
Thèse de doctorat

**Les enjeux juridiques de la
numérisation du renseignement**

Darius FADIER

Soutenue le 24 octobre 2024

Sous la direction du Professeur Bertrand WARUSFEL

Discipline

Droit public

École doctorale

ED-401 Sciences sociales

**Laboratoire/Partenaires de
recherche**

Centre de recherches juridiques
de Paris 8 (CRJP8)

Composition du jury

Xavier LATOUR

Professeur à l'Université de Côte d'Azur

Valère NDIOR

Professeur à l'Université de Bretagne Occidentale

Bénédicte BEVIÈRE-BOYER

*Maître de conférences-HDR à l'Université de Paris
8 Vincennes-Saint-Denis*

Sébastien-Yves LAURENT

Professeur à l'Université de Bordeaux

Bertrand WARUSFEL, Directeur de thèse

*Professeur à l'Université de Paris 8 Vincennes-
Saint-Denis*

L'Université Paris 8 Vincennes-Saint-Denis n'entend ni approuver ni désapprouver les opinions émises dans cette thèse. Elles doivent être considérées comme propres à leur auteur qui seul en répond.

Titre : Les enjeux juridiques de la numérisation du renseignement

Résumé :

L'utilisation des technologies du numérique par le renseignement d'Etat dans l'organisation et le fonctionnement de ses missions n'est pas un phénomène nouveau. Cependant, les progrès de l'informatique avec le Big data et l'Intelligence artificielle ainsi que l'émergence du cyberspace ont démultiplié les capacités du renseignement numérique, notamment pour lutter efficacement contre le terrorisme, et renouvelé ses missions pour les besoins de la cyberdéfense. Cette numérisation suscite des inquiétudes pour les droits et libertés face au risque d'une surveillance de masse liberticide mais aussi pour l'économie numérique qui peut être fragilisée par les capacités de cyberespionnage. Par conséquent, la numérisation du renseignement n'a pas manqué d'être appréhendée par le droit, tant au niveau international et européen qu'au niveau national. Plus particulièrement, l'encadrement de la numérisation du renseignement fait l'objet d'une dualité entre le droit du renseignement et le droit du numérique qui pose la question de leur articulation dans la conciliation des activités du renseignement numérique et ses développements avec les droits et libertés et la protection du cyberspace. Si un droit du renseignement numérique émerge pour réguler de façon autonome les moyens numériques de renseignement, il faut tenir compte de l'application du droit du numérique pour appréhender l'encadrement des activités du renseignement au-delà des moyens de recherche et de collecte des données. Dans un contexte de renforcement continu du renseignement numérique, l'articulation entre le droit du renseignement et le droit du numérique doit pouvoir davantage renforcer l'encadrement de cette activité particulière du renseignement en tenant compte de la cybersécurité de la société, tant dans son organisation que dans l'attribution de ses moyens.

Mots clés : Droit du renseignement – Droit du numérique – Renseignement numérique – Cyberespionnage – Surveillance – Cyberspace – Economie numérique – Cybersécurité – Libertés et droits fondamentaux – Sécurité nationale – Cyberdéfense – Protection des données

Title: The legal issues of the digitalization of intelligence

Abstract:

The use of digital technologies by state intelligence in the organization and operation of its missions is not a new phenomenon. However, advances in computing with Big Data and Artificial Intelligence, as well as the emergence of cyberspace, have multiplied the capabilities of digital intelligence, in particular to fight terrorism effectively, and renewed its missions for the needs of cyberdefence. This digitalization raises concerns for rights and freedoms in the face of the risk of oppressive mass surveillance, but also for the digital economy, which can be weakened by cyber espionage capabilities. Consequently, the digitization of intelligence has not failed to be apprehended by the law, both at the international and European level and at the national level. More specifically, the supervision of the digitalization of intelligence is the subject of a duality between intelligence law and digital law which raises the question of their articulation in the reconciliation of digital intelligence activities and its developments with the fundamental rights and the protection of cyberspace. While digital intelligence law is emerging to independently regulate digital intelligence resources, it is necessary to consider the application of digital law to understand the supervision of intelligence activities beyond the means of intelligence research and data collection. In a context of continuous reinforcement of digital intelligence, the articulation between intelligence law and digital law must be able to further strengthen the supervision of this particular intelligence activity by taking into account the cybersecurity of society, both in its organization and in the allocation of its resources.

Keywords : Intelligence law – Digital law – Digital intelligence – Cyber espionage – Surveillance – Cyberspace – Digital economy – Cybersecurity – Fundamental rights – National security – Cyberdefense – Data protection

Remerciements

Je tiens tout d'abord à remercier le Professeur Bertrand Warusfel qui m'a accordé sa confiance pour la réalisation de ces travaux de recherche. Je souhaite tout particulièrement le remercier pour son écoute, ses conseils et sa transparence ainsi que pour sa patience respectueuse des idées développées dans cette étude. Je remercie les Professeurs Xavier Latour, Sébastien-Yves Laurent, Valère Ndior et Madame Bénédicte Bévière-Boyer d'avoir accepté de constituer mon jury de soutenance.

