » donner un pouvoir contraignant (couplé à un pouvoir d'injonction) à la CNCTR. Quoiqu'il en soit, la CNCTR est devenue avec cette loi un véritable garde-fou, en veillant à la légalité et à la proportionnalité des mesures souhaitées, ce qui est une réelle avancée pour le contrôle des activités de renseignement, et d'une manière plus générale pour l'État de droit.

Paragraphe 2 : La CNCTR par rapport à ses homologues européennes

64. ***Rappels***. Comme vu précédemment, la CNCTR est l'organe de contrôle mis en place en 2015 pour contrôler a priori et a posteriori le recours aux techniques de renseignement prévues au livre VIII du CSI. Elle n'est pas dotée d'un pouvoir contraignant, même si en cas d'avis défavorables non respectés par le Premier ministre, le Conseil d'État est obligatoirement saisi (double contrôle).

65. ***Le contrôle a priori des activités de renseignement en Belgique.*** Le droit belge s'est penché plus tôt sur l'encadrement juridique à donner aux activités de renseignement. Un contrôle a été mis en place dès 1991 avec la création du Comité permanent de contrôle des services de renseignement et de sécurité (appelé Comité permanent R). Cet organe, composé de membres nommés par les parlementaires, opère un double contrôle : « *sur la légitimité (le contrôle du respect des lois qui réglementent la matière)* » et « *sur l'efficacité et la coordination des services de renseignement* »[86]. Mais l'organe se rapprochant le plus de la CNCTR n'est pas ce Comité permanent R, mais la commission[87]. Cette dernière a été créée par la loi du 4 février 2010[88] pour venir encadrer et permettre l'usage de techniques intrusives[89] aux services de renseignement belges. Le recours à ces techniques intrusives exceptionnelles fait l'objet d'un contrôle en deux temps. Tout d'abord, la commission réalise un contrôle a priori, puis le Comité permanent R veille au respect du droit dans l'application de la mesure. Cette commission est composée de trois magistrats nommés par le Roi sur proposition du ministre de la Justice et du ministre de la Défense[90]. Cette commission « *effectue sa tâche de contrôle en toute indépendance* »[91]. La commission rend des avis conformes, c'est-à-dire obligatoires. En effet, l'article 18/10 de la loi précitée dispose que « *si la commission rend un avis négatif, la méthode exceptionnelle (…) ne peut pas être mise en œuvre par le service concerné* ». La commission réalise un contrôle entier visant à notamment vérifier le respect des principes de proportionnalité et de subsidiarité (vérifier si une méthode classique ne permet pas d'obtenir le résultat escompté)[92].

66. ***Le contrôle a priori des activités de renseignement en Belgique : remarques.*** La commission et la CNCTR jouent un rôle relativement similaire dans le cadre du contrôle a priori. Elles rendent toutes les deux un avis préalable avant la décision d'autorisation d'une technique de renseignement par le pouvoir exécutif. Cependant, deux principaux points de différences sont à

---

[86] V. site internet du Comité permanent de contrôle des services de renseignement et de sécurité (https://www.comiteri.be/index.php/fr/comite-permanent-r).
[87] Est appelée comme cela par le droit belge.
[88] Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité.
[89] Ces techniques sont celles relatives à la conservation et à l'accès aux données conservées. L'article 1 ladite loi les qualifie de « *méthode spécifique ou exceptionnelle* ».
[90] V. article 43/1 de la loi du 4 février 2010.
[91] V. article 43/1 de la loi du 4 février 2010.
[92] V. article 18/10 de la loi du 4 février 2010.

relever. Le premier est que la commission donne un avis que sur les « *méthodes exceptionnelles* », c'est-à-dire celles s'affairant à la conservation des données, or la CNCTR donne des avis sur un panel de techniques plus large (allant de l'accès aux données jusqu'à la possibilité de poser un dispositif d'écoute). Le second, le plus important, est que la commission, contrairement à la CNCTR, donne un avis conforme (elle n'a pas le besoin d'une quelconque « *validation* » par une juridiction belge). Dès lors, l'hypothèse explicitée dans le paragraphe précédent (selon laquelle le législateur aurait pu conférer un pouvoir contraignant à la CNCTR) prend tout son sens, car nos voisins belges l'ont fait. La commission belge est dotée d'un pouvoir contraignant alors qu'elle jouit d'une légitimité démocratique beaucoup moins importante que son homologue français (composée que de magistrats et non de parlementaires).

67. ***Le contrôle a priori des activités de renseignement aux Pays-Bas (P-B)***. À la lumière de ce qui est fait chez leurs voisins belges, les Néerlandais ont deux organes de contrôle issus de deux lois successives. La CTIVD[93] est une commission créée dès 2002 divisée en deux départements : contrôle et plainte. Elle est chargée de rendre des rapports classifiés à une commission parlementaire. Pour donner suite à l'instauration de nouvelles techniques liées à la surveillance de masse par le législateur néerlandais (2017), le contrôle a été renforcé par la création d'un nouvel organe : la TIB. Ce dernier, comme la CNCTR, rend un avis préalable avant l'autorisation donnée par le pouvoir exécutif de recourir à une « *méthode spéciale* ». Mais encore une fois, à la différence de la CNCTR, cet organe de contrôle jouit d'un pouvoir contraignant. Il est important de noter que le projet de loi relatif à la loi de 2017 avait fait l'objet d'un référendum. Ce dernier avait été rejeté par les Néerlandais, notamment en raison des risques de surveillance de masse. Cependant, la loi a tout de même été adoptée, mais ce refus populaire a entraîné un renforcement des prérogatives pour les organes de contrôles[94]. Là encore, les mêmes constats peuvent être présentés que pour le cas belge.

68. ***Le contrôle a priori des activités de renseignement dans d'autres États***. Au Royaume-Uni (R-U), *The Office for Communications Data Authorisations*[95] *(OCDA)* prend des décisions

[93] *Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten* (néerlandais).
[94] V. *Approche comparée des droits du renseignement*, Guy Rapaille dans *le droit du renseignement*, actes du colloque, académie du renseignement, 2019.
[95] Fait partie de *The Investigatory Powers Commissioner's.*

indépendantes sur l'opportunité d'accorder ou de refuser des demandes relatives aux données de communication, en veillant à ce que toutes les demandes soient légales, nécessaires et proportionnées. Autrement dit, ce bureau autorise le recours par les services de renseignement à des techniques utilisant les données[96]. Le fonctionnement britannique est très intéressant, car il est basé sur un système juridique complètement différent du nôtre et que les moyens du R-U sont comparables à ceux de la France. Le rapport annuel rendu par *The Investigatory Powers Commissioner's* pour l'année 2021 précise le nombre de demandes ainsi que les raisons, le cas échéant, de refus (ou de renvoi au demandeur) de la mesure. Entre 2020 et 2021, le OCDA a statué sur 245 272 demandes, sur ces dernières 20 244 ont été renvoyées au demandeur (afin que le service la modifie) et 282 ont été rejetées[97]. Sur les 20 244 renvois, 7 377 l'étaient en raison de manquement aux obligations de nécessité et de proportionnalité. Là encore, le OCDA est doté de pouvoir important, car elle peut s'opposer, sans nécessiter de recourir à un second contrôle, à une demande de mise en place d'un service de renseignement.

Le cas suédois est aussi fort intéressant même s'il diffère fortement du cas français. En effet, dès 2009, il a été mis en place, pour les techniques de renseignement électromagnétique[98] utilisées dans le cadre des activités de renseignement de défense, une juridiction spécialisée : la Cour de renseignement de la défense[99]. Cette dernière rend des décisions protégées par le « *secret absolu* ». Ce tribunal autorise le recours à toutes les techniques de renseignement électromagnétique. Là encore, le cas suédois aurait pu inspirer le législateur français. En effet, il aurait pu créer une juridiction administrative spécialisée (car donner l'ensemble du contentieux relatif aux demandes d'autorisation à la formation spécialisée du Conseil d'État aurait été impossible).

Dans d'autres États, le contrôle des activités de renseignement pourrait être qualifié de faible. C'est le cas de l'Italie par exemple. En effet, en 2007[100], sous l'impulsion du gouvernement

---

[96] L'*Investigatory Powers Act 2016* précise les techniques concernées. Y figurent notamment l'interception des communications ainsi que l'acquisition ou la conservation de données de communication.
[97] V. *Investigatory Powers Commissioner's Annual Report 2021*, p. 38,
[98] Les techniques relatives aux données en font partie.
[99] *FÖRSVARSUNDERRÄTTELSEDOMSTOLEN* en suédois. La Cour EDH traduit ce terme par « *tribunal pour le renseignement extérieur* » dans l'arrêt *Centrum för rättvisa c. Suède* (Cour EDH, 2021).
[100] *Legge n. 124 del 3 agosto 2007*.

de centre gauche dirigé par Romano Prodi[101], l'organisation de renseignement italien a été bouleversée. Le législateur en a profité pour améliorer les prérogatives de la commission parlementaire chargée de contrôler les services de renseignement : *la Comitato parlamentare per la sicurezza della Repubblica* (COPASIR). Cependant, malgré ce renforcement, le contrôle reste faible. Au-delà d'un pouvoir d'interroger les acteurs du renseignement, elle peut uniquement, lorsqu'elle constate une violation du droit par les services de renseignement, demander au Président du Conseil des ministres d'ordonner des enquêtes internes. Forcé de le reconnaître que l'Italie a encore des progrès à faire pour avoir un contrôle digne d'une démocratie.

69. ***Remarques générales***. Lorsque les États européens se sont dotés d'organe similaire à la CNCTR (autorité indépendante), comme c'est le cas pour la Belgique ou les Pays-Bas, ces organes jouissent d'un pouvoir contraignant. Autrement dit, ils peuvent s'opposer à la mise en place d'une technique de renseignement par leur seule volonté. Ces organes sont donc dotés d'un plus grand pouvoir que la CNCTR, car elles n'ont pas besoin d'un second contrôle. Ici, le cas français pourrait donc être qualifié de sui generis, de sorte qu'il est le seul en Europe à rendre obligatoire un double contrôle de la demande d'autorisation d'une technique de renseignement lorsque l'organe chargé du contrôle a priori a rendu un avis négatif non respecté. Ce double contrôle ne paraît pas trouver une réelle justification comme expliqué précédemment. D'autres États européens ont fait le choix d'un contrôle parlementaire fort, avec parfois la mise en place d'une autorisation directe de la technique par la commission de contrôle parlementaire (v. R-U). D'autres choisissent de faire un contrôle juridictionnel sur toutes les demandes, c'est le cas de la Suède. Enfin, certains États, comme l'Italie, se démarquent par leur retard par rapport à leur pair sur le contrôle des activités de renseignement.

Concernant la composition des organes de contrôle, il est possible de distinguer deux types de membres : les techniciens et les élus (ou politiques). Les premiers sont souvent des magistrats ou des experts du monde du renseignement (légitimité technocratique). Les seconds sont soit des parlementaires, soit des personnes nommées par le pouvoir exécutif ou le pouvoir législatif (légitimité démocratique). En ce qui concerne la CNCTR, sa composition paraît réfléchie et

[101] Homme d'État italien du parti démocrate italien ayant été Premier ministre de 2006 à 2008 ainsi que président de la Commission européenne.

optimale. En effet, elle est, à la fois, composée de magistrats des deux ordres de juridiction (notamment judiciaire), ce qui permet une atténuation des critiques concernant la volonté de certains visant à placer les activités de renseignement sous le contrôle du juge judiciaire (et non du juge administratif), et, à la fois, de parlementaires. La CNCTR est donc dotée d'une légitimité démocratique et technocratique[102], ce qui rend ce double contrôle complexe à justifier.

Après avoir vu, d'une part, que le législateur a renforcé l'impact du contrôle a priori réalisé par la CNCTR et, d'autre part, comparé cette dernière à ce qui se fait dans les autres démocraties européennes, il est important de démontrer l'impact des autres contrôles.

Section 2 : Le rôle non négligeable des autres organes de contrôle.

70. ***Annonce***. Même si la part significative du contrôle a priori, concernant l'usage des techniques de renseignement prévues au livre VIII du CSI, est réalisée par la CNCTR, d'autres organes contrôlent les activités de renseignement. Ce contrôle peut être à la fois direct comme indirect. L'un des contrôles souvent oublié, mais d'une grande importance, est le contrôle hiérarchique (***paragraphe 1***). À ce dernier s'ajoute le contrôle d'autres organes, juridictionnels ou administratifs, dont leur office principal ne concerne pas les activités de renseignement, mais qui en raison de leur finalité se mêlent à ces dernières (***paragraphe 2***).

Paragraphe 1 : L'accroissement du contrôle hiérarchique grâce à l'action du législateur

71. ***Rappel***. Avant la loi du 24 juillet 2015, le contrôle hiérarchique était le seul contrôle à être exercé sur les services de renseignement, à l'exception des techniques concernant l'interception des communications émises par voie électronique[103]. Il s'agit donc du contrôle le plus ancien (avec le contrôle médiatique). Nonobstant cette antériorité, ce contrôle a été impacté (de manière positive) par la loi du 24 juillet 2015. Il s'est vu optimisé, plus ou moins indirectement, par l'encadrement des activités de renseignement opéré par ladite loi. Pour reprendre les mots du préfet Renaud Vedel, après avoir rappelé que cet encadrement augmentait la légitimité de l'action des

[102] De plus un spécialiste des télécommunications aident les membres à comprendre les enjeux techniques.
[103] Qui faisait l'objet d'un contrôle administratif indépendant par la CNCIS (v. introduction point 13).

services, ce dernier argue que, bien que ce contrôle soit peu visible de l'extérieur, « *il est extrêmement fort et prégnant* »[104]. Le contrôle hiérarchique intervient tant avant la mise en place de l'autorisation de recourir à une technique de renseignement (a priori donc) que dans l'exécution de cette dernière (a posteriori donc).

72. Les modifications apportées au contrôle hiérarchique. Les modifications apportées sont multiples, elles permettent de mettre en place un réel contrôle, qui s'ajoute donc aux contrôles administratif et juridictionnel créés par le législateur. Malgré, l'opacité de fonctionnement de ces services pour des raisons que chacun peut comprendre, la loi et la doctrine (voire la presse) permettent d'avoir une vue d'ensemble sur la manière dont les services de renseignement fonctionnent.

73. ***La conjugaison entre responsabilité administrative et responsabilité politique : l'axe central de la modification du contrôle hiérarchique.*** Depuis 2015, la responsabilité de l'ensemble du service, c'est-à-dire de l'agent demandeur au directeur du service auquel l'agent appartient, ainsi que la responsabilité politique du ministre auquel se rattache le service et du Premier ministre sont engagées lorsqu'une autorisation est donnée. La loi permet donc un partage de la responsabilité entre responsabilité administrative des services demandeurs et responsabilité politique du Premier ministre et du ministre auquel se rattache le service demandeur. Cette conjugaison des responsabilités est illustrée par le formalisme de l'acte d'autorisation. En effet, ce dernier comprend trois signatures : celle du chef de service demandeur (par exemple le directeur général de la DGSI), celle du ministre de rattachement (le ministre de l'Intérieur dans notre exemple) et enfin celle du Premier ministre.

Cette conjugaison de la responsabilité politique et administrative décharge en partie les services de renseignement et légitime leur action. Désormais, chaque technique de renseignement est autorisée par le Premier ministre (pour celle comprise dans le livre VIII du moins), ce qui confère à l'action des services une légitimité plus importante qu'auparavant. De plus, par l'engagement de la responsabilité politique du Premier ministre et du ministre visé, ces derniers veillent de plus près au respect des principes de nécessité et de proportionnalité auxquels doit

[104] *Les contrôles internes*, par Renaud Vedel, *Le droit du renseignement*, 2019.

répondre le recours aux techniques de renseignement. L'engagement de la responsabilité politique dans le cadre des activités de renseignement constitue aussi le terreau d'une potentielle évolution du contrôle parlementaire (v. infra).

En pratique, avant même d'arriver au ministre de rattachement, l'agent souhaitant recourir à une technique de renseignement doit convaincre ses pairs de l'opportunité, de la nécessité et de la proportionnalité de sa demande. Autrement dit, l'agent demandeur doit convaincre l'ensemble de sa hiérarchie, c'est-à-dire du chef de groupe (ou unité) au directeur du service. Dès cette étape, qui est le premier contrôle réalisé du point de vue chronologique, les demandes dont la motivation est manifestement non fondée sont écartées. Face aux flux importants de demandes posées par les agents[105], les services de renseignement, du moins en ce qui concerne les plus importants, ont mis en place des cellules de conformité spécialisées dont la mission est de contrôler la conformité et possiblement réviser les demandes faites par les agents. Ces cellules, par leur rôle de filtrage des demandes, rendent plus efficient le contrôle hiérarchique, et ce pour plusieurs raisons. D'une part, elles permettent de spécialiser des agents dans le traitement des demandes d'autorisation de techniques de renseignements[106]. D'autre part, elles échangent directement avec l'agent à l'origine de la demande (ce qui n'est pas toujours le cas lorsque ces cellules n'existent pas). Ce dernier point permet notamment aux agents qui réalisent ce premier contrôle de comprendre directement pour quelles raisons l'agent souhaite mettre en place cette technique de renseignement.

74. ***Le corollaire de cette double responsabilité : la centralisation***. L'introduction de cette double responsabilité est à l'origine de la nécessité de centraliser l'ensemble des demandes. Chaque demande, peu importe où l'agent à l'origine de cette demande se trouve, doit passer par le pouvoir central, à savoir le gouvernement. La mise en place d'une procédure très formalisée par la loi du 24 juillet 2015 permet de faire transiter l'ensemble des demandes par un même cheminement. Avant de conférer son autorisation, autrement dit d'engager sa responsabilité, le Premier ministre (son cabinet en réalité) prend connaissance du dossier entourant cette demande. Cette centralisation

---

[105] Pour rappel, en 2021, 87 588 techniques de renseignement avaient été autorisées par le Premier ministre. V. Rapport d'activité de la CNCTR, p. 62.

[106] Renaud Vedel explique que les agents qui composent ces cellules présentent « *des complémentarités pluridisciplinaires, opérationnelles et juridiques* » et disposent « *d'une connaissance assez précise de la doctrine de la commission* ». V. *Les contrôles internes*, par Renaud Vedel, dans *Le droit du renseignement*, 2019, p. 152.

a été grandement facilitée par le GIC[107] qui a mis en place une procédure dématérialisée pour répondre aux exigences légales, ainsi qu'à l'exigence de célérité à laquelle doivent répondre les services de renseignement. Cette centralisation, en plus de faciliter le contrôle hiérarchique, permet au gouvernement d'avoir une vue d'ensemble sur les finalités poursuivies par la mise en place des techniques de renseignement demandées. Cela permet aussi au gouvernement de plus facilement orienter les services de renseignement, car pour rappel, les services de renseignement sont orientés par le gouvernement, et ce pour deux raisons. La première est qualifiable de démocratique, en effet, les services de renseignement doivent répondre aux besoins du peuple français et donc sont soumis à ses représentants démocratiquement élus. La seconde, plus terre-à-terre, renvoie aux moyens limités avec lesquels les services de renseignement doivent agir, ce qui nécessite une orientation sur certaines menaces, voire une hiérarchisation de ces dernières (finalement ces deux raisons ont un lien).

75. ***Création de l'inspection des services de renseignement***. Une année avant l'entrée en vigueur de la loi de 2015, un décret est venu créer l'inspection des services de renseignement[108]. Cette dernière s'ajoute aux inspections internes qui existaient déjà dans lesdits services. Elle permet d'avoir un contrôle hiérarchique interservices. Elle est placée sous l'autorité du Premier ministre, ce dernier nomme ses membres et définit ses missions. Cette inspection interservices peut contrôler, conseiller, évaluer ou encore réaliser des audits. Elle démontre encore une fois l'antériorité du contrôle hiérarchique et son importance.

76. ***Remarques générales sur le contrôle hiérarchique***. Le contrôle hiérarchique est, comme il a été vu, important. Au-delà de son rôle de filtrage, il permet de rendre conscients les agents de renseignement des prérogatives dont ils bénéficient et les limites de leur utilisation. De plus, l'efficacité de ce contrôle conditionne l'image des services de renseignement. Désormais, il est compliqué pour ces derniers de cacher un dysfonctionnement, notamment en raison du contrôle de

---

[107] Le GIC (groupement interministériel de contrôle) est un service du Premier ministre « *à compétence nationale chargé de centraliser les demandes d'autorisation pour la mise en œuvre de techniques de renseignement émises par les services. Il les présente au Premier ministre après les avoir soumises à l'avis de la Commission nationale de contrôle des techniques de renseignement, autorité indépendante chargée de vérifier que celles-ci sont employées dans le respect du cadre légal* ». v. Site internet du gouvernement : https://www.gouvernement.fr/groupement-interministeriel-de-controle-gic.

[108] Décret n° 2014-833 du 24 juillet 2014 relatif à l'inspection des services de renseignement.

la CNCTR. Le nombre d'avis défavorables (635 en 2021[109]) rendus par la CNCTR, par rapport au nombre de demandes réalisées (environ 88 000) doit donner lieu à deux remarques. D'une part, le contrôle hiérarchique peut être qualifié d'efficace, car seulement 0,72 % des demandes reçoivent un avis défavorable de la CNCTR. D'autre part, même si ce chiffre semble bas, il démontre surtout que le contrôle hiérarchique est loin d'être suffisant, ce qui permet de mettre en exergue l'importance des autres contrôles (notamment juridictionnel et administratif).

Paragraphe 2 : Les contrôles indirects d'autres organes non spécialisés dans les activités de renseignement

77. Au-delà des contrôles a priori réalisés par la CNCTR et les membres des services eux-mêmes, d'autres entités interviennent plus indirectement dans le cadre du contrôle des activités de renseignement. Avec les actions multiples du législateur depuis 2015, les organes réalisant ces contrôles plus indirects sont amenés à s'immiscer dans le contrôle réalisé par la CNCTR. Par exemple, la CNIL dispose d'un champ de compétence concernant la protection des données, ce qui la rend primordiale dans le cadre des techniques de renseignement relatives aux données. Dans ce paragraphe, seuls les contrôles estimés les plus impactant sur les activités de renseignement seront traités.

78. ***L'affirmation du rôle du juge constitutionnel dans le contrôle des lois relatives au renseignement***. Les diverses lois entrées en vigueur depuis 2015 ont permis aussi au juge constitutionnel de se saisir des activités de renseignement. L'encadrement apporté principalement par la loi du 24 juillet 2015 permet de légitimer le contrôle réalisé par le Conseil constitutionnel. En effet, jusque-là la crainte d'une immixtion dans le fonctionnement du renseignement valait également pour le juge constitutionnel, qui comme l'explique le Professeur Xavier Latour, refusait de se pencher sur le sujet[110]. De plus, avec la multiplication des lois relatives aux activités de renseignement, le juge constitutionnel a pu se prononcer sur un grand nombre d'entre elles.

[109] V. rapport d'activité de la CNCTR pour l'année 2021, p. 67.
[110] Article du Professeur Xavier Latour, *Le contrôle du Conseil constitutionnel sur le renseignement*, dans *Le droit du renseignement*, 2019.

Les décisions rendues par le Conseil constitutionnel dans le domaine du renseignement sont critiquées par les défenseurs des libertés. Ces critiques s'inscrivent dans cette tendance générale à la normalisation de l'urgence et à une sécurisation globale de la société[111]. Malgré les critiques, le Conseil constitutionnel tente de trouver un équilibre entre sécurité et libertés, même si la tendance actuelle semble pencher pour la première.

Plus précisément, le Conseil constitutionnel rattache l'action des services de renseignement à la préservation de la sécurité nationale (en rapprochant le contenu de cette notion à celui des intérêts fondamentaux de la Nation)[112]. Dans le cadre de son contrôle, il vise notamment à sanctionner l'incompétence négative du législateur. En effet, le droit du renseignement touche directement aux « *droits civiques* » et aux « *garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* »[113], et donc laisser le pouvoir réglementaire légiférer (souvent porteur d'une vision sécuritaire) dans ce domaine pourrait, au-delà de son inconstitutionnalité, s'avérer dangereux pour les prérogatives d'un Parlement déjà bien endormi[114]. Le Conseil constitutionnel a eu aussi une importance dans la délimitation entre police administrative et police judiciaire en ce qui concerne les activités de renseignement (v. introduction, point 6). De plus, dans le cadre de la décision relative à la loi du 24 juillet 2015, le Conseil constitutionnel réalise un contrôle restreint en se bornant uniquement à relever les atteintes « *manifestement disproportionnées* »[115], ce qui explique pourquoi, à l'exception de la procédure dite d'urgence opérationnelle, la quasi-totalité de la loi a été validée par le juge. Le choix de se borner à un contrôle restreint s'explique avant tout par la volonté de ne pas interférer avec l'expression de la volonté générale (ce point n'est pas seulement applicable aux activités de renseignement).

Concernant la loi du 30 juillet 2021, le Conseil ne s'est pas penché sur les dispositions relatives au renseignement, et cela est bien dommage. En effet, cette loi rend pérenne la technique dite de l'algorithme, qui renvoie directement à l'idée même d'une potentielle surveillance de masse (article L851-3 du CSI). Même si cette technique est prévue que pour la prévention du terrorisme,

---

[111] À titre d'exemple, le projet de loi relatif à l'organisation des JO 2024 prévoit le recours à un système de vidéoprotection dit intelligent (utilisant l'IA). Même si le gouvernement mentionne que la reconnaissance faciale ne sera pas utilisée, cette avancée inquiète certain défenseur des libertés.

[112] Décision n° 2015-478 QPC du 24 juillet 2015, *Association French Data Network et autres*.

[113] V. article 34 de la Constitution.

[114] Voir par exemple, point 78, décision n° 2015-713 DC.

[115] Décision n° 2015-713 DC du 23 juillet 2015 (v. par exemple point 25).

elle avait fait l'objet de doutes concernant sa proportionnalité et les dangers pour les données de chaque utilisateur dans l'avis de la CNIL[116]. Il aurait été intéressant de voir le Conseil constitutionnel se pencher dessus (il pouvait le faire, car pour rappel, il peut statuer ultra petita).

Le contrôle du Conseil constitutionnel est donc primordial (qu'il soit par voie d'exception ou a priori), il permet d'éviter l'entrée en vigueur (ou l'abrogation) de dispositifs jugés liberticides que le législateur souhaiterait mettre en place. Or, son contrôle n'est pas facile à réaliser, car il doit en permanence allier protection des libertés et préservation de la sécurité nationale. Par une censure des dispositifs législatifs, notamment liés aux moyens techniques des services de renseignement, il pourrait porter atteinte au bon fonctionnement des services de renseignement.

79. ***Le rôle important de la CNIL pour les techniques en lien avec les « données »***. Même si le rôle de la CNIL[117] est avant tout de réguler les données personnelles, notamment en veillant au respect du RGPD, elle peut jouer un rôle relativement important dans le cadre des activités de renseignement. Les techniques de renseignement utilisent de plus en plus les données pour prévenir les atteintes aux intérêts fondamentaux, ce qui amène la CNIL à venir se mêler du contrôle des activités de renseignement.

Premièrement, en vertu de l'article 8 de la loi relative à l'informatique, aux fichiers et aux libertés, la CNIL est chargée d'émettre un avis avant la création, par arrêté ministériel ou décret en Conseil d'État, d'un fichier intéressant « *la sûreté de l'État, la défense ou la sécurité publique* » ou qui a pour objet « *la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté* »[118]. Font par exemple

[116] Délibération n° 2021-040 du 8 avril 2021 portant avis sur un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement : « *La Commission considère que les modifications apportées par le projet de loi à l'article L. 851-3 du CSI ne permettent pas d'appréhender de manière claire et précise les évolutions envisagées et ainsi la manière dont cette technique de renseignement sera mise en œuvre. Elle estime indispensable que le texte soit précisé* ».

[117] La CNIL est une AAI composée de quatre parlementaires, deux membres du CESE et six représentants des hautes juridictions (deux conseillers d'État, deux magistrats de la Cour de Cassation et deux magistrats de la Cour des Comptes).

[118] V. article 31 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

partie de ces fichiers le FPR[119], le FSPRT[120] ou encore le CRISTINA[121]. Ces fichiers sont quotidiennement utilisés par les services de renseignement, car ils permettent le suivi des personnes potentiellement dangereuses pour les intérêts fondamentaux de la Nation. L'avis rendu est annexé à l'arrêté ou au décret créant le fichier. Il n'est certes pas obligatoire, mais il peut être utilisé par le requérant qui souhaiterait obtenir l'annulation du décret créant ce fichier. En effet, ces décrets ou arrêtés sont susceptibles de recours pour excès de pouvoir devant le Conseil d'État[122].

De plus, toujours en vertu de l'article 8 de ladite loi, la CNIL est consultée dès qu'un projet de loi ou de décret souhaite légiférer dans le domaine de « *la protection des données à caractère personnel ou au traitement de telles données* ». Dans ce cadre, elle dispose d'un pouvoir de proposition. Par exemple, lors de son avis du 8 avril 2021 relatif à la loi sur la prévention d'actes de terrorisme et au renseignement, la CNIL avait encouragé le gouvernement à apporter des précisions. Même si ces avis ne sont pas obligatoires, ils peuvent être utilisés par le Conseil constitutionnel pour justifier une censure de la loi et touchent, en cas d'avis défavorable, à la légitimité de la législation.

Enfin, en vertu de l'article 118 de ladite loi, la CNIL est compétente pour recevoir « *les demandes tendant à l'exercice du droit d'accès, de rectification et d'effacement* » des fichiers intéressant la sûreté de l'État. Le cas échéant, un membre de la CNIL procède aux vérifications nécessaires, et peut soit autoriser l'accès aux données, soit refuser cet accès. Dans ce second cas le demandeur peut réaliser un recours devant la formation spécialisée du Conseil d'État (v. infra).

80. ***La Commission du secret de la Défense nationale***. Cette autorité administrative indépendante[123], dont la finalité est de rendre plus transparente l'opposition du secret de la défense nationale, intervient notamment dans le cadre d'une procédure juridictionnelle. Elle rend un avis

[119] Fichier des personnes recherchées.
[120] Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste.
[121] Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux.
[122] Lorsqu'en vertu de l'article en vertu de l'article 31 de la loi du 6 janvier 1978, le gouvernement refuse par décret de publier le décret créant le fichier, le requérant peut attaquer le décret refusant la publication. V. par exemple : Conseil d'État*, 16 avril 2010,* n° 320196 concernant le fichier CRISTINA.
[123] Créée en 1998, elle est composée d'un conseiller d'État, d'un magistrat de la Cour de cassation, d'un magistrat de la Cour des comptes, d'un député et d'un sénateur

sur les demandes de déclassification d'information lorsque cette dernière est demandée par une juridiction[124]. Son rôle ne concerne donc pas la formation spécialisée du Conseil d'État, car, pour rappel, ses membres sont tous habilités. En revanche, elle joue un rôle clé dans le cadre pénal lorsque, pour les besoins de son enquête, un juge d'instruction a besoin qu'une information soit déclassifiée. C'est donc lorsqu'une infraction en lien avec les activités de renseignement aura été commise que cette autorité administrative indépendante pourra jouer un rôle important. Lorsque cette infraction est relevée par la CNCTR, concomitamment après avoir saisi le procureur de la République « *dans le respect du secret de la défense nationale* », elle doit d'office transmettre les éléments classifiés à la connaissance de la CSDN pour qu'elle émette son avis (et que le procureur en prenne éventuellement connaissance)[125]. À titre d'exemple, la CSDN a permis à l'enquête relative aux écoutes de l'Élysée de se terminer, ce qui a donné lieu à un procès en 2005 (alors que les écoutes s'étaient déroulées entre 1983 et 1986)[126].

81. ***Conclusion chapitre***. Le renforcement opéré par le législateur concernant l'organe principal de contrôle qu'est la CNCTR vient mettre en conformité le droit national par rapport aux exigences posées par le droit européen. L'instauration d'un double contrôle (lorsque le Premier ministre passe outre un avis défavorable de la CNCTR) fait du cas français une particularité par rapport à ses pairs européens. Au-delà de ce renforcement amené par le législateur, d'autres contrôles s'exercent plus ou moins directement sur les activités de renseignement. Ces derniers existaient déjà avant 2015, mais l'action du législateur a modifié leur contenu. L'importance de ces contrôles n'est pas à négliger, notamment en ce qui concerne le contrôle hiérarchique. L'encadrement juridique du renseignement mise en place dès 2015 a amené la CNCTR à collaborer avec d'autres organes. Le Professeur Bertrand Warusfel avait notamment encouragé une

[124] Cet avis est rendu au gouvernement, qui choisit discrétionnairement de déclassifier ou non l'information grevée.

[125] Article L861-3 CSI : « *Lorsque la commission estime que l'illégalité constatée est susceptible de constituer une infraction, elle saisit le procureur de la République dans le respect du secret de la défense nationale et transmet l'ensemble des éléments portés à sa connaissance à la Commission du secret de la défense nationale afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République* ».

[126] V. notamment, Le Monde, *Les principaux condamnés au procès des écoutes de l'Élysée se pourvoient en cassation*, 27 mars 2007.

articulation entre le contrôle des techniques de renseignement et les régulateurs spécialisés, notamment la CNIL[127].