Je remercie également chacune des personnes du monde universitaire et professionnel, civiles et militaires, qui m'ont permis d'appréhender les différents sujets de cette étude et d'éclairer ma réflexion, notamment durant mes années de consultant en cyberdéfense et cybersécurité au sein de la Compagnie européenne d'intelligence stratégique (CEIS).

Enfin, je remercie chaleureusement ma famille et mes proches qui m'ont soutenu à chaque instant de ces travaux et permis de traverser toutes les étapes de ce long projet malgré ses difficultés.

SOMMAIRE

INTRODUCTION

PREMIERE PARTIE

UNE AUTONOMISATION DU DROIT DU RENSEIGNEMENT NUMERIQUE

TITRE I : LE RENFORCEMENT DES MOYENS NUMERIQUES DE RENSEIGNEMENT

CHAPITRE I : La recherche numérique des renseignements

CHAPITRE II : L'exploitation numérique des renseignements

TITRE II : L'ADAPTATION DES GARANTIES AUX MOYENS NUMERIQUES DE RENSEIGNEMENT

CHAPITRE I : L'ambivalence du régime de mise en œuvre des moyens numériques

CHAPITRE II : La spécialisation du contrôle sur les moyens numériques

SECONDE PARTIE

L'APPLICATION DU DROIT DU NUMERIQUE AU RENSEIGNEMENT

TITRE I : LES INTRICATIONS DU DROIT DU NUMERIQUE ET DU DROIT DU RENSEIGNEMENT

CHAPITRE I : La diffusion du droit européen relatif à la vie privée numérique

CHAPITRE II : L'affirmation du droit pénal du numérique

TITRE II : LE RENSEIGNEMENT ET LA PROTECTION DU CYBERESPACE

CHAPITRE I : L'encadrement de la militarisation du cyberspace

CHAPITRE II : Le renseignement numérique et la cybersécurité

CONCLUSION GENERALE

RENFORCER L'ENCADREMENT DU RENSEIGNEMENT NUMERIQUE

LISTE DES PRINCIPALES ABREVIATIONS

AAI	Autorité administrative indépendante
ACCRéD	Automatisation de la consultation centralisée de renseignements et de données
AJDA	Actualité Juridique Droit Administratif
ANSSI	Agence nationale de la sécurité des systèmes d'information
AQSSI	Autorité qualifiée en sécurité des systèmes d'information
ARCEP	Autorité de régulation des communications électroniques et des postes
BCR-DNRED	Base centrale de renseignement de la DNRED
BDU	Biens à double usage
CDI	Captation de données informatiques
CE	Conseil d'Etat
CEDH	Cour européenne des droits de l'homme
CEPD	Comité européen de la protection des données
CERT	Computer emergency response team
CJUE	Cour de justice de l'Union européenne
CNCDH	Commission nationale consultative des droits de l'homme
CNCIS	Commission nationale de contrôle des interceptions de sécurité
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNIL	Commission nationale de l'information et des libertés
CNNum	Conseil national du numérique
CNRLT	Coordination nationale du renseignement et de la lutte contre le terrorisme

COMCYBER	Commandement de la cyberdéfense
Conv.EDH	Convention européenne des droits de l'homme
CRISTINA	Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux
CSDN	Commission du secret de la défense nationale
DCRI	Direction centrale du renseignement intérieur
DGSE	Direction générale de la sécurité extérieure
DGSI	Direction générale de la sécurité intérieure
DIH	Droit international humanitaire
DNRED	Direction nationale du renseignement et des enquêtes douanières
DPR	Délégation parlementaire au renseignement
DRM	Direction du renseignement militaire
DRPP	Direction du renseignement de la Préfecture de police de Paris
DRSD	Direction du renseignement et de la sécurité de la défense
EASP	Enquêtes administratives liées à la sécurité publique
EDVIGE	Exploitation documentaire et valorisation de l'information générale
EDVISP	Exploitation documentaire et valorisation de l'information relative à la sécurité publique
ENISA	Agence de l'Union européenne pour la cybersécurité
FAI	Fournisseur d'accès à internet
FIJAIT	Fichier judiciaire national automatisé des auteurs d'infractions terroristes
FIT	Fichier informatisé du terrorisme
FPR	Fichier des personnes recherchées
FSPRT	Fichier des signalements pour la prévention de la radicalisation à caractère terroriste
GCHQ	Government Communications Headquarters

GESTEREXT	Gestion du terrorisme et des extrémismes à potentialité violente
GIC	Groupement interministériel de contrôle
GIPASP	Gestion de l'information et prévention des atteintes à la sécurité publique
IA	Intelligence artificielle
INRIA	Institut national de recherche en sciences et technologie du numérique
ISR	Inspection des services de renseignement
L2I	Lutte informatique d'influence
LCEN	Loi pour la confiance dans l'économie numérique
LID	Lutte informatique défensive
LII	Lutte informatique informationnelle
LIO	Lutte informatique offensive
LPM	Loi de programmation militaire
NSA	Nation Security Agency
OIV	Opérateur d'importance vitale
OSE	Opérateur de services essentiels
OVC	Objectifs à valeur constitutionnelle
PASP	Prévention des atteintes à la sécurité publique
PNOR	Plan national d'orientation du renseignement
PNR	Passenger Name Record
QPC	Question prioritaire de constitutionnalité
RDI	Recueil de données informatiques
RG	Renseignements généraux
RGPD	Règlement général sur la protection des données
RIC	Renseignement d'intérêt cyber
ROC	Renseignement d'origine cyber
ROSO	Renseignement d'origine sources ouvertes