82. ***Conclusion titre.*** Depuis l'entrée en vigueur de la loi de 2015, le contrôle des activités de renseignement a connu de nombreuses évolutions. Il s'est étoffé. Cette évolution est la conséquence directe des exigences européennes, constamment rehaussées afin de suivre l'évolution des techniques de renseignement. Cependant, le régime de contrôle instauré est encore perfectible. Les pistes d'évolutions vont être traitées dans un second titre.

[127] Professeur Bertrand Warusfel, *Quelques réformes pour le droit du renseignement*, 2020 (Colloque de l'AFDSD).

<u>TITRE II :</u> UN CONTRÔLE DES ACTIVITÉS DE RENSEIGNEMENT ENCORE PERFECTIBLE

83. ***Annonce***. Malgré un renforcement du contrôle des activités de renseignement réalisé par le législateur français sous l'impulsion du droit européen, ce contrôle reste encore perfectible. Plusieurs évolutions concernant l'ensemble des contrôles déjà existants sont à souhaiter afin d'éviter un détournement des techniques de renseignement de leur but initial, c'est-à-dire garantir les intérêts fondamentaux de la Nation. La première repose sur la nécessité de durcir, ou du moins favoriser, le contrôle a posteriori (***chapitre 1***). La seconde repose sur la nécessité et l'importance primordiale d'avoir un contrôle parlementaire digne et fort, ce qui n'est pas encore le cas malheureusement (***chapitre 2***).

CHAPITRE 1 : UN DURCISSEMENT NÉCESSAIRE ET SOUHAITABLE DU CONTRÔLE A POSTERIORI

84. ***Annonce***. Le contrôle a posteriori est d'une importance capitale dans le contrôle des activités de renseignement. Il permet de s'assurer qu'une fois l'autorisation donnée par le Premier ministre, l'exécution de la technique de renseignement ne porte pas de manière illégale atteinte aux droits et libertés des administrés. Ce contrôle est principalement réalisé par deux organes : la CNCTR et la formation spécialisée du Conseil d'État. Dans le cadre du contrôle a posteriori réalisé par la formation spécialisée, il est aisé de constater un problème majeur concernant la procédure actuelle et le respect du contradictoire (***section 1***). De plus, concernant les prérogatives de la CNCTR dans le cadre du contrôle a posteriori, il est souhaitable que ces prérogatives soient accrues, notamment face à l'augmentation des moyens techniques dont jouissent les services de renseignement (***section 2***).

Section 1 : Les problèmes de la procédure mise en place devant la formation spécialisée du Conseil d'État

85. ***Annonce***. La procédure mise place par la loi du 24 juillet 2015 plonge le requérant dans une situation obscure (***paragraphe 1***). Il sera intéressant d'expliquer quelles solutions le législateur pourrait mettre en place pour améliorer cette situation déséquilibrée (***paragraphe 2***).

Paragraphe 1 : Une procédure obscure pour le requérant

86. ***Saisine de la formation spécialisée a posteriori***. À l'origine, la loi du 24 juillet 2015 cantonnait la formation spécialisée du Conseil d'État à un contrôle a posteriori. Certes, la loi du 30 juillet 2021 lui confère un rôle dans le cadre du contrôle a priori, mais le cœur de son rôle reste cantonné au contrôle a posteriori. Les missions de cette formation spécialisée sont fixées aux articles L841-1 et L841-2 du CSI.

Premièrement, elle est compétente pour connaître des requêtes relatives aux techniques de renseignement. Elle peut dans ce cadre être saisie par tout administré « *souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard* »[128]. L'introduction de cette requête doit se faire obligatoirement après la saisine de la CNCTR (comparable à un recours administratif préalable obligatoire), qui va déjà réaliser un contrôle. Elle peut aussi être saisie par le président de la CNCTR (ou trois de ses membres) lorsque le Premier ministre refuse de donner des suites (ou donne des suites estimées insuffisantes) aux recommandations et aux avis rendus par la CNCTR[129]. Là encore, le but de cette disposition est clair, elle permet indirectement de rendre les recommandations et avis de la CNCTR obligatoire par l'intermédiaire du pouvoir d'injonction du juge administratif (si ce dernier suit les conclusions rendues par la CNCTR). La formation spécialisée du Conseil d'État peut aussi être saisie à titre préjudiciel par une autre juridiction administrative ou une juridiction judiciaire « *lorsque la*

[128] Article L841-1 du CSI.
[129] Articles L841-1 et L833-8 du CSI.

solution du litige dépend de l'examen de la régularité d'une ou de plusieurs techniques de recueil de renseignement »[130].

Deuxièmement, la formation spécialisée est compétente, toujours en vertu des articles précités, pour connaître des requêtes relatives « *aux traitements ou parties de traitements intéressant la sûreté de l'État* »[131]. Ces traitements sont des fichiers détenus notamment par les services de renseignement dans lesquels des individus peuvent être placés. L'article R841-2 du CSI liste ces « fichiers ». Par exemple y figure le FSPRT[132], ce dernier est « *une base de données collaborative partagée avec les services de plusieurs ministères engagés dans la lutte contre le terrorisme et la radicalisation violente* »[133]. Là encore, comme pour les techniques de renseignement, le requérant doit avoir, avant la saisine du Conseil d'État, fait une demande, par écrit[134], à la CNIL visant à accéder, rectifier et/ou effacer les données contenues dans l'un des fichiers intéressants la sûreté de l'État. C'est donc uniquement lorsque l'administré aura reçu une décision de la CNIL jugée non concluante qu'il saisira le juge administratif.

87. ***Composition de la formation spécialisée***. Cette formation du Conseil d'État est composée, selon l'article R773-8 du CSI, de trois conseillers d'État ainsi que deux suppléants (« *ayant au moins le grade de maître des requêtes* »). Les membres de cette formation spécialisée exercent aussi la fonction de rapporteur. Pour rappel, l'ensemble des membres sont habilités secret défense, il en va de même des agents qui les assistent (v. article L773-2 du CJA).

88. ***L'office du juge***. Lorsqu'elle est saisie, la formation spécialisée du Conseil d'État jouit de prérogatives importantes, qualifiables, pour se référer à la distinction classique, de prérogatives de plein contentieux. Tout d'abord, la formation spécialisée peut annuler une décision, cette dernière

---

[130] Le cas échéant il aura un mois pour statuer à compter de sa saisine.
[131] Article L841-2 du CSI.
[132] Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste. Créé par le décret du 5 mars 2015 portant création d'un traitement automatisé de données à caractère personnel dénommé « Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste » après l'avis de la CNIL.
[133] https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents/fichier-de (site DGSI).
[134] Article 141 du Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

sera souvent une décision de refus d'accès à un fichier rendue par l'administration[135] (ou bien une décision de la CNCTR lorsque le recours concerne la régularité d'une technique de renseignement). La formation spécialisée pourra aussi recourir à son pouvoir d'injonction, notamment pour enjoindre le service de renseignement concerné d'effacer les données qui ont été recueillies ou conservées de manière irrégulière[136]. Enfin, elle peut aussi condamner l'administration à réparer le préjudice subi par le requérant du fait de la mise en place d'une technique irrégulière à son encontre ou de l'apparition de son nom de manière irrégulière dans un traitement intéressant à la sûreté de l'État. Sur ce dernier point, l'article L773-7 du CJA autorise la formation spécialisée à condamner l'État à réparer le préjudice subi par le requérant. Cependant, la formation spécialisée n'a pas encore prononcé une condamnation de l'administration pour les faits énoncés. D'après une analyse des décisions rendues, les conclusions des requérants tendent très souvent à la réparation du préjudice subi, mais le Conseil d'État écarte systématiquement les demandes de réparation jusqu'ici[137]. Les pouvoirs du juge sont donc qualifiables d'habituels, qualificatif compliqué à appliquer à la procédure…

89. ***L'état de la procédure actuelle devant la formation spécialisée : « une contradiction asymétrique »[138]***. Le principe du contradictoire est le principe central des procédures juridictionnelles. Il est rattaché au droit de la défense et est protégé tant par le droit national que par le droit international[139]. Il permet à chaque partie d'avoir été en mesure de discuter les faits et les arguments avancés par l'autre partie. En ce qui concerne la procédure administrative, l'article

---

[135] « *Mme B…demande (…) d'annuler la décision, révélée par le courrier de la présidente de la Commission nationale de l'informatique et des libertés (CNIL) du 27 juin 2013, par laquelle le ministre de la défense lui a refusé l'accès aux données susceptibles de la concerner et figurant dans les traitements automatisés (…)* ». V. Conseil d'État, Formation spécialisée, 08/11/2017, n°396549.

[136] « *Article 1er : Il est enjoint à la ministre des armées, direction du renseignement militaire, de procéder à l'effacement des données concernant Mme B...illégalement contenues dans les traitements de données nominatives de la direction du renseignement militaire* ». V. Conseil d'État, Formation spécialisée, 08/11/2017, n°396549.

[137] « *Mme D... A… demande au Conseil d'Etat (…) de condamner l'Etat à lui verser une somme de 10 000 euros en réparation du préjudice moral subi (…)* », « (…) ses conclusions doivent être rejetées, y compris ses conclusions à fin d'injonction, à fin d'indemnisation et celles présentées au titre de l'article L. 761-1 du code de justice administrative ». V. Conseil d'État, Formation spécialisée, 04/02/2022, n°449791, Inédit au recueil Lebon.

[138] Locution utilisée par la Conseillère d'État Emmanuelle Prada-Bordenave, v. *Le contrôle juridictionnel : un contrôle précisément défini par le législateur et confié à une formation spécialisée du Conseil d'État*, Le droit du renseignement, 2019.

[139] Rattaché à l'article 6 de la CEDH.

L5 du CJA dispose que : « *l'instruction des affaires est contradictoire. Les exigences de la contradiction sont adaptées à celles de l'urgence, du secret de la défense nationale et de la protection de la sécurité des personnes* ». Dès la lecture de cet article, il est aisé de comprendre que le contradictoire comprend des exceptions, notamment lorsque les exigences de préservation du secret de la défense nationale s'ajoutent[140]. La loi du 24 juillet 2015 préserve au maximum les potentielles fuites d'informations classifiées. Cette prudence créée un déséquilibre entre la partie requérante, qui se demande si elle est visée par une technique de renseignement irrégulière ou si son nom figure dans un fichier de manière irrégulière, et la partie défenderesse, à savoir le gouvernement et les services de renseignement.

Dès l'instruction, cette « *contradiction asymétrique* » est remarquée. L'article L773-2 du CJA précise que les membres de la formation peuvent connaître de l'ensemble des pièces, même classifiées, possédées par la CNCTR ou les services de renseignement dès lors que ces pièces sont « *utiles à l'exercice de leur office* ». L'article R773-20 du même code dispose que le défendeur, c'est-à-dire le service de renseignement et le gouvernement, indique les pièces grevées du secret de la défense nationale. Le requérant aura accès aux pièces du dossier, sauf pour celles classifiées. Dès lors que dans ce contentieux la quasi-totalité des pièces est classifiée[141], le requérant n'aura accès à aucune pièce relative à ce qu'il entend contester. De plus, comme le précise l'article L773-2 dudit code, lors de l'instruction, les parties peuvent être auditionnées. Ces auditions auront lieu séparément lorsque sera en cause le secret de la défense nationale (c'est-à-dire systématiquement).

Cette inégalité n'est pas réglée une fois l'instruction finie. Lors de l'audience, dès que le secret de la défense nationale est en cause, le président de la formation doit ordonner le huis clos (article L773-4 du CJA). Autrement dit, la partie requérante et son représentant ne participent pas à l'audience. Le prononcé de la décision de la formation spécialisée est très encadré. Lorsque le juge ne constate pas d'illégalité, le requérant est informé qu'aucune illégalité n'a été constatée sans préciser si ce dernier fait réellement l'objet d'une technique de renseignement (article L773-6 du

[140] Cette idée est reprise à l'article L773-3 du CJA : « *les exigences de la contradiction mentionnées à l'article L5 du présent code sont adaptées à celles du secret de la défense nationale* ».
[141] Constat couplé au phénomène de ce que certains qualifient d'abus de recours à la qualification secret défense. V. par exemple : https://www.senat.fr/leg/ppl04-023.html (site du Sénat).

CJA). En revanche, si le juge constate une illégalité (par exemple une technique de renseignement mise en place de façon irrégulière), il peut annuler la technique ou exiger la destruction des renseignements irrégulièrement collectés. Le cas échéant, il en informe le requérant sans dévoiler des informations classifiées (articles L773-7 et L773-8 du CJA).

90. ***Les conséquences de cette inégalité procédurale***. Même si le contentieux dont est saisie la formation spécialisée doit préserver les informations grevées du secret défense, le législateur semble avoir été très prudent sur la procédure mise en place, voire trop prudent, et ce sans minimiser les progrès apportés par la création d'un contrôle juridictionnel spécialisé. En effet, le principe du contradictoire n'est pas appliqué dans la procédure prenant place devant cette formation. Le requérant est placé dans une obscurité totale et doit par conséquent espérer que les juges réalisent un réel contrôle et qu'ils appliquent réellement le droit, surtout que personne ne défend ses droits lors de l'audience. D'autant plus que lors de cette dernière le juge entend les défenseurs, ce qui au vu des arguments avancés (par exemple la dangerosité supposée du requérant), pourrait amener le juge à fermer les yeux sur une irrégularité. Ce défaut de contradictoire pourrait être sanctionné par les juridictions européennes, soit sur le fondement de l'article 6 de la CEDH (si condamnation par la CEDH) ou soit sur celui de l'article 47 de la Charte des droits fondamentaux (si condamnation par la CJUE). Ces risques de condamnation de la France sont accrus lorsqu'est comparé le cas français à certains de ses homologues, qui forcé de le reconnaître donnent une place plus importante à la protection des droits du requérant. De plus en cas d'illégalité constatée, certes le requérant en est informé, mais comment peut-il s'assurer que cette dernière soit stoppée ? Encore une fois, il est laissé face à l'espérance que l'administration respecte l'État de droit. Cette espérance ne suffit pas pour les requérants, ils ont besoin d'une plus grande certitude sur l'effectivité du contrôle exercé par le juge et sur les suites données à la décision rendue. D'autant plus que l'exigence d'un contrôle a posteriori des activités de renseignement est primordiale afin d'éviter les dérives dans l'application des autorisations de techniques de renseignement ou dans l'usage des traitements intéressants la sûreté de l'État. Par conséquent, la procédure actuelle ne permet pas de satisfaire réellement les exigences d'un procès équitable. Pourtant, des solutions pourraient être mises en place, par le législateur, afin d'améliorer la prise en compte du contradictoire et les droits du requérant lors du contrôle juridictionnel a posteriori des activités de renseignement…

Paragraphe 2 : Les éventuelles solutions pour une meilleure prise en compte du contradictoire

91. ***Contextualisation.*** Après avoir démontré dans le paragraphe précédent que la procédure mise en place par le législateur devant la formation spécialisée du Conseil d'État plongeait le requérant dans une situation obscure qui devait évoluer, il est temps de proposer des solutions. Ces dernières sont parfois inspirées de ce qui se fait dans les autres États occidentaux.

92. ***L'accès du requérant aux pièces classifiées le concernant.*** Certains pourraient se demander pour quelles raisons le requérant ne pourrait pas avoir accès aux pièces qui le concernent. En effet, autoriser l'accès du requérant aux pièces réglerait directement les problèmes liés à ce « *contradictoire asymétrique* ». Cependant cette solution n'est aucunement viable, et ce pour plusieurs raisons.

D'abord, l'objet de la loi du 24 juillet 2015 est d'encadrer le recours aux techniques de renseignement les plus liberticides, et donc de garantir les droits des administrés, mais cet encadrement ne doit pas se faire au détriment de l'efficacité des services de renseignement, qui, pour rappel, sont essentiels à la sauvegarde des intérêts fondamentaux de la Nation (et à l'exercice des libertés fondamentales). La ratio legis du livre VIII du CSI est fondée sur cette recherche d'équilibre, par conséquent ouvrir l'accès des requérants aux pièces classifiées serait non souhaitable, cette amélioration de la procédure contentieuse ne peut pas passer par une solution aussi radicale.

Certes, le requérant se doute qu'une technique de renseignement a été mise en place à son encontre (ou qu'il pourrait figurer dans certains fichiers) lorsqu'il demande d'abord à la CNCTR (ou la CNIL) puis au Conseil d'État de vérifier qu'aucune technique n'est mise en place de manière irrégulière. Mais la simple certitude qu'une technique est bien mise en place à son encontre reviendrait à paralyser l'action des services de renseignement. En effet, l'accès aux pièces classifiées viendrait confirmer son doute. Il ne faut pas oublier que les services de renseignement surveillent, en principe, des individus dont la dangerosité inquiète les pouvoirs publics. C'est pourquoi le formalisme contenu dans le CJA est logique et doit rester ainsi.

Enfin, au-delà d'affirmer les questionnements du requérant, l'accès de ce dernier aux pièces classifiées reviendrait à dévoiler les méthodes de fonctionnement des services de renseignement, ce qui serait réellement problématique pour leur efficacité. Le dossier comprend des pièces classifiées retraçant les moyens par lesquels ces techniques sont mises en place, les résultats apportés par ces dernières et surtout les noms des agents exécutants (ce qui pourrait les exposer à des atteintes à leur intégrité physique ou celle de leurs proches).

Pour l'ensemble de ces raisons, il est impossible pour le législateur d'autoriser l'accès du requérant, qui est en principe potentiellement dangereux pour les intérêts fondamentaux de la Nation, à l'ensemble des pièces permettant au Conseil d'État d'exercer son contrôle. Par conséquent, il apparaît clairement que les solutions jugées sérieuses devront obligatoirement passer par l'intermédiaire d'un tiers. Ce dernier pourra soit être en contact avec le requérant soit sans contact avec ce dernier.

93. ***La création d'un avocat spécialisé habilité secret-défense.*** Cette idée est loin d'être une hypothèse comme les autres. En effet, elle est déjà appliquée dans certains pays anglo-saxons sous l'appellation « *special advocate* ». Cette piste d'amélioration a été mentionnée notamment par le Professeur Bertrand Warusfel dans l'un de ses articles[142]. Ce « *special advocate* » est un avocat habilité secret-défense, autre que l'avocat habituel du requérant, qui en raison de son habilitation a accès à l'ensemble des pièces classifiées du dossier, au même titre que la partie défenderesse et que les juges. Cet avocat spécial pourra donc défendre les intérêts de son client pendant l'instruction et l'audience nonobstant l'absence de ce dernier lors des différentes étapes grevées par le secret-défense. L'intronisation de ce type d'avocat permettrait à cette procédure contentieuse spécifique de devenir contradictoire.

Au Canada, ce « *special advocate* » est nommé par le tribunal. Il est donc indépendant des pouvoirs publics et n'a aucune relation avec le client qu'il défend. Bien évidemment les avocats spéciaux sont tenus de respecter la confidentialité des informations auxquelles ils vont avoir accès. Ce mécanisme a été mis en place dans le pays dès 2008 par une modification de la loi relative à

[142] Bertrand Warusfel, *Acquis et limites de l'encadrement : premier bilan d'étape de la réforme*, 28 octobre 2018 (https://hestia.hypotheses.org/1053).

l'immigration et à la protection des réfugiés[143]. L'avocat spécial jouit d'un panel de prérogatives large, il peut « *contester la pertinence, la fiabilité et le caractère suffisant des renseignements* » (…) *« fournis par le ministre »* (…) *« et l'importance qui devrait leur être accordée* »[144] sans le communiquer à la partie exclue de la procédure. Il peut aussi présenter des observations orales ou écrites, « *contre-interroger* » les témoins ainsi qu' « *exercer tout autre pouvoir nécessaire à la défense des intérêts de l'intéressé* ». Selon l'État canadien, ce « *special advocate* » permet « *d'accroître l'équité des audiences tenues à huis clos sans empêcher le Canada de protéger les renseignements confidentiels* »[145]. Ce type d'avocats existe également au Royaume-Uni.

La retranscription de ce mécanisme au cas français serait tout à fait plausible. Certains avocats au Conseil d'État et à la Cour de cassation pourraient être habilités secret-défense et être désignés par la formation spécialisée pour défendre le requérant. Ce dernier pourrait être défendu par un avocat réellement indépendant tant pendant l'instruction que pendant l'audience à huis clos. Il serait même possible pour cet avocat habilité de suivre l'exécution par les services de renseignement de la décision rendue par la formation spécialisée lorsque cette dernière constaterait une irrégularité. Le requérant serait donc assuré, le cas échéant, que les irrégularités soient stoppées (par exemple la suppression des données irrégulièrement conservées). Cela permettrait donc une meilleure confiance pour le requérant dans l'effectivité du contrôle et de ses conséquences.

Pour les plus craintifs concernant les éventuelles fuites d'informations (ou de méthodes) classifiées, ces avocats spécialisés seraient soumis, comme l'ensemble des personnes habilitées secret-défense, aux dispositions pénales protégeant les informations classifiées. En d'autres termes, l'article 413-10 du Code pénal[146] s'appliquerait aux avocats spéciaux. Si la preuve que ces derniers ont divulgué une information classifiée est amenée, ils s'exposeraient à une peine allant jusqu'à sept ans d'emprisonnement et 100 000 euros d'amende. Au vu de la sélection à laquelle font l'objet

---

[143] Cette modification fait suite à une décision de la Cour Suprême du Canada, affaire Charkaoui contre Canada (23 février 2007).

[144] Site internet du ministère de la Justice canadienne (https://www.justice.gc.ca/fra/fina-fund/sjp-jsp/es-sa.html).

[145] *Ibid*.

[146] « *Est puni de sept ans d'emprisonnement et de 100 000 euros d'amende le fait, par toute personne dépositaire (…) d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit d'en donner l'accès à une personne non qualifiée ou de le porter à la connaissance du public ou d'une personne non qualifiée (...)*».

les avocats au Conseil d'État et la Cour de cassation et la possibilité de se voir engager leur responsabilité pénale, les risques de fuite d'informations classifiées seraient quasiment inexistants (ou du moins pas plus importants que pour certains agents des services de renseignement). D'autant plus que lors de leur habilitation, ces avocats feraient déjà l'objet d'un premier contrôle.

Cette possibilité d'instaurer des avocats spéciaux semble donc totalement possible, mais au vu des habitudes institutionnelles françaises, une évolution de la procédure contentieuse mise en place devant la formation spécialisée ne semble pas en préparation, seule une condamnation de la France (par la Cour EDH par exemple) sur ce point précis laisserait penser à la possibilité d'une évolution législative.

93. ***L'instauration d'un représentant chargé de la protection de la vie privée***. Cette solution rejoint celle du *special advocate* dans le sens où elle fait intervenir un tiers indépendant à la procédure. Ce représentant serait donc un tiers chargé de veiller à ce que la vie privée du requérant soit respectée, que le droit soit appliqué, de veiller au contrôle effectif du Conseil d'État et de l'application de ses décisions.

Ce type de représentant a été instauré en Suède dans la procédure mise en place devant le Tribunal de renseignement de la défense. Cependant, le cas suédois jouit de nombreux problèmes que la France ne doit pas reproduire. En effet, ce représentant chargé de la protection de la vie privée est nommé par un le gouvernement pour un mandat de quatre ans renouvelables[147], ce qui pose des doutes importants concernant sa réelle indépendance. De plus, se représentant est supposé défendre l'intérêt public et non réellement représenter la partie requérante, il n'est donc pas chargé de veiller uniquement à l'application du droit. Enfin, en cas d'urgence, ce représentant n'est même pas consulté. Ces carences importantes ont amené à la condamnation, par la Cour EDH, de la Suède en 2021 pour violation de l'article 8 de la convention[148].

La France pourrait s'inspirer à la fois du cas suédois et des exigences de la Cour EDH concernant ce représentant pour améliorer le contradictoire dans la procédure mise en place devant

[147] À cela s'ajoute la composition du Tribunal de renseignement de la défense qui a déjà une coloration politique (pas de juge professionnel).
[148] Affaire *Centrum för Rättvisa contre Suède*, 25 mai 2021.

la formation spécialisée du Conseil d'État. Ce représentant serait donc habilité secret-défense et représenterait uniquement le requérant de l'instruction à l'exécution de la décision rendue par la formation spécialisée. Trois hypothèses pourraient alors être mises en place.

Premièrement, ce représentant pourrait recevoir le statut juridique d'autorité administrative indépendante à la lumière du Défenseur des droits ou du Contrôleur général des lieux de privations de liberté. À la différence du *special advocate*, il pourrait être dédié uniquement à cette fonction, ce qui éviterait d'éventuels conflits d'intérêts. Ce représentant chargé de la protection privée serait donc nommé par le pouvoir exécutif ou par le Parlement pour un mandat non renouvelable (pour une meilleure indépendance). Cette hypothèse offrirait une réelle indépendance pour le représentant et une spécialisation de ce dernier. Cette personne habilitée secret-défense pourrait être un journaliste, un magistrat judiciaire, un magistrat administratif, etc.

Deuxièmement, ce représentant pourrait être un membre du Conseil d'État nommé par le vice-président pour une durée donnée. Ce choix aurait l'avantage d'avoir un représentant technicien et, certes moins indépendant que dans la première hypothèse, mais tout de même un conseiller d'État (donc en principe indépendant). Ce dernier pourrait même participer au délibéré.

Enfin, ce représentant pourrait être incarné par le rapporteur public, qui au-delà d'éclairer l'affaire pourrait défendre activement les intérêts du requérant. Cette idée a notamment a été émise par le Professeur Warusfel dans l'un de ses articles. Cependant, elle semble plus compliquée à réaliser. D'abord, car le rôle intrinsèque du rapporteur public n'est pas de défendre les intérêts du requérant (il doit prendre en compte d'autres éléments) et que ce dernier ne pourrait pas assister au délibéré (si demande d'une des parties) contrairement à la seconde hypothèse.

94. ***Conclusion section***. La procédure contentieuse mise en place dans le contrôle a posteriori devant la formation spécialisée du Conseil d'État n'est pas convaincante. Certes, les informations classifiées doivent être absolument protégées, mais le principe du contradictoire peut et doit être mieux traité. D'autant plus que le législateur dispose de nombreuses possibilités pour améliorer cette situation. La solution optimale serait de mettre en place un *special advocate* ou un représentant chargé de la protection de la vie privée sous forme d'AAI. Mais, comme souvent, il

faudra certainement attendre une condamnation de la France (si elle a lieu) par le Cour EDH pour que les choses évoluent. Ces évolutions sont également souhaitables dans le cadre des prérogatives et moyens conférés à la CNCTR pour réaliser son contrôle a posteriori, notamment face à l'augmentation des prérogatives dont jouissent les services de renseignement.

Section 2 : L'augmentation souhaitée des prérogatives de la CNCTR pour son contrôle a posteriori

95. ***Rappel***. La CNCTR joue un rôle primordial dans le cadre du contrôle a priori, en étant l'organe de contrôle principal. Ce rôle continue dans le cadre du contrôle a posteriori, c'est-à-dire pendant l'exécution de l'autorisation conférée par le Premier ministre. Le contrôle a posteriori est consubstantiel à un contrôle fort et effectif des activités de renseignement.

96. ***Annonce***. Après avoir étudié la nature et la contenance du contrôle opéré par la CNCTR (***paragraphe 1***), il sera temps d'expliquer pour quelles raisons les prérogatives de la CNCTR devraient être augmentées (***paragraphe 2***).

Paragraphe 1 : La nature et la contenance du contrôle opéré a posteriori par la CNCTR

97. ***Les deux types de contrôles a posteriori possibles***. La CNCTR peut recourir à deux méthodes pour réaliser la tâche qui lui est conférée par le livre VIII du CSI. Premièrement, elle peut faire un contrôle depuis ses locaux grâce à la mise à disposition, par le GIC, d'outils informatiques visant à vérifier la conformité de l'action des services dans la mise en place de la technique, dans l'extraction des données/informations et dans leur traitement. Le GIC joue donc un rôle capital, sans lui, le contrôle de la CNCTR (comme la centralisation des renseignements) serait très complexe (voire impossible). Ces contrôles sont les principaux, ce constat a été accentué avec les restrictions pendant la crise sanitaire. Deuxièmement, les membres de la CNCTR peuvent se déplacer dans les locaux des services de renseignements, afin de réaliser des contrôles sur pièces et sur place. Selon le sixième rapport d'activité de la CNCTR, ces contrôles sont en moyenne de deux (voire trois) par semaine.

98. ***Les missions et moyens conférés à la CNCTR dans le contrôle a posteriori par le Livre VIII du CSI***. L'article L833-1 du CSI confère une mission primordiale à la CNCTR, celle de veiller à « *ce que les techniques de recueil de renseignement soient mises en œuvre sur le territoire national conformément au présent livre* ». Cette mission est réalisée tant grâce au contrôle a priori précédemment mentionné que grâce au contrôle a posteriori. Pour réaliser ce dernier, la loi lui confère un « *accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions, extractions et transmissions* » ainsi qu' « *aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces derniers* »[149]. En d'autres termes, la CNCTR peut avoir accès en tout temps à l'ensemble de ces pièces, et ce en grande partie grâce au GIC. La CNCTR peut aussi demander à tout moment des précisions quant aux modalités d'exécution des autorisations en cours. De plus, elle peut demander au Premier ministre la transmission d'éléments « *nécessaires à l'accomplissement de ses missions* », sauf en ce qui concerne les renseignements donnés par les services étrangers ou des organismes internationaux, car selon la loi cela pourrait amener à divulguer l'identité de certaines sources[150]. Enfin, la CNCTR peut demander la transmission de rapport par l'inspection des services de renseignement en passant par le Premier ministre. La commission se voit donc conférer des moyens sérieux pour résoudre sa tâche, d'autant plus qu'en cas de mauvaise volonté du gouvernement ou de l'administration, ces derniers s'exposent à des sanctions pénales. En effet, l'article L833-3 du CSI punit d'un an d'emprisonnement et de 15 000 euros d'amende le fait d' « *entraver l'action de la commission* », notamment en refusant de communiquer les documents sollicités en vertu de l'article L833-2.

En outre, la CNCTR réalise ce contrôle également grâce aux « *fiches de traçabilité* » tenues par les services de renseignement. Ces fiches visent à tracer l'évolution de l'exécution des autorisations conférées par le Premier ministre. Elles sont également numérisées et rendues accessibles à la commission grâce encore une fois au GIC. Elles permettent notamment à la CNCTR de préparer ses contrôles sur pièce et sur place, mais aussi de dialoguer avec les services de renseignement.

---

[149] V. article L833-2 CSI.

[150] Ce point sera traité dans le second paragraphe.

La CNCTR exerce cette mission de contrôle de l'exécution des techniques de renseignements au quotidien. Elle peut aussi être saisie par tout administré souhaitant vérifier s'il est visé par une technique de renseignement autorisée ou exécutée de manière irrégulière (article L833-4 du CSI). Pour rappel, le requérant pourra saisir la formation spécialisée du Conseil d'État si ce dernier n'est pas convaincu par la réponse rendue (v. supra).

99. ***Le contenu du contrôle a posteriori***. La CNCTR est chargée de veiller à ce que l'exécution des techniques de renseignement des chapitres 1er, 2nd et 3ème du titre V respectent l'article L801-1[151]. Autrement dit, elle veille à ce que la technique soit exécutée par une autorité compétente, que la technique ait été autorisée conformément à la procédure prévue, que la technique entre dans les missions dévolues aux services de renseignement, que la technique réponde à l'une des finalités de l'article L811-3[152] et enfin à la proportionnalité de cette technique[153].

En outre, la CNCTR vielle au respect des règles concernant le stockage et la conservation des renseignements collectés (ou aux stockages des informations brutes, c'est-à-dire non traitées). Ces règles relatives à la conservation sont fixées par le Premier ministre en vertu de l'article L822-1 et sont regroupées à l'article L822-2. La durée de conservation diffère en fonction du type de technique utilisée. Par exemple, cette durée est de 30 jours pour les correspondances interceptées via la technique dite des « *interceptions de sécurité* » de l'article L852-1. Pour information, les services de renseignement peuvent déroger à ces durées de conservation lorsque cela est motivé par des fins « *de recherche et de développement en matière de capacités techniques de recueil et d'exploitation des renseignements* ». Cette exception est contrôlée par la CNCTR (qui veille à ce que ces données exceptionnellement conservées plus longtemps le soient pour les raisons avancées).