RSC	Revue de science criminelle et de droit pénal comparé
RTD Eur.	Revue trimestrielle de droit européen
SCRT	Service central du renseignement territorial
SDAO	Sous-direction de l'anticipation opérationnelle
SDIG	Services du renseignement territorial de sécurité publique
SGDSN	Secrétariat général de la Défense et de la Sécurité nationale
SILT	Loi renforçant la sécurité intérieure et la lutte contre le terrorisme
SIREX	Système d'information de la recherche et de l'exploitation du renseignement de contre-ingérence
SNEAS	Service national des enquêtes administratives de sécurité
SNR	Stratégie nationale du renseignement
SNRP	Service national du renseignement pénitentiaire
STAD	Système de traitement automatisé de données
STARTRAC	Système de traitement et analyse du renseignement de Tracfin
TAJ	Traitement des antécédents judiciaires
UCLAT	Unité de coordination de la lutte antiterroriste
UE	Union européenne
UIT	Union internationale des télécommunications
URL	Uniform Resource Locator
VEP	Vulnerabilities Equities Process
VIGINUM	Service de vigilance et de protection contre les ingérences numériques étrangères

INTRODUCTION

Avec le développement du « tout numérique », il est facile d'imaginer que les services de renseignement disposeraient de capacités hors normes permettant d'intercepter, à chaque instant, l'ensemble de nos communications. En 2013, un article du Monde prétendait ainsi révéler l'existence d'un Big Brother français dans lequel « *la DGSE collecte et stocke l'ensemble des mails, SMS, relevés d'appels téléphoniques, accès à Facebook, Twitter..., en dehors de tout contrôle* »¹.

Il est vrai que la numérisation du renseignement démultiplie les capacités des programmes de surveillance des Etats. Le système de « crédit social » chinois constitue un bon exemple des potentiels de la surveillance numérique. Basé sur l'utilisation des technologies du Big data, c'est-à-dire la convergence de la collecte massive de données et des capacités de traitement des données avec l'intelligence artificielle (IA), ce système permet aux autorités chinoises de surveiller les comportements des citoyens afin de leur attribuer une note qui entraînera des conséquences sur leurs droits².

Si le modèle politique chinois n'est en rien comparable à celui de la France, il n'en demeure pas moins que la numérisation du renseignement n'a cessé de se développer avec les progrès des technologies (**Section I**) en suscitant la controverse dans les démocraties libérales (**Section II**). Phénomène porteur d'enjeux juridiques, la numérisation du renseignement n'a pas manqué d'être appréhendée par le droit (**Section III**).

¹ Cf. Le Monde, *Révélation sur le Big Brother français*, 4 juillet 2013, https://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html.

² Sur le régime chinois, voir France culture, *Surveiller pour punir : la notation des citoyens chinois*, 9 janvier 2019, <https://www.franceculture.fr/emissions/les-nouvelles-de-leco/les-nouvelles-de-leco-du-mercredi-09-janvier-2019>.

SECTION I : Les développements de la numérisation du renseignement

L'utilisation des technologies du numérique par les services de renseignement dans l'organisation et le fonctionnement de leurs missions n'est pas un phénomène nouveau. Le « renseignement technique », par opposition au « renseignement humain », s'est très rapidement approprié les innovations des technologies du XXème siècle de l'information et de la communication pour collecter, traiter, analyser et échanger les renseignements¹. Durant les deux guerres mondiales et pendant la guerre froide, le renseignement technique a constitué une branche spécialisée du renseignement, notamment axée sur les interceptions des communications électroniques, la cryptologie² ou encore l'imagerie.

Avec les progrès de l'informatique et l'émergence d'Internet dans les années 2000, le renseignement technique opère une mutation vers le renseignement numérique³. Ce dernier renvoie à la banalisation de la collecte des données numériques et de la coopération des services de renseignement avec les entreprises privées du numérique. Il tend également vers une banalisation de l'utilisation du Big data et des réseaux informatiques comme le Cloud computing⁴ au sein des services de renseignement pour l'analyse et le partage des renseignements⁵.

Aujourd'hui, le renseignement numérique constitue une activité quotidienne et essentielle des services de renseignement à l'ère du cyberspace.

¹ Sur ce point, voir J. -C. Cousseran et P. Hayez, *Leçon sur le Renseignement*, Odile Jacob, septembre 2017, p. 96 à 101.

² « Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage. » Comprendre les grands principes de la cryptologie et du chiffrement, 25 octobre 2016, site internet de la Commission nationale de l'informatique et des libertés (CNIL), <https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>.

³ A ce sujet, voir J. -C. Cousseran et P. Hayez, *Leçon sur le Renseignement*, op. cit., p. 101 à 105.

⁴ « Le cloud computing (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (cloud) composé de nombreux serveurs distants interconnectés. » Cloud Computing, site internet de la CNIL, <https://www.cnil.fr/fr/definition/cloud-computing>.

⁵ En ce sens, voir O. Chopin et B. Oudet, *Renseignement et sécurité*, Armand Colin, septembre 2019, p. 176 et suivantes.

Cette mutation est notamment renforcée par les avantages que procurent les outils numériques aux services de renseignement sur le plan opérationnel :

- d'une part, ils réduisent les risques de mise en danger de la vie des agents de renseignement ou des sources humaines tout en permettant de collecter de nombreuses informations ;
- d'autre part, les capacités du Big data et de l'IA permettent de traiter et d'analyser rapidement de nombreuses données variées, ce qui apporte plus de réactivité aux services¹. En outre, les possibilités d'analyse prédictive et de profilage qu'offrent le Big data sont particulièrement adaptées aux besoins des services de renseignement, qui anticipent les menaces ou cherchent à détecter des signaux faibles en matière de lutte anti-terroriste par exemple ;
- enfin, l'ère du cyberspace offre de nouvelles opportunités pour les services de renseignement qui peuvent recourir à des cyber-opérations comme le piratage informatique pour dérober des données de manière totalement anonyme².

La numérisation du renseignement est un phénomène qui n'a cessé de se développer comme en témoigne la montée en puissance d'agences autonomes de renseignement numérique dans certains pays comme les Etats-Unis avec la National Security Agency (NSA) ou le Royaume-Uni avec le Government Communications Headquarters (GCHQ). Ce phénomène est entré dans son âge d'or avec l'émergence du cyberspace et devrait continuer son expansion.

Sur le plan des missions du renseignement, soulignons que la priorité laissée à la lutte anti-terroriste dans cette dernière décennie a particulièrement incité le renseignement à se numériser³. En outre, la numérisation du renseignement est considérée comme une nécessité stratégique pour les années à venir, notamment en matière de cyberdéfense. En France, le Livre blanc de 2013 a

¹ En ce sens, voir O. Becht et T. Gassilloud, *Rapport d'information en conclusion des travaux d'une mission d'information (1) sur les enjeux de la numérisation des armées*, 30 mai 2018, p. 29 et suivantes.

² A ce sujet, voir O. Chopin et B. Oudet, *Renseignement et sécurité*, op. cit., p. 183 et suivantes.

³ En ce sens, voir B. Warusfel, *Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement*, in *Le droit du renseignement*, Actes du colloque de l'Académie du renseignement tenu le 8 février 2019, La Documentation française, 2019, p. 75 et suivantes.

ainsi affirmé le besoin de renforcer « *les capacités techniques de recueil et d'exploitation du renseignement* »¹. La *Revue stratégique de cyberdéfense* de 2018 a pris en compte les risques de cyberespionnage et consacré la place du renseignement dans l'organisation de la cyberdéfense française². Selon le rapport parlementaire sur la souveraineté numérique de 2019³ et le rapport de la Délégation parlementaire au renseignement (DPR) de 2019-2020⁴, le renseignement est amené à jouer un rôle défensif et offensif dans la politique publique de cyberdéfense, notamment en disposant de capacités d'action destinées à entraver ou faire cesser une cyberattaque. Ces considérations ont été confirmée par la *Stratégie nationale du renseignement* (SNR) de juillet 2019 qui fait de la numérisation l'un des enjeux prioritaires de la communauté française du renseignement en affirmant que :

« Des progrès considérables ont été réalisés en termes de décloisonnement entre les services de renseignement. Le partage de l'information et l'échange tendent à devenir la norme, allant même jusqu'à l'intégration complète dans les domaines les plus sensibles comme la lutte contre le terrorisme. Les défis technologiques constituent également une priorité pour la communauté du Renseignement. Au-delà de la poursuite indispensable des mutualisations, trois enjeux sont majeurs pour les années à venir :

o la diffusion de l'expertise entre les services pour permettre à chacun de s'approprier les nouveaux outils ;

o la valorisation des données, de plus en plus volumineuses et hétérogènes ;

o la conception de nouveaux outils en anticipant les évolutions technologiques et en s'appuyant sur une culture de l'innovation en lien avec la Recherche et l'industrie »⁵.

¹ Cf. Livre blanc sur la défense et la sécurité nationale de 2013, p. 137.

² Cf. *Revue stratégique de cyberdéfense* du 12 février 2018.

³ Cf. G. Longuet, *Rapport fait au nom de la commission d'enquête (1) sur la souveraineté numérique*, 1er octobre 2019, p.107 et suivantes.

⁴ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, 11 juin 2020, p. 256 et suivantes.

⁵ Cf. *Stratégie nationale du renseignement*, juillet 2019, p. 11.

La numérisation du renseignement s'est légitimement développée en suivant les avancées technologiques et en fonction de l'importance croissante de la place stratégique qu'occupe le cyberspace en matière de sécurité et de défense. Cependant, elle suscite la controverse en raison des bouleversements qu'elle entraîne dans les pratiques de surveillance.

SECTION II : Une numérisation controversée

La numérisation croissante du renseignement fait l'objet de critiques de la part des défenseurs des libertés et des droits fondamentaux du fait qu'elle pourrait conduire à une surveillance de masse liberticide des citoyens (§1). Par ailleurs, le développement du cyber-renseignement est également critiqué dans son rapport avec l'économie numérique (§2).