Enfin, la CNCTR joue un rôle en cas de transmission de renseignements d'un service à un autre. Le service titulaire de l'autorisation peut collecter des renseignements sans lien avec la

---

[151] C'est-à-dire les techniques relatives aux données de connexion (chapitre I), aux interceptions de sécurité (chapitre II) et à « *la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques* » (chapitre III).
[152] Article L822-3 du CSI.
[153] Article L833-5 du CSI.

finalité prévue dans l'autorisation uniquement si ces derniers intéressent une autre finalité mentionnée à l'article L811-3 utiles pour ses missions. Par exemple, lorsqu'un service met en place une technique de surveillance des télécommunications pour prévenir le terrorisme, il peut, si le cas se présente, transcrire des renseignements en lien avec « *la prévention de la criminalité et de la délinquance organisées* ». Cette règle permet donc aux services de renseignement de ratisser très large… Lorsque ce service veut transmettre un renseignement à un autre service (du 1er ou du 2nd cercle) deux cas se présentent. En principe, la transmission audit service est libre si « *cette transmission est strictement nécessaire à l'exercice des missions du service destinataire* ». En revanche, lorsque le renseignement transmis poursuit « *une finalité différente de celle qui en a justifié* » son recueil[154] ou lorsque le renseignement a été recueilli grâce à une technique que le service destinataire ne peut pas utiliser au titre de la finalité motivant la transmission, une nouvelle autorisation du Premier ministre doit avoir lieu après avis de la CNCTR[155]. Ce contrôle a pour objet principal d'éviter que les services n'ayant pas accès à la technique souhaitée (soit, car le service ne peut pas y procéder soit, car la finalité invoquée ne le permet pas) contourne cette interdiction en s'arrangeant avec un autre service.

Lorsqu'elle constate une irrégularité[156] dans l'exécution de l'autorisation, la CNCTR jouit de deux possibilités. D'une part, elle peut procéder à un dialogue avec le service concerné pour demander la destruction des renseignements collectés irrégulièrement. D'autre part, lorsque la première possibilité échoue, la commission peut adresser des recommandations[157] au Premier ministre, au ministre concerné ou encore au service concerné[158]. Lorsque la commission n'est pas satisfaite des suites données (aux recommandations) par le Premier ministre, elle peut[159], en vertu de l'article L833-8, saisir la formation spécialisée du Conseil d'État. Cette disposition est capitale. Elle permet à la CNCTR de se reposer sur le pouvoir d'injonction du Conseil d'État (s'il suit la

[154] Par exemple, un renseignement collecté par un service A pour une finalité visant la prévention du terrorisme qui est transmis à un service B pour « *la prévention de la criminalité et de la délinquance organisées* ».
[155] Article L822-3 CSI.
[156] Par exemple, la commission constate que la durée d'autorisation de quatre mois est dépassée.
[157] Parfois, elle n'a pas besoin de recourir aux recommandations et une discussion avec les services de renseignement suffit à faire stopper l'irrégularité.
[158] Article L833-6 du CSI.
[159] Plus précisément son président ou trois de ses membres.

demande de la CNCTR bien évidemment) dans le cas où le Premier ministre ne serait pas (ou pas assez) coopératif.

100. ***Quelques chiffres sur le contrôle a posteriori réalisé par la CNCTR***. La commission relève plusieurs irrégularités dans l'exécution des autorisations par les services de renseignement, dont certaines sont récurrentes. Sont comprises parmi ces irrégularités récurrentes, d'une part le dépassement du délai pour lequel les autorisations sont données (4 mois pour rappel), et d'autre part, le dépassement du délai de conservation des données collectées. Même si ces dernières sont constatées chaque année, elles restent tout de même rares par rapport au nombre d'autorisations exécutées (de plus, elles sont souvent non intentionnelles). Par exemple, pour l'année 2021, le dépassement du délai d'autorisation a été relevé qu'une seule fois, et seulement trois fois pour les années 2019 et 2020.

Une autre irrégularité récurrente, selon le sixième rapport d'activité de la CNCTR, renvoie à la retranscription de conversations obtenues grâce aux techniques d'interception de communication ou de captation de paroles sans aucun lien avec les finalités prévues à l'article L811-3. Ces irrégularités ne sont pas anodines, car elles viennent directement porter une atteinte non justifiée à la vie privée. Il est rassurant que la CNCTR puisse relever ce type d'irrégularité. D'autant plus que ce constat entraîne la destruction des transcriptions par le service concerné, et ce à la suite d'un dialogue entre la commission et ledit service. Pour information, ce contrôle des transcriptions est obligatoire pour les personnes protégées (magistrat, avocat, parlementaire et journaliste)[160].

Une autre irrégularité problématique relevée par la CNCTR renvoie à une erreur de ciblage par les services de renseignement. Autrement dit, les services transcrivent ou extraient des informations sans lien avec la personne visée par l'autorisation. Là encore, un dialogue suffit généralement entre le service concerné et la commission pour faire cesser l'irrégularité, même si en 2021, la CNCTR a dû recourir à son pouvoir de recommandation une fois pour faire cesser cette irrégularité.

Enfin, la dernière irrégularité importante concerne les manquements à la traçabilité des données recueillies. Autrement dit, il se produit lorsque les services de renseignement ne signalent pas les transcriptions effectuées ou ne rendent pas immédiatement accessibles ces dernières. Ce

[160] Article L821-7 du CSI.

manquement a été constaté vingt fois au cours de l'année 2021. La lutte contre ces manquements est importante, car ces derniers empêchent la réalisation du contrôle effectif de la CNCTR.

101. ***Remarques sur les prérogatives actuelles de la CNCTR***. La CNCTR est en mesure de réaliser un contrôle relativement complet sur l'exécution des activités de renseignement. Cette possibilité est avant tout garantie par l'accès direct aux relevés, registres, renseignements collectés, transcriptions et extractions par l'intermédiaire du GIC. Le législateur ajoute parfois des améliorations au contrôle de la CNCTR. Par exemple, la loi du 30 juillet 2021 vient rendre obligatoire la transmission à la CNCTR des transcriptions ou des extractions par les services de renseignement lorsqu'elles « *poursuivent une finalité différente de celle au titre de laquelle les renseignements ont été recueillis* »[161]. Cependant, face au développement important de nouvelles techniques par les services de renseignement (et de la fréquence à laquelle ils y recourent), la CNCTR paraît parfois en difficulté. De plus, son contrôle ne porte pas sur l'ensemble des techniques de renseignement du Livre VIII utilisées par les services de renseignement.

Paragraphe 2 : La nécessité d'augmenter les prérogatives de la CNCTR au vu du contexte actuel

102. ***Les raisons nécessitant l'augmentation des prérogatives de la CNCTR.*** Les techniques de renseignement utilisées par les services sont en perpétuelle évolution, et ce en raison des progrès techniques qui irriguent nos sociétés. Chaque année le champ des possibles se voit élargi, et généralement, les services de renseignement jouissent des avancées technologiques les plus récentes. Par exemple, la loi du 30 juillet 2021, au-delà de pérenniser la technique dite de l'algorithme, vient permettre aux services d'intercepter des correspondances émises par voie satellitaire, et ce sans avoir à demander l'accès aux opérateurs offrant ce service[162]. Cette technique vient donc permettre la surveillance des individus qui recouraient aux communications satellitaires pour contourner la surveillance des fournisseurs de réseaux. Concomitamment à ces évolutions technologiques, le recours aux techniques de renseignement prévues au livre VIII ne cesse

[161] Article L822-4 du CSI.

[162] Cette technique est prévue à l'article L852-3 du CSI, et est limitée aux « *seules finalités prévues aux 1°, 2°, 4° et 6° de l'article L. 811-3* ». De plus, l'autorisation est donnée pour une durée de 30 jours (exception au délai de droit commun qui est de 4 mois) et est soumise à un nombre limite d'autorisation prononcée simultanément.

d'accroître. Selon le sixième rapport d'activité de la CNCTR, entre 2017 et 2021, le nombre de techniques autorisées a augmenté de 24,4 %[163]. Le nombre de personnes surveillées a, quant à lui, augmenté de 7,4 %, ce qui montre que certains individus sont visés par plusieurs techniques de renseignement. Cette augmentation peut en partie s'expliquer par l'augmentation du nombre de services faisant partie du « *second cercle* ». Or, les moyens et les prérogatives de la CNCTR, pour contrôler a posteriori l'exécution des autorisations, ne suivent pas une évolution comparable aux moyens dont disposent les services de renseignement. D'autre part, la CNCTR ne peut pas réaliser un contrôle sur certaines actions liées directement ou indirectement à des techniques de renseignement du livre VIII. Enfin, le législateur confère de plus en plus de missions à la CNCTR. Par exemple, la loi du 30 juillet 2021 charge la commission de contrôler la transmission de renseignements entre services (v. point 84 et article L822-3 du CSI).

103. ***L'instauration nécessaire d'un contrôle de la CNCTR sur les renseignements issus des services étrangers***. Pour rappel, l'article L833-2 permet à la CNCTR, afin de réaliser sa mission de contrôle, de « *solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions* ». Cependant, l'article prévoit une exception pour les « *éléments communiqués par des services étrangers ou par des organismes internationaux* », car cela pourrait amener à « *donner connaissance à la commission, directement ou indirectement, de l'identité des sources des services spécialisés de renseignement* ». La raison évoquée par la loi paraît ici absurde. Quels seraient les risques liés au fait que les membres de la CNCTR connaissent l'identité des sources des services de renseignement ? La réponse à la question semble limpide, aucun. L'exception soulevée par ledit article fonde aussi le refus fréquent d'interdire l'accès de la CNCTR aux données contenues dans les fichiers intéressants la sûreté de l'État. Cette restriction paraît encore moins justifiable lorsque la loi permet à la CNIL d'accéder aux fichiers intéressants la sûreté de l'État (et devient susceptible de connaître l'identité de certaines sources des services spécialisés)… Comme l'explique la CNCTR, ce point expose le régime français à une condamnation de la Cour EDH pour ne pas mettre en place des garanties de « *bout en bout* »[164]. L'exception soulevée à l'article L833-2 obstrue de manière non justifiée le contrôle de la CNCTR, et doit, par conséquent, être supprimée par le législateur.

[163] V. page 62 du 6ème rapport d'activité de la CNCTR.
[164] V. p. 107 du 6ème rapport d'activité de la CNCTR.

De plus, cette absence de contrôle amène un risque de « *sous-traitance* » du renseignement[165]. En effet, face à l'absence de contrôle de la commission sur les renseignements transmis par les services étrangers, il est craint que les services de renseignement français procèdent à une sorte de « *sous-traitance* » via un service étranger afin de contourner le droit français. En d'autres termes, le droit français, par cette absence de contrôle, permet aux services français de demander à un service étranger de procéder à une surveillance d'une cible (par quelques procédés que cela soit) pour contourner les dispositifs de contrôle mis en place. Ce point met en exergue les carences du droit français concernant les partages de renseignements entre les États. Pourtant, cette absence de contrôle sur les renseignements donnés par les services étrangers peut venir porter atteinte à la ratio legis de la loi qui, pour rappel, est de trouver un équilibre entre respect de la vie privée et l'efficacité d'action. D'autant plus que la Cour EDH ne s'oppose pas aux échanges entre services de renseignement du moment que le droit interne apporte des garanties suffisantes (notamment un contrôle indépendant), ce qui n'est pas le cas actuellement en France. L'ouverture du contrôle de la CNCTR à ces échanges de renseignement semble ici être la solution adéquate. La commission a émis une autre solution qui est de mettre en place une coopération entre les organes de contrôle afin de savoir si le renseignement a été collecté de manière régulière avant d'être transmis. Cette solution paraît plus complexe à mettre en place. Elle nécessite une coopération et une réciprocité relative au niveau du droit entre les États concernés.

104. ***L'extension de l'accès direct aux transcriptions et extractions demandées par la CNCTR***. Le renforcement des exigences de centralisation et de traçabilité ainsi que la généralisation de l'accès à distance par la CNCTR aux données, transcriptions et extractions a permis de rendre efficient ce contrôle a posteriori. Cette centralisation touche progressivement la plupart des techniques. Par exemple, en 2019, le GIC a mis en place cette centralisation concernant les paroles et images capturées grâce aux techniques de sonorisation de certains lieux et véhicules et de captation d'images et de données informatiques[166]. Malgré tout, plusieurs techniques ne sont toujours pas couvertes par cette centralisation (et donc pas de contrôle à distance possible).

Premièrement, la technique de surveillance des communications électroniques internationales prévue à l'article L854-1 du CSI n'offre aucun moyen de contrôle à distance pour

[165] La CNCTR appelle ce risque le phénomène du « *tiers service* ».
[166] Article L853-1 du CSI.

la CNCTR. La commission est donc obligée de réaliser des contrôles sur pièce et sur place, ce qui diminue le nombre de contrôles. Ces contrôles ont démontré certaines irrégularités récurrentes. Par exemple, la commission remarque que les agents dépassent (de façon non intentionnelle généralement) les limites attachées à l'autorisation.

Deuxièmement, deux autres techniques ne sont pas encore concernées par cette centralisation : la technique dite de *l'IMSI catcher*[167] et celle de recueil ou de captation de données informatiques[168]. L'absence de centralisation s'explique ici pour des raisons d'ordre technique. En effet, ces techniques recueillent énormément de données, ce qui rend, pour le moment, impossible leur centralisation en sécurité. Ce volume de données abondants ne permet pas, non plus, à la CNCTR de contrôler sur pièce et sur place de manière efficace l'exécution de ces techniques. Par conséquent, pour le moment, ces techniques ne font pas l'objet d'un contrôle a posteriori efficace, et ce à cause de raisons indépendantes de la volonté des services de renseignements et de la CNCTR. Cependant, la commission émet une solution : l'accès direct (à distance) de la CNCTR aux données recueillies, et ce sans passer par le GIC.

Sur ce point, même si la CNCTR souhaite l'augmentation de ses moyens concernant le contrôle à distance, elle n'entend pas pour autant négliger les contrôles sur pièce et sur place, car ces derniers permettent d'échanger avec les services de renseignement. L'augmentation de ces accès à distance semble être la solution la plus pertinente et indispensable pour que la commission puisse exercer un contrôle complet.

105. ***Les problèmes liés à la traçabilité de certaines techniques***. Même si la CNCTR constate une rigueur des services de renseignement dans la tenue des « fiches de traçabilité », et que, le GIC garantit l'accès à distance de la commission pour ces fiches, certaines difficultés subsistent. En effet, les fiches de certaines techniques ne font toujours pas l'objet d'une centralisation par le GIC. Cela s'explique en partie par l'absence d'outil prévu à ce titre. La technique dite de l'algorithme est notamment concernée par cette non-centralisation des « *fiches de traçabilité* ». Cette absence oblige la commission à s'adresser directement aux services exécutants pour connaître l'évolution

[167] Prévue à l'article L851-6 du CSI, cette technique vise à imiter la présence d'une antenne relai dans un périmètre donné pour que l'ensemble des téléphones portables (non-éteints ou pas en mode avion) se trouvant dans ce périmètre se connecte à cette antenne et par conséquent soit identifiés. Cette technique est de plus en plus utilisée (hausse de 110 % entre 2017 et 2021).

[168] Prévue à l'article L853-2, cette technique permet de s'introduire par divers moyens dans un système informatique afin de copier, conserver et traiter les données informatiques contenues dans ce système.

de la mise en place (ou non) de la technique de renseignement, ce qui fait perdre un temps précieux tant à la CNCTR qu'aux services de renseignement.

106. ***Quelques pistes d'amélioration concernant les prérogatives de la CNCTR***. Au-delà d'étendre l'accès à distance de la commission, tant aux relevés, registres, renseignements collectés, transcriptions et extractions qu'aux « *fiches de traçabilité* », que cela soit par le GIC ou directement avec les services de renseignements, d'autres pistes d'améliorations doivent être mentionnées.

La première de ces solutions relève des moyens humains dont est dotée la commission. Les neuf membres composant cette dernière sont accompagnés pour réaliser ses missions d'un secrétariat général de dix-sept agents, dont onze recrutés pour leur maîtrise des enjeux juridiques et/ou techniques. La CNCTR émet fréquemment le souhait de voir un renforcement de ses effectifs. L'augmentation de ses moyens humains lui permettrait logiquement d'augmenter quantitativement, voire qualitativement, les contrôles effectués.

De plus, en 2020, la commission a essayé de mettre en place un nouveau moyen d'échanger avec les services de renseignement grâce à une communication sécurisée. Cependant, la plupart des services se sont opposés à cette mise en place. Dans son rapport d'activité rendu en 2021, la CNCTR espère que cette difficulté sera surmontée. Le développement de ces moyens de communication sécurisés permettrait une meilleure célérité dans les échanges avec les services de renseignement, ce qui lui permettrait de dégager du temps pour d'autres contrôles, voire de pallier parfois l'absence d'accès à distance à certaines « *fiches de traçabilité* ».