§1. Surveillance de masse et libertés

La collecte et le traitement massif de données par les services de renseignement, notamment avec la collaboration des opérateurs de télécommunications et d'Internet, entraînent un changement de paradigme dans la pratique de la surveillance. S'éloignant des traditionnelles méthodes d'observation humaine comme la « filature » ou la « planque »¹, la surveillance numérique permet de collecter et traiter des informations sur de nombreuses cibles simultanément. La collaboration entre les opérateurs de télécommunications et les services de renseignement permet par exemple à ces derniers de surveiller de nombreux moyens de communications électroniques en recueillant leurs métadonnées (comme la date et l'heure des communications ou encore les données de localisation des équipements utilisés).

En 2013, les révélations d'Edward Snowden, ancien employé de la NSA, sur les programmes américains de surveillance numérique ont démontré le passage d'une pratique de la surveillance ciblée à la pratique d'une surveillance de masse².

¹ A ce sujet, voir H. Moutouh et J. Poirot, *Surveillance*, in Dictionnaire du renseignement, Perrin, 2018, p.744 à 746.

² A ce sujet, voir E. Snowden, *Mémoires vives*, Editions du Seuil, 19 septembre 2019 ou encore C. Delesse, NSA, *Histoire de la plus secrète des agences de renseignement*, collection Texto, Editions Tallandier, 2016 et 2018, p. 217 à 241 et p. 247 et suivantes.

Selon ces révélations, la NSA aurait collecté massivement et de manière indifférenciée des données sur les citoyens américains pour les besoins de la lutte anti-terroriste avec l'aide des géants du numérique Google, Apple, Facebook, Amazon et Microsoft (GAFAM). Les outils utilisés par l'agence permettent notamment, en temps réel, de collecter directement les données dans les réseaux des opérateurs de télécommunications et d'Internet. Si ces programmes de surveillance de masse peuvent être considérés comme liberticides, ils auraient pourtant été autorisés selon l'USA Patriot Act (USAPA) de 2001 jusqu'en 2015. Par la suite et sans remettre en cause la surveillance numérique, l'USA Freedom Act de 2015 est toutefois venu renforcer les limites des moyens de la NSA pour protéger la vie privée des citoyens américains, notamment en imposant la destruction des renseignements collectés ne relevant pas du renseignement extérieur¹.

En France, la Délégation parlementaire au renseignement (DPR) a confirmé le phénomène d'un passage possible de la surveillance ciblée à la surveillance de masse par l'emploi des moyens numériques dans son rapport d'activité pour l'année 2014. En revanche, elle a tenu à préciser que la philosophie du renseignement technique reste la surveillance ciblée en France et que les moyens consentis aux services ne permettent pas d'égaliser ceux de la NSA². Néanmoins, la loi relative au renseignement de 2015³ a considérablement renforcé les moyens numériques de renseignement en introduisant notamment la possibilité de recourir à des techniques algorithmiques de filtrage des communications chez les opérateurs du numérique pour détecter des connexions susceptibles de révéler une menace terroriste⁴. Ces « boîtes noires » ont d'ailleurs pu être comparées aux outils de surveillance de masse utilisés par la NSA⁵.

¹ Pour en savoir plus, voir notamment C. Delesse, *NSA, Histoire de la plus secrète des agences de renseignement*, op. cit., p. 468 et 469.

² Cf. J. -J. Urvoas et J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, DPR, 18 décembre 2014, p. 133.

³ Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

⁴ Article L851-3 du code de la sécurité intérieure.

⁵ A ce sujet, voir par exemple Franceinfo, « Boîte noire » et surveillance du web : le projet de loi sur le renseignement est-il liberticide ? 5 avril 2015, <https://www.francetvinfo.fr/faits-divers/terrorisme/boite-noire-et-surveillance-du-web-le-projet-de-loi-sur-le-renseignement-est-il-liberticide-867611.html>.

Par ailleurs, le changement d'échelle dans la collecte des données induit par la numérisation du renseignement s'accompagnerait d'une augmentation du fichage de la population et d'un risque de profilage prédictif et discriminatoire des citoyens¹. Ce risque est effectivement intrinsèque à l'utilisation des algorithmes qui, à l'heure de l'IA, peuvent être biaisés dans leur paramétrage, ce qui peut entraîner un important taux de faux positifs dans les résultats du traitement des données². Il n'est donc pas certain que l'utilisation des algorithmes soit également gage d'efficacité.

Si les risques d'atteinte aux libertés sont à prendre très au sérieux, il convient de rester prudent sur l'efficacité et sur les réelles capacités des moyens numériques des services de renseignement en matière de surveillance de masse secrète, notamment en raison du peu d'informations disponibles publiquement. En outre, il ne faut pas oublier la raison d'être des services de renseignement qui agissent pour la protection de la sécurité nationale et de la défense nationale, et qui alors œuvrent pour la préservation des libertés dans les démocraties libérales comme en France.

Comme soulevé par Dominique Guibert, ancien vice-président de la Ligue des droits de l'homme (LDH), dans le rapport de 2014 de Jean-Pierre Sueur sur « *le numérique, le renseignement et la vie privée* », les considérations précédentes posent particulièrement les questions de savoir jusqu'à quel point les services de renseignement peuvent bénéficier des avancées du numérique et s'il est pertinent de constituer des bases de données considérables pour les besoins de leurs missions³.

¹ En ce sens, voir G. Virginie et D. Monniaux. « *De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme* », Archives de politique criminelle, vol. 38, no. 1, 2016, pp. 123-135.

² A ce sujet, voir le rapport de la CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, décembre 2017.

³ Cf. J.-P. Sueur, *Rapport d'information sur le numérique, le renseignement et la vie privée : de nouveaux défis pour le droit*, 27 juin 2014, p. 43.

§2. Cyber-renseignement et économie numérique

La numérisation du renseignement soulève des débats relatifs à l'économie numérique et au secteur privé. Ces débats concernent notamment le chiffrement des données, le piratage informatique, la privatisation et l'externalisation du renseignement.

La polémique du chiffrement. Les difficultés pour les services de renseignement ou d'enquête judiciaire d'accéder aux communications sécurisées d'auteurs d'attentats terroristes aux Etats-Unis ou en Europe ont suscité, ces dernières années, une polémique sur la liberté et la généralisation du chiffrement¹. Les débats concernent notamment la possibilité d'obliger les opérateurs du numérique à prévoir des « portes dérobées »² dans leurs solutions de chiffrement pour les services de renseignement et d'enquête judiciaire. Cependant, le Conseil national du numérique (CNNum) a tenu à souligner, dans son avis « Prédications, chiffrement et libertés » de 2017, que ce type de mesure pourrait présenter « *des conséquences dramatiques pour l'ensemble des utilisateurs* »³. En effet, l'introduction de « portes dérobées » aurait pour effets d'affaiblir le chiffrement et de permettre, par exemple, à des cybercriminels ou à des services de renseignement étrangers d'accéder au contenu de communications en ligne et à des données sensibles.

Le piratage informatique. Les services de renseignement sont régulièrement accusés de développer et d'utiliser, sans limite, des logiciels malveillants à des fins de cyber-espionnage et de contribuer à la militarisation du cyberspace. A titre d'exemple, la NSA et le GCHQ ont été accusés de piratage informatique contre la société Belgacom, l'un des plus importants opérateurs

¹ A ce sujet, voir F. Pellegrini, *Sécurité et numérique : Entre fantasmes d'efficacité et violations avérées des droits fondamentaux*. in Mustapha Afroukh ; Christophe Maubernard ; Claire Val. La sécurité : mutations et incertitudes, Institut universitaire Varenne, pp.89-100, 2019, Collection Colloques & Essais, 978-2-37032-204-3.

² « Une porte dérobée (ou backdoor) est un point d'accès à un système d'exploitation, à un programme ou à un service en ligne. Ces passages secrets sont généralement introduits à l'insu de l'utilisateur. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle. Pour des pirates ou des services de renseignement, l'intérêt réside dans la possibilité de surveiller les activités de l'utilisateur, copier ou détruire des données, prendre le contrôle d'un ordinateur, etc. » Conseil national du numérique, *Prédications, chiffrement et libertés*, op. cit., p. 6.

³ Ibid.

belges de télécommunications et d'Internet (« Operation Socialist »)¹. Au-delà d'un risque de surveillance de masse des communications des individus, le piratage d'un opérateur de télécommunications et d'Internet, chargé d'assurer le fonctionnement d'infrastructures critiques du cyberspace, pourrait entraîner des conséquences préjudiciables pour les Etats et les entreprises.

Autre exemple, la responsabilité de la NSA a été mise en cause par Microsoft dans la cyberattaque mondiale WannaCry de 2017 qui a touché plus de 150 pays². L'entreprise américaine a reproché à la NSA d'avoir développé et perdu, sans alerter, les failles de sécurité informatiques qui ont servi à la cyberattaque³. Cette affaire a soulevé la question de la possibilité pour les services de renseignement de conserver et de ne pas divulguer des failles de sécurité informatiques pour les besoins du cyber-espionnage alors que de telles failles sont de nature à remettre en cause la sécurité du cyberspace. À la suite de cette affaire, Microsoft avait alors proposé l'élaboration d'une Convention de Genève numérique pour encadrer ce type de situation et protéger la société civile numérique, notamment contre les risques de dérives des cyber-opérations étatiques⁴. Par ailleurs, la perte des failles de sécurité par l'agence américaine démontre également que les systèmes numériques des services de renseignement peuvent être vulnérables, ce qui implique que la numérisation du renseignement peut présenter un risque pour la protection du secret de la défense nationale. A ce sujet, le rapport de la DPR de 2019-2020 a tenu à communiquer sur l'importance du rôle des mesures de cybersécurité applicables aux services de renseignement pour assurer la protection du secret de la défense nationale⁵.

¹ A ce sujet, voir C. Delesse, « La NSA, « mauvais génie » du cybermonde ? », Sécurité globale, vol. 8, no. 4, 2016, pp. 67-104.