Une autre solution serait de réduire le nombre de services ayant accès aux techniques comprises dans le livre VIII. L'augmentation progressive du nombre de services compris dans le second cercle augmente le nombre de techniques autorisées, et donc par corrélation, le nombre de techniques à contrôler. D'autant plus que la commission souhaitait, dès 2015[169], que seuls les services faisant du renseignement à titre principal puissent faire partie de ce « *second cercle* », et ce notamment en raison des craintes autour de la capacité de certains services à mettre en œuvre de manière sûre l'ensemble des techniques. Or, la vision du pouvoir exécutif ne s'est pas inscrite dans celle souhaitée par la commission, de plus en plus de services judiciaires accèdent, en vertu de l'article L811-4 du CSI, aux techniques du livre VIII. Il serait préférable, d'une part pour alléger le nombre de contrôles à effectuer par la CNCTR, et d'autre part pour clarifier la distinction entre

[169] V. délibération du 12 novembre 2015, n°02-2015.

police administrative et police judiciaire, de retirer les services dont leur vocation principale est la police judiciaire. Bien entendu, ces derniers peuvent accéder aux techniques dans le cadre d'une enquête judiciaire, par conséquent leur activité ne serait pas mise à mal.

107. ***Conclusion chapitre***. Le régime encadrant le contrôle des activités de renseignement reste perfectible. Certaines imperfections pourraient entraîner une condamnation de la France par une décision future de la Cour EDH, c'est le cas par exemple de la procédure non contradictoire mise en place devant la formation spécialisée du Conseil d'État, ou encore, de l'absence de contrôle de la CNCTR sur les renseignements fournis par les services étrangers. Cependant, les solutions pour mettre fin à ces imperfections, comme il a été expliqué, ne manquent pas. Il serait souhaitable de voir le législateur intervenir sur ces points, car il ne faut pas oublier la finalité de ce régime qui est d'avoir un contrôle efficace et complet sur les activités de renseignement, afin d'éviter que ces derniers soient détournés de leur rôle initial (et ce, sans bloquer leur action). Par ailleurs, au-delà des problématiques liées au contrôle de l'exécution des techniques de renseignement, la question concernant le rôle et la présence d'un contrôle politique fort sur ces activités de renseignement se pose.

CHAPITRE 2 : L'ÉLARGISSEMENT SOUHAITABLE DU RÔLE DU PARLEMENT EN MATIÈRE DE RENSEIGNEMENT

108. ***Rappels***. La tâche principale du Parlement est de participer à l'élaboration de la loi. Cependant, en vertu de l'article 24 de la Constitution du 4 octobre 1958, le Parlement se voit confier les missions de contrôler « *l'action du Gouvernement* » et d'évaluer les politiques publiques. Ces contrôles sont primordiaux. La Constitution de 1958 rend responsable le gouvernement devant le Parlement, en découle de nombreuses prérogatives pour ce dernier. Il peut aller jusqu'à voter une mention de censure afin de renverser le gouvernement en place[170]. Cependant, les mécanismes de rationalisation du Parlement mis en place par le constituant de 1958 ont affaibli le Parlement, cet affaiblissement a été accentué par l'avènement du fait majoritaire consolidé par la révision constitutionnelle de 1999[171].

109. ***Annonce***. Le contrôle parlementaire des activités de renseignement s'est développé aux cours de ces dernières décennies, il est important de faire un état des lieux de la teneur actuelle de ce contrôle (***section 1***). Malgré un saisissement des activités de renseignement par le contrôle parlementaire, ce dernier reste timide. Il parait donc nécessaire pour diverses raisons d'augmenter l'impact du contrôle parlementaire (***section 2***).

[170] V. article 49 de la Constitution du 4 octobre 1958.
[171] Cette révision vient faire passer le mandat du président de la République de 7 ans à 5 ans et aligner le calendrier électoral pour faire succéder de près les élections présidentielles puis les élections législatives.

Section 1 : La teneur actuelle du contrôle parlementaire sur les activités de renseignement

110. ***Annonce***. Le contrôle parlementaire actuel est un contrôle qui porte sur les moyens, et non sur les activités de renseignement dans leur entièreté (***paragraphe 1***). Après avoir étudié la teneur de ce contrôle parlementaire, ce dernier sera comparé aux autres contrôles parlementaires réalisés par les démocraties occidentales (***paragraphe 2***).

Paragraphe 1 : Un contrôle limité réalisé par la DPR

111. ***Rappels***. Le contrôle parlementaire des activités de renseignement s'est spécialisé avec la loi du 9 octobre 2007. Cette dernière créée la Délégation parlementaire au renseignement (DPR). Cette loi est précédée de quinze tentatives visant à créer un contrôle parlementaire sur ce type d'activités. Par conséquent, la volonté d'instaurer un contrôle parlementaire spécifique n'est pas une idée récente et reste antérieure à l'encadrement de la plupart des techniques de renseignement orchestré par la loi du 24 juillet 2015 (v. point 14).

Comme vu précédemment, les parlementaires jouent aussi un rôle dans le contrôle administratif mis en place avec la CNCTR, car pour rappel quatre parlementaires en font partie. Il en va de même pour la CNIL. Au-delà de conférer une légitimité démocratique à ces autorités administratives indépendantes, cela permet au Parlement d'être un acteur du contrôle. Or, cette intégration de parlementaires dans les organes de contrôle spécialisés ne doit pas amener à laisser de côté l'une des missions principales du Parlement qui est d'exercer un contrôle politique sur le gouvernement. Or, le présent chapitre se concentrera sur le contrôle parlementaire stricto sensu, et donc en grande partie sur le travail réalisé par la DPR.

112. ***Les missions de la DPR***. Les missions de cette délégation parlementaire ont évolué depuis sa création en 2007. La loi du 9 octobre 2007 vient modifier l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires en créant un article 6 nonies. Cet article correspond au régime de compétences et de fonctionnement de la DPR. Originellement, la loi de 2007 chargeait cet organe parlementaire « *de suivre l'activité générale et les moyens des services spécialisés à cet effet placés sous l'autorité des ministres chargés de la*

sécurité intérieure, de la défense, de l'économie et du budget ». Cette loi faisait donc entrer timidement le contrôle parlementaire des activités de renseignement dans l'ordonnancement juridique. Cependant, même si le rôle de la DPR s'avérait plus être un rôle d'information que de contrôle, cela a permis de rapprocher le Parlement de la communauté du renseignement.

La LPM pour 2014-2019[172] est venue modifier cet article, avec la volonté de conférer un rôle plus important à cette délégation. Elle vient modifier l'article 6 nonies en précisant que la DPR « *exerce le contrôle parlementaire de l'action du Gouvernement en matière de renseignement, évalue la politique publique en ce domaine et assure un suivi des enjeux d'actualité et des défis à venir qui s'y rapportent* ». Désormais, le texte associe la DPR à l'idée de contrôler l'action du gouvernement en matière de renseignement. Yaël Braun-Privet, présidente de la DPR d'avril 2018 à avril 2019, considère l'évolution apportée en 2013 comme une « *véritable mutation philosophique* »[173]. Certes, même si la loi autorise un contrôle de l'action gouvernementale, il semblerait que dans les faits cela ne soit pas encore le cas, mais aujourd'hui ce contrôle est possible.

La loi du 24 juillet 2015 a aussi modifié l'article 6 nonies. Elle élargit notamment le nombre de personnes pouvant être entendu par la délégation. Désormais, « *les directeurs en fonction des services mentionnés au I, accompagnés des collaborateurs de leur choix en fonction de l'ordre du jour de la délégation, ainsi que toute personne placée auprès de ces directeurs et occupant un emploi pourvu en conseil des ministres* » peuvent être auditionnés par cette dernière. Comme l'explique Yaël Braun-Privet, cet ajout permet de recevoir les cadres des services de renseignements sans que leur hiérarchie, c'est-à-dire le Premier ministre ou le ministre auquel est rattaché ce service, s'y oppose[174]. Jusque-là, la DPR pouvait, afin de réaliser les missions qui lui sont conférées, entendre le Premier ministre, les membres du Gouvernement et leur directeur de cabinet, le secrétaire général de la défense et de la sécurité nationale, le coordonnateur national du renseignement et de la lutte contre le terrorisme. De plus, elle peut aussi entendre le directeur de l'Académie du renseignement, les directeurs d'opérateurs de communications électroniques et les

---

[172] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
[173] Yaël Braun-Pivet, *Dix ans de contrôle parlementaire du renseignement : l'exigence démocratique est-elle satisfaite ?* dans *le droit du renseignement*, 2020, p. 141.
[174] *Ibid*., p. 142.

personnes mentionnées à l'article L34-1 du CPCE ainsi que les directeurs des autres administrations centrales ayant à connaître des activités des services de renseignement.

113. ***La spécificité du contrôle liée à celle des activités de renseignement***. Pour rappel, les contrôles s'afférent aux activités de renseignement sont contaminés par la spécialité de la matière dont ils ont la charge de contrôler. Pour éviter de porter atteinte à l'efficience des services de renseignement, le contrôle parlementaire, à la lumière des autres contrôles, est grevé de nombreuses spécificités.

La première spécificité renvoie à la composition de la DPR. D'une part, elle est composée uniquement de huit parlementaires (quatre sénateurs et quatre députés). Ce chiffre est très faible. À titre comparatif, la Délégation aux droits de la femme est composée de trente-six membres, soit quatre fois plus. Ce nombre réduit de parlementaires peut s'expliquer par la spécificité des missions à traiter. D'autre part, les parlementaires concernés sont habilités secret-défense, il en va de même pour les personnes qui les assistent. Cette habilitation est logique, car sans cette dernière les parlementaires ne pourraient pas réaliser les missions qui leur sont conférées. Cependant, leur habilitation connaît une limite. Les membres de la délégation ne peuvent pas connaître « *des données dont la communication pourrait mettre en péril l'anonymat, la sécurité ou la vie d'une personne relevant ou non des services intéressés, ainsi que les modes opératoires propres à l'acquisition du renseignement* ». Cette limitation est importante, car elle exclut le cœur d'activité des services de renseignement. Toujours dans cette idée de préservation de l'efficacité des services de renseignement, les travaux de la DPR sont couverts par le secret-défense.

De plus, le champ du contrôle de la DPR est restreint. Les méthodes opérationnelles, les opérations en cours ainsi que les coopérations internationales en matière de renseignement échappent à son contrôle. Encore une fois, cette disposition limite fortement l'impact du contrôle parlementaire. Cette restriction peut s'expliquer par la crainte de voir une atteinte porter au secret des opérations en cours, voire l'ajout d'une charge sur les agents de renseignement.

114. ***Les moyens de la DPR***. Les moyens dont la délégation dispose sont relativement classiques. Comme mentionné précédemment, la DPR peut entendre une multitude de personnalités interférant

directement ou indirectement avec les activités de renseignement. De plus, la DPR « *est destinataire des informations utiles à l'accomplissement »* de ses missions. Ces informations concernent notamment la « *stratégie nationale du renseignement* » (possible depuis la loi du 30 juillet 2021), « *des éléments d'information issus du plan national d'orientation du renseignement* », « *des éléments d'appréciation relatifs à l'activité générale et à l'organisation des services spécialisés* », « l*es observations que la Commission nationale de contrôle des techniques de renseignement adresse au Premier ministre* », les rapports de l'inspection des services de renseignement, etc. La DPR peut également saisir la CNCTR pour que cette dernière rende un avis sur une problématique donnée.

115. ***Le contrôle des fonds spéciaux***. La LPM pour 2014-2019 apporte une autre modification majeure aux missions de la délégation. Son article 13 vient faire absorber la commission de vérification des fonds spéciaux (CVSP) par la DPR en modifiant l'article 154 de la loi de finances pour 2002. Il dispose que désormais « *la commission de vérification constitue une formation spécialisée de la délégation parlementaire au renseignement* ». Ce rattachement fait suite aux préconisations des rapports de la DPR (2011 et 2012) et de la Commission des lois (2013). La LPM visée précise la composition de la CVSP. Elle est composée « *de deux députés et de deux sénateurs, membres de la délégation parlementaire au renseignement, désignés de manière à assurer une représentation pluraliste* »[175].

Cette commission, créée en 2002, a pour objet de contrôler l'usage des fonds spéciaux par les services de renseignement. Ces fonds spéciaux renvoient aux crédits alloués par le législateur au gouvernement pour le financement de « *missions secrètes* ». Par exemple, ces fonds spéciaux permettent aux services de renseignement de rémunérer une source. Ces fonds bénéficient d'un régime particulier dérogatoire au droit commun budgétaire. Le recours aux fonds spéciaux est encadré par un régime juridique extrêmement strict, car il s'agit de donner de l'argent public aux services de renseignement. Il est donc normal que ce contrôle existe. La commission rend un

[175] Cette précision vient mettre fin à un différend entre la Cour des comptes et le Parlement. En effet, à l'origine cette commission devait être composée de parlementaires et de magistrats de la Cour des comptes. Or, cette dernière a refusé que des magistrats siègent au sein de cette commission.

rapport annuel (non public) sur le recours à ces fonds à la DPR. Le montant des dépenses de crédits alloués aux fonds spéciaux était d'environ 86 millions d'euros en 2018[176].

116. ***Remarques sur le contrôle actuel exercé par la DPR***. Même si la DPR se voit conférer de plus en plus de missions, elle semble souffrir d'un manque de moyens. Comme l'explique Yaël Braun-Pivet, ces moyens demeurent trop limités pour « *permettre à la DPR d'exercer la plénitude de ses prérogatives* ». En d'autres termes, les textes permettent la mise en place d'un réel contrôle de la politique publique du renseignement, mais dans les faits ce contrôle n'est pas réalisé. Comme l'explique le Professeur Bertrand Warusfel[177], il serait souhaitable que la DPR passe d'un contrôle des moyens à un contrôle des activités de renseignement dans leur ensemble. En effet, à la lecture des rapports rendus annuellement par la DPR, elle semble davantage se concentrer sur les moyens dont sont dotés les services de renseignement, plutôt que de contrôler la tenue et l'orientation par le gouvernement des services de renseignement. Surtout que depuis la loi du 30 juillet 2021, la délégation peut auditionner le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT) pour que ce dernier lui présente le plan national d'orientation du renseignement. Après avoir présenté la teneur du contrôle actuel réalisé par la DPR, il paraît intéressant de comparer le contrôle parlementaire français des activités de renseignement avec ce qui se fait dans les autres États européens ou plus généralement occidentaux.

Paragraphe 2 : Le contrôle parlementaire français par rapport à ses homologues

117. ***Rappel***. Le cas français se distingue par la mise en place tardive d'un contrôle parlementaire sur les activités de renseignement (même constat que pour l'encadrement juridique). À titre de comparaison, les Pays-Bas ont mis en place, dès 1952, un contrôle parlementaire avec une commission dédiée aux services de renseignement et de sécurité. L'objectif ici sera de savoir si les États occidentaux réalisent un contrôle parlementaire plus complet et intrusif des activités de renseignement.

---

[176] Projet de loi de finances pour 2020 : Direction de l'action du Gouvernement : Coordination du travail gouvernemental, Avis n° 142 (2019-2020), tome IX, déposé le 21 novembre 2019 (https://www.senat.fr/rap/a19-142-9/a19-142-912.html#toc170).

[177] Bertrand Warusfel, *Quelles réformes pour le droit du renseignement ?* intervention au 8ème colloque annuel de l'Association française de droit de la sécurité et de la défense, Université Lyon 3, 25 septembre 2020.

118. ***Le cas étasunien : un exemple ?*** Dès la création de la CIA en 1947, l'idée d'allier renseignement et contrôle démocratique est née. Les deux chambres parlementaires jouissent d'une commission permanente afin de contrôler les activités de renseignement. Pour le Sénat, c'est la *United States Senate Select Committee on Intelligence* (SSCI)[178] qui réalise ce contrôle. Pour la Chambre des représentants, ce contrôle est exercé par la *United States House Permanent Select Committee on Intelligence* (HPSCI)[179].

Le champ d'intervention de ces deux commissions permanentes concerne tout ce qui a trait aux activités de renseignement. Première différence avec le contrôle parlementaire français, les membres de ces deux commissions peuvent connaître des opérations en cours. Elles peuvent donc décider d'enquêter et d'entendre les acteurs du renseignement même concernant une opération en cours[180]. Dans leurs missions, les commissions étasuniennes ont accès à toutes les informations possibles, même les plus sensibles. Les informations auxquels elles ont accès peuvent être utilisées discrétionnairement par les commissions tant que cette utilisation ne contrevient pas à la sécurité nationale ou à la sécurité des personnels concernés. De plus, la loi oblige les services à fournir toute information/preuve à ces commissions. En revanche, avant la publication d'informations sensibles, un échange a lieu entre le pouvoir exécutif et les membres de la commission pour savoir si les éléments susceptibles d'être publiés porteraient potentiellement atteinte à la sécurité nationale. De plus, les règles de confidentialité entourant les travaux des commissions sont très strictes. Sur ce point, là encore, les parlementaires étasuniens se distinguent par de larges prérogatives.