² A ce sujet, voir notamment Agence nationale de la sécurité des systèmes d'information (ANSSI), *Etat de la menace rançongiciel à l'encontre des entreprises et institutions*, 5 février 2020, p. 6

³ Cf. Le Monde, *Le rançongiciel WannaCry ravive le débat sur les failles de sécurité*, 16 mai 2017, https://www.lemonde.fr/pixels/article/2017/05/16/le-rancongiel-wannacry-ravive-le-debat-sur-les-failles-de-securite_5128242_4408996.html.

⁴ A ce sujet, voir notre article D. Fadier, *Avis d'Experts CEIS : Convention de Genève numérique de Microsoft, une protection adaptée ?*, l'Espresso, 1 décembre 2017, <https://www.itespresso.fr/avis-expert/ceis-convention-geneve-numerique-microsoft>.

⁵ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 168 et suivantes.

La privatisation et l'externalisation du renseignement. La numérisation du renseignement incite les services de renseignement à développer des partenariats technologiques avec le secteur privé. En effet, les expertises dans les domaines du Big data ou de l'IA se sont développées au sein des entreprises privées et dans le cadre d'applications commerciales¹. Cette tendance à recourir au secteur privé s'est affirmée aux Etats-Unis² et semble s'exporter en France avec, par exemple, la création de l'*Intelligence Campus* en 2017 au sein de la Direction du renseignement militaire (DRM) ou encore le choix pour la Direction générale de la sécurité intérieure (DGSI) de recourir aux services de Big data de l'entreprise américaine Palantir³. Pour autant, le recours à l'expertise privée en matière de numérique pourrait entraîner l'émergence d'un « marché du renseignement »⁴ potentiellement contradictoire avec la dimension régaliennne des missions des services de renseignement. Il s'agit là d'un enjeu lié à la construction d'une souveraineté numérique française et européenne.

Véritables enjeux juridiques, les débats relatifs à la surveillance de masse et aux libertés ainsi qu'à l'économie numérique font de la numérisation du renseignement un phénomène de plus en plus appréhendé par le droit.

¹ A ce sujet, voir O. Chopin et B. Oudet, *Renseignement et sécurité*, op. cit., p. 178 et suivantes.

² En ce sens, voir J. -C. Cousseran et P. Hayez, *Leçon sur le Renseignement*, op. cit., p. 293 et suivantes.

³ Cf. A. Drif, *Big Data : faute de solution française, les services secrets signent à nouveau avec Palantir*, Les Echos, 27 novembre 2019, <https://www.lesechos.fr/industrie-services/air-defense/big-data-faute-de-solution-francaise-les-services-secrets-signe-a-nouveau-avec-palantir-1151255>.

⁴ En ce sens, voir O. Chopin et B. Oudet, *Renseignement et sécurité*, op. cit., p. 180.

SECTION III : Une numérisation appréhendée par le droit

Bien que la numérisation du renseignement ne soit pas une notion juridique, le droit international et européen (§1) et le droit national (§2) s'intéressent à l'encadrement et au contrôle de ce phénomène. Une certaine dualité entre le droit du renseignement et le droit du numérique tend à assurer la conciliation entre les besoins numériques du renseignement et la protection des droits et libertés à l'ère du cyberspace (§3).

§1. Le droit international et européen

Depuis que la « cyberdimension » exerce un véritable impact sur la société internationale¹, la surveillance numérique et les cyberopérations étatiques d'espionnage font l'objet d'une intense production juridique en droit international et européen.

Tout d'abord, la communauté internationale et la doctrine se sont saisies de la question de la légalité du cyber-renseignement dans le cadre des réflexions sur l'application du droit international public au cyberspace et aux cyberopérations². En outre, la communauté internationale s'est également saisie de la question de la prolifération des moyens numériques d'espionnage et des cyberarmes³ en introduisant, par exemple, la notion de « logiciel d'intrusion »⁴ dans la Liste des biens et technologies à double usage (BDU) de l'Arrangement de Wassenaar, régime multilatéral de contrôle des exportations des biens et technologies à usage civil et militaire fondé en 1994⁵. Par ailleurs, notons que la surveillance des communications électroniques entre également dans le champ du droit international des droits de l'homme. A cet égard, on peut mentionner l'article

¹ En ce sens, voir J. -C. Cousseran et P. Hayez, *L'adaptation du renseignement à la cyberdimension*, in *Leçon sur le Renseignement*, op. cit., p. 229 à 248.

² A ce sujet, voir O. Chopin et B. Oudet, *Renseignement et sécurité*, op. cit., p. 185 et suivantes ; J. -C. Cousseran et P. Hayez, *L'adaptation du renseignement à la cyberdimension*, in *Leçon sur le Renseignement*, op. cit., p. 229 à 248.

³ A ce sujet, voir A. Géry, *Droit international et prolifération des cyberarmes*, *Politique étrangère*, vol. Été, no. 2, 2018, pp. 43-54.

⁴ Sur l'introduction de la notion de « logiciel d'intrusion », voir Observatoire du monde cybernétique, *La révision de l'Arrangement de Wassenaar dans le domaine des logiciels d'intrusion et ses conséquences*, Lettre n° 70, Janvier 2018.

⁵ Sur l'Arrangement de Wassenaar et son fonctionnement, voir le site internet dédié <https://www.wassenaar.org/>.