Le cas étasunien est donc un exemple de jusqu'où peut aller l'instauration d'un contrôle politique par une commission parlementaire. Cependant, pour en arriver jusqu'ici, l'évolution a été progressive. C'est pourquoi le contrôle parlementaire étasunien pourrait être un objectif à atteindre à long terme. Comme l'explique le député Arthur Paecht, le cas étasunien peut être un « *modèle de contrôle parlementaire pour les uns* » ou une « *machine de harcèlement de services pour les*

[178] Créée en 1976.
[179] Créée en 1977.
[180] Assemblée nationale, rapport n°1 951 tendant à la création d'une délégation parlementaire pour les affaires de renseignement, M. Arthur PAECHT, 23 novembre 1999, p. 20.

autres »[181]. Il n'en demeure pas moins que ce contrôle parlementaire poussé n'a pas empêché les États-Unis de développer des services de renseignement très performants.

119. ***L'Allemagne : un autre exemple de contrôle parlementaire fort sur les activités de renseignement***. D'autres États ont décidé de se doter d'un contrôle parlementaire fort, c'est le cas de la République fédérale d'Allemagne par exemple. Dès 1956, un organe parlementaire fut créé : le *parlementarisches Vertrauensmännergrenium.* Son rôle était de surveiller les trois grands services de renseignement fédéraux, à savoir le BND (*Bundesnachrrichtendienst*), le *Bundesamt für Verfassungsschutz* (équivalent de la DGSI) et le *militärisher Abschirmdienst* (équivalent de la DRM). Face à des problèmes d'ordre politique, cet organe fut remplacé en 1979 par une commission parlementaire dénommée *parlamentarische Kontrollkommission*. Cependant, cette commission de contrôle ne dispose pas d'un monopole sur le contrôle politique des activités de renseignement puisque le *Bundestag* garde des compétences de contrôle. Cette commission parlementaire de contrôle est chargée de veiller au respect des droits de chaque citoyen allemand par les services de renseignement.

Concernant les prérogatives de cette commission parlementaire de contrôle, cette dernière peut obliger les services de renseignement à donner toute information nécessaire à son contrôle. Les services peuvent exceptionnellement refuser de donner certaines informations (motivation exigée), mais un vote de la commission avec une majorité de deux tiers peut faire lever ce refus. Là encore, sur ce point, la DPR dispose d'un accès aux informations beaucoup plus restreint délimité par l'article 6 nonies de l'ordonnance de 1958. Plus classiquement, la *parlamentarische Kontrollkommission* peut aussi procéder aux auditions des acteurs du renseignement. Enfin, elle peut aussi procéder à des contrôles sur pièces et sur place. Sur ce dernier point, là encore le cas allemand se distingue du cas français, dans le sens où les membres de la DPR ne peuvent pas réaliser des contrôles sur pièces et sur place (mais peut uniquement faire des visites).

Là encore, le contrôle parlementaire mis en place par l'Allemagne offre plus de prérogatives aux parlementaires chargés de ce contrôle. Cependant, encore une fois, le contrôle parlementaire allemand est ancien et a pu être amélioré progressivement.

---

[181] *Ibid.,* p. 17.

120. ***Le contrôle parlementaire dans d'autres États***. Les États n'ont pas tous choisi un modèle dans lequel le contrôle parlementaire des activités de renseignement est poussé comme en Allemagne ou aux États-Unis. Certains États ont opté pour un contrôle parlementaire limité des activités de renseignement tandis que d'autres ont mis en place des contrôles parlementaires plus spécifiques.

Par exemple, la Belgique a fait un choix plutôt original. Comme vu précédemment, la Belgique est dotée de deux organes de contrôle des activités de renseignement : d'une part, le « *Comité R* » (chargé d'un contrôle général), d'autre part, la commission[182] (chargée d'autoriser le recours aux techniques spéciales). La particularité du système belge est qu'il n'existe pas directement de contrôle parlementaire sur les activités de renseignement. En effet, il existe une commission sénatoriale, pas chargée de contrôler les services de renseignement belge, mais dont le rôle est de contrôler le « *Comité R* ». Comme l'explique Floran Vadillo, l'absence de contrôle direct correspond « *à une pratique institutionnelle, car, sans que la Constitution belge ne le précise, la coutume veut que le législateur n'exerce pas de contrôle direct sur les administrations, mais passe par l'entremise des ministres* »[183]. Il n'en demeure pas moins que l'idée de contrôler les organes de contrôle paraît intéressante dans le cadre des activités de renseignement, mais ce cas ne pourrait pas être retranscrit au cas français pour des raisons qui seront présentées plus tard.

En Italie, comme précisé précédemment, la COPASIR (organe parlementaire) est le seul organe qui contrôle les activités de renseignement. Cependant, elle dispose de prérogatives faibles, visant uniquement à une possibilité d'auditionner les acteurs du renseignement et de demander la réalisation d'enquêtes internes au Président du Conseil des ministres.

Au Royaume-Uni, *The Inteligence service Act* de 1994 crée *The Intelligence and Security Committee of Parliament* (ISC). Cette commission parlementaire, composée de neuf parlementaires, a pour mission de contrôler les activités de renseignement. Malgré un renforcement

[182] Nommée la Commission chargée du suivi parlementaire du Comité permanent de contrôle des services de renseignements et de sécurité (Comité permanent R).
[183] Floran Vadillo, *Originalités du modèle belge de contrôle des services de renseignement*, dans Les cahiers de la sécurité, n°25, septembre 2013, p. 127-132.

des prérogatives de cette commission par the *Justice and Security Act* de 2013, le contrôle exercé reste timide. Ce régime se rapproche du cas français pour plusieurs raisons. D'une part, il se démarque par son caractère récent. D'autre part, à la lumière du cas français, cette commission parlementaire fut créée alors que les activités de renseignement n'étaient pas encadrées.

121. ***Remarques générales***. Le contrôle limité exercé par la DPR sur les activités de renseignement n'est pas une particularité, puisque d'autres États exercent un contrôle parlementaire limité, c'est le cas par exemple du Royaume-Uni (ou même des Pays-Bas). En revanche, d'autres États ont mis en place de manière progressive un contrôle parlementaire complet des activités de renseignement.

Même si comme le précise Yaël Braun-Privet, « *en matière de contrôle parlementaire, comparaison n'est pas raison : on ne saurait transposer en France des mécanismes de contrôle parlementaire en vigueur dans des pays où les équilibres institutionnels sont très éloignés des nôtres, comme aux États-Unis* »[184]. Cependant, ce constat ne doit pas empêcher de s'inspirer de l'idée générale des contrôles complets mis en place dans les pays précités, car un contrôle parlementaire fort est synonyme d'une démocratie forte. D'autant plus qu'aux États-Unis, régime présidentialiste par excellence, bien que le pouvoir exécutif prime très souvent, l'exemple d'un contrôle parlementaire fort sur cette primauté devrait inspirer. Désormais, il paraît nécessaire de démontrer que l'impact du Parlement français, notamment par l'intermédiaire de la DPR, doit s'accroître.

[184] Yaël Braun-Pivet, *Dix ans de contrôle parlementaire du renseignement : l'exigence démocratique est-elle satisfaite ?* dans *le droit du renseignement*, 2019, p. 144.

<u>Section 2</u> : La nécessité d'augmenter le contrôle parlementaire

122. ***Annonce***. Après avoir fait cet état des lieux de la teneur du contrôle parlementaire français sur les activités de renseignement puis de l'avoir comparé à ses homologues, il est temps d'expliquer pour quelles raisons le contrôle parlementaire doit passer d'un contrôle limité à un contrôle complet (***paragraphe 1***). Après avoir expliqué ces raisons, il sera désormais temps d'émettre certaines pistes d'amélioration de ce contrôle (***paragraphe 2***).

<u>Paragraphe 1 : Les raisons fondant cette nécessité d'accroissement</u>

123. ***Rappels***. Le contrôle parlementaire n'est pas uniquement propre aux activités de renseignement, autrement dit, il s'insère dans un contexte institutionnel plus vaste : celui de la Vème République. Plusieurs raisons seront donc évoquées, une liée directement au régime juridique encadrant les activités de renseignement, et d'autres plus liées au contexte institutionnel et politique traversé par la société française.

124. ***Le contrôle parlementaire : un contrôle complet rendu nécessaire en raison du champ d'application du livre VIII***. Le livre VIII, introduit dans le CSI par la loi du 24 juillet 2015, couvre un panel, certes large, mais non exhaustif des techniques de renseignement utilisées par les services. Pour rappel, ce livre n'a vocation qu'à encadrer les techniques de renseignement, jugées par le législateur, les plus liberticides. En d'autres termes, certaines activités des services de renseignement ne sont pas soumises au régime instauré par le livre VIII. Par conséquent, l'ensemble du travail réalisé en source ouverte n'est pas soumis à ce livre. Il en va de même pour toutes les activités visant à recourir à des sources humaines. D'autant plus que concernant ces dernières, la CNCTR, pour le moment, n'a pas accès aux informations qui pourraient amener à identifier une source humaine d'un des services[185]. Par exemple, les services de renseignement ne sont pas soumis au livre VIII lorsqu'ils réalisent des filatures ou traitent avec une source humaine.

[185] Refus fondé sur l'article L833-2 du CSI. Ce dernier motive le refus de donner accès aux renseignements issus des services étrangers ou aux fichiers intéressants la sûreté de l'État.

Enfin, s'ajoute à cela l'absence de contrôle, par la CNCTR, sur les renseignements issus des services étrangers[186].

Par conséquent, l'absence de contrôle réalisé par les organes instaurés par la loi du 24 juillet 2015 sur l'ensemble des activités de renseignement laisse un vide. Même si, le livre VIII concerne les techniques jugées les plus liberticides, certaines techniques non saisies par ledit livre peuvent amener à violer les libertés des individus concernés[187]. Par exemple, un usage disproportionné des moyens[188] pour obtenir une source humaine pourrait attenter aux libertés de l'individu concerné. Cet espace non contrôlé rend le rôle du contrôle parlementaire primordial. En effet, la DPR, contrairement à la CNCTR, n'est pas limitée par le livre VIII, car elle a pour mission d'exercer « *le contrôle parlementaire de l'action du Gouvernement en matière de renseignement* »[189]. Ce champ de compétence plus large offert à la DPR doit être utilisé pour se concentrer sur les activités non saisies par le livre VIII. Par exemple, la délégation pourrait veiller au respect des règles éthiques grâce aux rapports rendus par les inspections du renseignement et par l'inspection générale du renseignement (auxquels la DPR a accès).

La CNCTR et la DPR doivent donc opérer des contrôles complémentaires. La première réalise un contrôle juridique, technique et relativement complet sur les procédés les plus liberticides, alors que la seconde devrait réaliser un contrôle politique large, notamment sur l'orientation des services de renseignement par le gouvernement.

125. ***Le contrôle parlementaire : un garde de fou face à la sécurisation globale.*** Les questions concernant l'efficacité des contrôles assujettis aux activités de renseignement s'inscrivent dans un mouvement de sécurisation globale de la société française. De nombreux exemples peuvent venir étayer ce constat : l'inflation normative autour de la notion de sécurité, la pérennisation dans le droit commun de mesures exceptionnelles, les dernières années marquées par les états d'urgence

---

[186] V. point 89.
[187] Cheminement du recrutement des sources humaines présentées par la DGSI (https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/contre-espionnage/processus-de-recrutement-dune-source-humaine).
[188] Et ce par rapport à la finalité à protéger.
[189] Article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

successifs, les débats actuels autour de la reconnaissance faciale, etc. L'adaptation du droit aux menaces actuelles est nécessaire, cependant, cette adaptation doit rester cloisonner par les grands principes forgeant la démocratie et l'État de droit français. Ce mouvement de sécurisation est parfaitement illustré par l'accroissement des moyens et des prérogatives dont sont dotés les services de renseignement. Par exemple, entre 2015 et 2019, le nombre des effectifs affectés dans les services de renseignement a augmenté de 22,1 % pour un total de 20 168 agents en 2019[190]. Le budget alloué aux services de renseignement suit exactement la même courbe que celle de l'évolution des effectifs.

Le contrôle parlementaire sur les services de renseignement doit donc être regardé comme un garde-fou à une sécurisation trop importante de la société française. Il est normal, face aux menaces rencontrées par la France, que les moyens humains et budgétaires des services augmentent, cependant, cette augmentation légitime doit être suivie par un contrôle important. La DPR doit donc se concentrer sur quelles finalités vont être orientés les services de renseignement. Elle doit aussi veiller à ce que les directives gouvernementales reçues par les services de renseignement soient conformes aux finalités fixées. En effet, sous le régime de l'état d'urgence, des recours abusifs aux moyens offerts par le droit ont pu être remarqués. Les moyens exceptionnels mis en place dans le cadre de la lutte contre le terrorisme ont malheureusement été utilisés pour « *neutraliser* » certains militants écologistes (ici, la légalité des mesures questionne notamment sur un éventuel détournement de procédure)[191]. C'est pour éviter des détournements du type que la DPR doit réaliser un contrôle politique fort sur les activés de renseignement, elle doit veiller à ce que les prérogatives des services de renseignement ne soient pas détournées par le gouvernement pour des finalités ne justifiant par leurs actions (proportionnalité, nécessité et protection des intérêts fondamentaux de la Nation).

126. ***Le contrôle parlementaire : un contrôle devenu substantiel avec le phénomène de présidentialisation.*** La dernière raison justifiant un contrôle parlementaire complet sur les activités

[190] Ce chiffre comptabilise les agents du 1er et du 2nd cercle (14 512 sont affectés aux services de la communauté du renseignement). V. *6 ans après le 13 novembre, quelle évolution des services de renseignement ? Trois questions à Benjamin Oudet*, Institut Montaigne, 22 octobre 2021.
[191] Le point, *COP21 : dérive de l'état d'urgence contre les militants écolos* ? 28 novembre 2015. V. notamment Le Monde, *Les militants de la COP21, cibles de l'état d'urgence*, 27 novembre 2015.

de renseignement s'inscrit dans un contexte institutionnel défavorable aux prérogatives du Parlement. Le phénomène de rationalisation subi par le Parlement dès 1958 couplé à l'avènement du fait majoritaire a modifié le rôle intrinsèque du Parlement. Ce dernier n'est plus le principal acteur de la fonction législative, dans le sens où avec l'avènement du fait majoritaire, il coopère constamment avec le pouvoir exécutif. L'activité de contrôle du gouvernement a gagné en importance. Cette activité de contrôle doit être complète et concerner l'ensemble des activités dont le gouvernement a la charge. Instaurer un contrôle complet dans le cadre des activités de renseignement serait une preuve que le pouvoir exécutif reste contrôlé par les représentants de la Nation (notamment l'opposition), et ce même dans la direction des activités les plus régaliennes.

127. ***Remarques générales***. Les raisons de l'instauration d'un contrôle parlementaire fort et complet sont nombreuses. Un contrôle parlementaire fort est le signe d'un bon équilibre entre les pouvoirs. Pour rappel, le contrôle actuel ne peut pas être qualifié de complet, et ce malgré les évolutions opérées notamment par la LPM pour 2014 à 2019. Pour étayer ce propos, il paraît important de citer une proposition de loi déposée en 2018 par des sénateurs visant à *« renforcer le contrôle parlementaire du renseignement »*[192]. Ces rédacteurs précisent que malgré **«** *les évolutions apportées par la loi de programmation militaire de 2013, le contrôle parlementaire du renseignement en France demeure en effet bien en deçà des dispositifs mis en place par d'autres démocraties »*[193]. Cette proposition de loi n'est malheureusement pas allée plus loin qu'une première lecture devant le Sénat. Or, elle montre que certains parlementaires œuvrent pour voir l'instauration en France d'un contrôle parlementaire fort. Il paraît donc intéressant de proposer quelques orientations que pourrait prendre le contrôle parlementaire, et ce pour atteindre un contrôle complet.

[192] Proposition de loi *tendant à renforcer le contrôle parlementaire du renseignement,* présentée par M. Philippe Bas, M. Christian Cambon, M. François-Noël Buffet, M. Marc-Philippe Daubresse et Mme Martine Berthet, enregistrée à la Présidence du Sénat le 11 mai 2018.
[193] *Ibid*.

Paragraphe 2 : Les pistes d'évolution du contrôle parlementaire

128. Le Contrôle parlementaire devrait être amené à évoluer dans les prochaines années. En effet, plusieurs nouveaux acquis devraient être amenés dans la lignée des évolutions faites par la LPM pour 2014 à 2019 ou la loi du 30 juillet 2021. La volonté de certains parlementaires de se rapprocher des démocraties exemplaires sur ce point devrait pousser la mise en place de ces modifications. D'autant plus que ces évolutions s'inscriraient dans une ambiance favorable, car la DPR est parvenue à tisser de bonnes relations avec les services de renseignement. Comme l'explique la proposition de loi sénatoriale précédemment évoquée, « *ce contexte de travail favorable ne doit toutefois pas se faire au détriment de l'exercice d'un contrôle objectif, plein et entier de l'activité des services, d'autant plus nécessaire que ces derniers ont été, au gré des récentes évolutions législatives et dans le cadre d'un contexte de menace terroriste élevée et durable, considérablement renforcés au cours des dernières années* »[194].

129. ***La nécessaire augmentation des moyens de la DPR***. Pour rappel, Yaël Braun-Pivet, ancienne présidente de la délégation, mentionne que les moyens dont dispose la DPR restent trop limités pour lui « *permettre »* (…) *« d'exercer la plénitude de ses prérogatives* »[195]. Concernant les moyens humains, la délégation est dotée de peu de membres. L'évolution du nombre de membres n'est pas forcément la solution idéale pour accroître les moyens humains de la délégation, car les parlementaires ont un emploi du temps chargé. En revanche, le nombre de personnes assistants les membres de la délégation pourrait être augmenté, ce qui permettrait d'accroitre les capacités de contrôle de la DPR. Bien évidemment, lesdits assistants feraient l'objet d'une enquête lors de leur habilitation, ce qui limiterait au maximum les risques de fuite d'information classifiée.

130. ***Une augmentation des prérogatives dans la lignée de la loi du 30 juillet 2021***. Cette loi est venue modifier l'article 6 nonies de l'ordonnance de 1958 relative au fonctionnement des assemblées parlementaires. Elle vient ajouter à cet article que : « *la délégation peut, dans la limite de son besoin d'en connaître, solliciter du Premier ministre la communication de tout ou partie des*

[194] *Ibid*., p. 3.
[195] Yaël Braun-Pivet, *Dix ans de contrôle parlementaire du renseignement : l'exigence démocratique est-elle satisfait ?*, dans *le droit du renseignement*, 2020, p. 141.

rapports mentionnés au 7° du présent I ainsi que de tout autre document, information et élément d'appréciation nécessaire à l'accomplissement de sa mission »[196]. Ce nouvel apport permet donc désormais à la délégation de demander, au Premier ministre, toute information jugée nécessaire à la réalisation de sa mission. Cependant, cette prérogative est grandement limitée, car pour rappel, la DPR ne peut pas être informée d'éléments portant sur les opérations en cours ou « *sur les instructions données par les pouvoirs publics à cet égard », « sur les procédures et méthodes opérationnelles »* ou encore *« sur les échanges avec des services étrangers* ». En d'autres termes, l'ajout mis en place par la loi de 2021 est presque vidé de sa portée, car il cantonne la DPR a un travail d'enquête a posteriori en lui permettant de demander des informations uniquement sur les opérations terminées et celles qui ne concernent ni les méthodes opérationnelles, ni les renseignements donnés par les services étrangers.

Par conséquent, l'une des pistes possibles seraient de supprimer ces limitations à la prérogative de demander des informations au Premier ministre. Bien sûr cette augmentation des prérogatives parlementaires serait suivie de limitations pour éviter que les activités de renseignement et leur efficacité soient mises en péril. La proposition de loi déposée en 2018 par les sénateurs parmi lesquels faisait partie Philippe Bas (ancien conseiller d'État) souhaitait une évolution dans ce sens. En effet, elle prévoyait de modifier l'ordonnance précitée en lui ajoutant les mots suivants : la DPR « *peut solliciter tout document, information ou élément d'appréciation nécessaire à l'accomplissement de sa mission. Lorsque la transmission d'un document, d'une information ou d'un élément d'appréciation est soit susceptible de mettre en péril le déroulement d'une opération en cours ou l'anonymat, la sécurité ou la vie d'un agent relevant d'un service spécialisé de renseignement » (...) « ou d'un service autorisé par le décret en Conseil d'État mentionné » (...) « soit concerne les échanges avec les services étrangers ou avec les organismes internationaux compétents dans le domaine du renseignement, le Premier ministre ou les ministres de tutelle des services mentionnés au présent alinéa peuvent, par une décision motivée, s'opposer à sa communication* »[197]. Cette proposition semblait être adaptée à l'idée développée. Cependant,

[196] Article 21 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

[197] Alinéa 3 de l'article 1er de la proposition de loi *tendant à renforcer le contrôle parlementaire du renseignement,* présentée par M. Philippe Bas, M. Christian Cambon, M. François-Noël Buffet, M. Marc-Philippe Daubresse et Mme Martine Berthet, enregistrée à la Présidence du Sénat le 11 mai 2018.

il serait préférable d'enlever à cette proposition l'exception liée aux renseignements fournis par les services étrangers, et donc de garder que la première (celle liée à la mise en péril de l'opération ou de la vie des agents). Modifier en ce sens l'article 6 nonies de ladite ordonnance amènerait plusieurs avantages.

D'une part, une modification du type permettrait de donner les prérogatives nécessaires pour que le Parlement, par l'action de la DPR, réalise un contrôle complet. D'autre part, cela permettrait enfin un contrôle sur les renseignements fournis par les services étrangers, point, qui pour rappel, n'est encore pas réglé et qui expose la France à une probable condamnation de la Cour EDH. Enfin, permettre l'accès de la DPR à des informations relatives à une opération en cours, lui permettrait de jouer un rôle actif dans son contrôle et donc, de ne pas attendre la fin d'une opération qui peut durer des années. Une telle modification rapprocherait la France des démocraties dotées d'un contrôle parlementaire efficace et complet sur les activités de renseignement, tout en respectant les deux principes directeurs : le respect des droits et libertés et l'efficacité des services de renseignement.

131. ***L'élargissement des personnes pouvant être auditionnées***. Même si la liste des personnes pouvant être auditionnées a été élargie lors des dernières modifications législatives, cette dernière reste encore perfectible. L'une des possibilités serait de permettre à la DPR d'auditionner un panel plus large de personnes pouvant aller jusqu'à l'ensemble des agents des services de renseignement. Cependant, même si cette modification serait un apport considérable pour la délégation, elle pourrait mener à des craintes d'une intrusion trop importante du Parlement dans les activités de renseignement. La proposition de loi précédemment citée souhaitait permettre à la délégation d'auditionner l'ensemble des agents de renseignement uniquement lorsqu'elle se rendait sur site[198]. Cette limitation du pouvoir d'audition au cas où les membres de la délégation se trouve sur place pourrait être qualifiée de sage dans le sens où le nombre d'audition d'agent serait limité, et s'apparenterait le plus souvent à des échanges.

[198] *Ibid*., « *Lorsqu'elle se rend sur le site de l'un des services mentionnés au même I, la délégation peut entendre tout personnel placé auprès de ce service* ».

132. ***Remarques générales*****.** Certes, le contrôle parlementaire mis en place en 2007 n'est pas encore qualifiable de complet (ou d'entier). Mais, l'évolution depuis sa création montre que la tendance va vers un renforcement des prérogatives parlementaires dans le contrôle des activités de renseignement. Les pistes d'amélioration de ce contrôle sont diverses, et plusieurs parlementaires sont porteur d'idées. L'instauration d'un contrôle parlementaire fort dépendra bien évidemment du contexte politique et de la capacité du Parlement à s'affirmer comme un véritable contrepouvoir (notamment pour l'opposition). Il ne faut pas oublier qu'un Parlement fort (que cela soit par son contrôle sur le pouvoir exécutif ou par son pouvoir de légiférer) est un marqueur d'une démocratie en bonne santé.

CONCLUSION GÉNÉRALE

L'entrée en vigueur de la loi du 24 juillet 2015 réalise un réel bouleversement dans la conception des activités de renseignement. Pour autant, malgré cette avancée pour l'État de droit, de nombreuses failles existaient, et ce notamment dans les contrôles mis en place. Comme il a été vu dans le premier titre de ce mémoire, certaines failles ont été résorbées par le législateur français, qui fut contrait à agir sous l'impulsion des juges européens.

Cependant, trois problématiques non négligeables demeurent. La première concerne le contrôle a posteriori, tant dans les moyens mis en œuvre que dans le champ d'application du contrôle réalisé par la CNCTR. La seconde concerne l'efficacité du contrôle politique mis en place sur les activités de renseignement. La dernière renvoie à la procédure contentieuse retenue devant la formation spécialisée du Conseil d'État. Le droit français, en ce qui concerne le contrôle des activités de renseignement, doit encore évoluer dans le but de mettre en place un contrôle optimal visant à limiter les risques de dérives sécuritaires (notamment de surveillance de masse) et empêcher les services d'être détournés de leur rôle naturel. Les solutions à la résolution des problématiques exposées ne manquent pas et doivent être mises en place tout en préservant l'efficacité des services de renseignement. C'est pourquoi ces derniers doivent être acteurs des évolutions à venir, afin de trouver un équilibre dans l'effectivité de leurs actions et la protection des droits et libertés de l'ensemble des administrés.

Par conséquent, le droit actuel doit évoluer pour combler ses lacunes. Il serait intéressant de voir le législateur intervenir rapidement avant une condamnation, qui pourrait arriver très prochainement, de l'État français par la Cour EDH. Cependant, cette action du législateur reste très peu probable, et il réagira comme souvent après une condamnation de la France par les juges de Strasbourg.

Plus largement, le contrôle des activités de renseignement s'inscrit dans un contexte où les moyens conférés aux services visant à préserver l'ordre public et la sécurité nationale sont augmentés de façon accrue. À ce phénomène s'ajoute les avancées technologiques qui permettent une surveillance généralisée de la population, tant en passant par le recours aux algorithmes de

surveillance dans une société de plus en plus numérisée que par la reconnaissance faciale. Il est temps de définir les limites à amener à ces évolutions. L'instauration d'un contrôle complet sur les activités de renseignement semble être une limite plus que nécessaire, pour éviter de mettre le doigt dans un engrenage qui amènerait notre société, basée sur l'État de droit et le respect des droits fondamentaux, dans une issue trop sécuritaire. Les évolutions évoquées dans ce travail permettraient de mettre en place en place les garde-fous nécessaires, tout en garantissant l'efficacité des services de renseignement, qui pour rappel sont essentiels à la protection de la sécurité nationale.

BIBLIOGRAPHIE

Les documents ont été classés dans l'ordre suivant :

I - Sources normatives

II - Sources doctrinales

III - Presse

I - Sources normatives

1. *Textes*

a. Textes français

Livre VIII du Code de la sécurité intérieure.

Articles L773-1 à L773-8 du CJA.

Ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

Décret n° 2021-1361 du 20 octobre 2021 relatif aux catégories de données conservées par les opérateurs de communications électroniques, pris en application de l'article L. 34-1 du CPCE.

Décret n° 2014-833 du 24 juillet 2014 relatif à l'inspection des services de renseignement.

b. Textes européens

Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Charte des droits fondamentaux.

2. Jurisprudences

a. Conseil d'État

Conseil d'État, assemblée, 8 février 2007, Société Arcelor, n°287110, publié au recueil Lebon.

Conseil d'État, 16 avril 2010, n° 320196 (concernant le fichier CRISTINA).

Conseil d'État, Formation spécialisée, 08/11/2017, 396549.

Conseil d'État, assemblée, 21 avril 2021, French Data Network, n°393099, publié au recueil Lebon.

Conseil d'État, Formation spécialisée, 04/02/2022, 449791, inédit au recueil Lebon.

b . Conseil constitutionnel

Décision du 2 mars 2004 (n° 2004-492 DC).

Décision du 23 juillet 2015 (n° 2015-713 DC).

Décision du 24 juillet 2015, Association French Data Network et autres (n° 2015-478 QPC).

c. Cour de justice

CJUE, 18 juillet 2013, *Kadi II.*

CJUE, 16 décembre 2016, *Tele2 Sverige.*

CJUE, 6 octobre 2020, *Quadrature du Net.*

CJUE, 5 avril 2022, *Dwyer.*

d. Cour européenne des droits de l'homme

Cour EDH, *Klass et autres contre Allemagne*, 6 septembre 1978.

Cour EDH, *Leander contre Suède*, 26 mars 1987.

Cour EDH, *Kruslin et Huvig contre France*, 24 avril 1990.

Cour EDH, *Liberty et autres contre Royaume-Uni*, 1er juillet 2008.

Cour EDH, *Big Brother watch contre Royaume-Uni*, 25 mai 2021.

Cour EDH, *Centrum för rättvisa contre Suède*, 25 mai 2021.

3. *Travaux préparatoires, rapports et actes de droit souple*

Assemblée nationale, rapport n°1 951 tendant à la création d'une délégation parlementaire pour les affaires de renseignement, M. Arthur PAECHT, 23 novembre 1999.

Proposition de loi relative au Secret-défense, texte n° 23 (2004-2005) de M. Michel DREYFUS-SCHMIDT et les membres du groupe socialiste et apparentés, déposé au Sénat le 13 octobre 2004.

Livre blanc sur la défense et la sécurité, 2008.

CNCTR, délibération du 12 novembre 2015, n°02-2015.

Rapport de la DPR, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017.

Proposition de loi tendant à renforcer le contrôle parlementaire du renseignement, présentée par M. Philippe Bas, M. Christian Cambon, M. François-Noël Buffet, M. Marc-Philippe Daubresse et Mme Martine Berthet, enregistrée à la Présidence du Sénat le 11 mai 2018.

CNCTR, 6ème Rapport d'activité pour l'année 2021.

Rapport de la DPR relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021.

CNIL, Délibération n°2021-040 du 8 avril 2021portant avis sur un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

Avis du Conseil d'État du 12 mai 2021 sur une lettre rectificative au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

Investigatory Powers Commissioner's Annual Report 2021 (Royaume-Uni).

II - Sources doctrinales

1. *Ouvrages, manuels, thèses*

Sherman Kent, « Strategic intelligence for American World Policy », *Princeton University Press*, 1949.

Alexis Deprau**, «** Renseignement public et sécurité nationale », Université Panthéon-Assas, 2017 (thèse).

Olivier Forcade et Bertrand Warusfel, « Le droit du renseignement », *La documentation française*, 2019.

Guilhem Marois, « Le contrôle des services de renseignement en France *»,* Université de Bordeaux, 2019 (thèse).

Alexis Deprau, « Le contrôle parlementaire du renseignement », Berger Levrault, 2022.

2. *Articles*

Floran Vadillo, « Originalités du modèle belge de contrôle des services de renseignement *», Les cahiers de la sécurité*, n°25, septembre 2013, p. 127-132.

Olivier de Maison Rouge, « Le renseignement sous l'oeil du juge *»*, *Dalloz IP/IT*, décembre 2018.

Bertrand Warusfel, « Acquis et limites de l'encadrement : premier bilan d'étape de la réforme *»*, 28 octobre 2018.

Bertrand Warusfel, « Quelques réformes pour le droit du renseignement *»*, *8ème Colloque de l'AFDSD*, 2020.

Institut Montaigne, « 6 ans après le 13 novembre, quelle évolution des services de renseignement ? Trois questions à Benjamin Oudet », 22 octobre 2021.

Bertrand Warusfel, « Droit du renseignement : entre imperfections et avancées », sur le blog *Chemins publics*, mars 2022.

III - Presse

Le Monde, « Les principaux condamnés au procès des écoutes de l'Élysée se pourvoient en cassation », 27 mars 2007.

Le Monde, « Révélations Snowden, un séisme planétaire », 21 octobre 2013.

Le Monde, « Les militants de la COP21, cibles de l'état d'urgence », 27 novembre 2015.

Le point, « COP21 : dérive de l'état d'urgence contre les militants écolos ? », 28 novembre 2015.

Le Monde, « La justice de l'UE s'oppose à la collecte massive des données de connexions Internet et téléphoniques par les États », 6 octobre 2020.

IV - Ressources électroniques

Le renseignement au service de l'enquête : retour sur la conférence du 21 mai 2019 (https://www.ihemi.fr/articles/le-renseignement-au-service-de-lenquete-retour-sur-la-conference-du-21-mai-2019).

Site internet du Comité permanent de contrôle des services de renseignement et de sécurité (https://www.comiteri.be/index.php/fr/comite-permanent-r).

Site internet du gouvernement concernant le GIC (https://www.gouvernement.fr/groupement-interministeriel-de-controle-gic).

Site internet de la DGSI (https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents/fichier-de).

Site internet du ministère de la Justice canadienne (https://www.justice.gc.ca/fra/fina-fund/sjp-jsp/es- sa.html).

Page internet du Conseil d'État concernant la conservation des données (https://www.conseil-etat.fr/actualites/donnees-de-connexion-le-conseil-d-etat-concilie-le-respect-du-droit-de-l-union-europeenne-et-l-efficacite-de-la-lutte-contre-le-terrorisme-et-la').

TABLE DES MATIÈRES