37 de la Constitution de l'Union internationale des télécommunications (UIT) qui consacre le secret des télécommunications internationales ou encore le Pacte international relatif aux droits civils et politiques (PIDCP) en matière de protection de la vie privée¹.

Ensuite, dans le cadre du Conseil de l'Europe, trois instruments conventionnels peuvent trouver à s'appliquer à la numérisation du renseignement :

- la Convention européenne des droits de l'homme (Conv. EDH) : l'application de cette convention, à travers la jurisprudence de la Cour européenne des droits de l'Homme (CEDH), constitue une source historique du développement du droit du renseignement français et de l'encadrement du renseignement numérique. Depuis trente ans, la CEDH a eu l'occasion de se prononcer de nombreuses fois sur l'application de la Conv. EDH aux législations nationales relatives aux outils numériques de surveillance. S'agissant de la France, la « légalisation du renseignement d'Etat » s'est imposée à la suite de deux condamnations de la CEDH dans ses arrêts *Huvig et Kruslin c. France* du 24 avril 1990 qui constataient les insuffisances du droit français en matière d'interception des communications électroniques. La Conv. EDH et la jurisprudence de la Cour ont d'ailleurs constituer un socle conventionnel pour l'élaboration de la loi relative au renseignement du 24 juillet 2015² ;
- la Convention sur la cybercriminalité de Budapest : « *Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux* »³, les Etats membres du Conseil de l'Europe et les autres Etats signataires de la Convention ont ainsi souhaité harmoniser leur législation pénale et renforcer leur coopération dans la lutte contre la cybercriminalité, ce qui

¹ A ce sujet, voir F. Lafouasse, *Le droit du renseignement : un droit conforme aux traités internationaux*, in *Le droit du renseignement*, Actes du colloque de l'Académie du renseignement tenu le 8 février 2019, op. cit., p. 187 et suivantes.

² Voir à ce sujet l'étude d'impact du projet de loi relatif au renseignement du 18 mars 2015.

³ Cf. Préambule de la Convention sur la cybercriminalité du Conseil de l'Europe signée à Budapest en 2001.

pourrait entraîner des risques de poursuites judiciaires à l'encontre des agents des services de renseignement ayant, par exemple, recours au piratage informatique ;

- la Convention 108+ sur la protection des données personnelles : ouverte à la signature en 1981, cet instrument constitue actuellement la seule convention multilatérale juridiquement contraignante en matière de protection des données. Elle a été modernisée en 2018 afin notamment de prendre en compte les flux internationaux des données et pourrait constituer un instrument pertinent dans « *la nécessité d'une supervision démocratique et effective des services de renseignement* »¹.

Enfin, le droit de l'Union européenne trouve également à s'appliquer dans trois domaines déjà évoqués précédemment dans les sources du droit international applicables à la numérisation du renseignement :

- premièrement, la compétence de l'Union européenne en matière de protection des droits fondamentaux et des données personnelles a permis à la Cour de justice de l'Union européenne (CJUE) d'exercer un contrôle sur le renseignement numérique et d'en préciser ses limites² ;
- deuxièmement, l'Union européenne tend à se doter de moyens juridiques visant à renforcer la cybersécurité de l'Union et de ses Etats membres, notamment avec la possibilité de prononcer des sanctions contre les responsables de cyberattaques³. Ces sanctions pourraient concerner des services de renseignement ayant recours au piratage informatique ;
- troisièmement, il convient de mentionner le régime de contrôle des exportations des biens à double usage de l'Union européenne qui s'inscrit dans la lignée de l'Arrangement de Wassenaar et qui constitue, par ailleurs, le régime applicable en France. Plus particulièrement, le régime européen

¹ En ce sens, voir la déclaration conjointe par Alessandra Pierucci, Présidente du Comité de la Convention 108 et Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l'Europe, Conseil de l'Europe, Strasbourg, 7 septembre 2020.

² A ce sujet, voir la jurisprudence CJUE, 6 octobre 2020, *affaire C-623/17 Privacy International et dans les affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, French Data Network e.a., ainsi que C-520/18 Ordre des barreaux francophones et germanophone e.a.*

³ Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres.

a fait l'objet d'une refonte en 2021 introduisant un contrôle spécifique sur les biens de cybersurveillance¹.

§2. Le droit national

La plupart des pays européens, dont la France, se sont dotés d'un cadre juridique spécifique pour encadrer les services de renseignement en droit interne. De manière générale, cet encadrement a pu être présenté sous la forme d'un triptyque comprenant un encadrement législatif des services de renseignement, un contrôle parlementaire des services et un contrôle des activités exercé par une autorité administrative ou judiciaire². En France, la « légalisation du renseignement d'Etat »³ a adopté ce modèle avec :

- la création d'une Délégation parlementaire au renseignement (DPR) en 2007⁴ ;
- la promulgation de la loi relative au renseignement de 2015 et la création d'un Livre VIII intitulé « Du renseignement » au sein du Code de la sécurité intérieure (CSI)⁵ ;
- la création d'une autorité administrative indépendante (AAI), la Commission nationale de contrôle des techniques de renseignement (CNCTR)⁶.

Si des similitudes existent entre les pays européens, l'organisation, le fonctionnement et les missions des services de renseignement restent bien spécifiques à chacun des Etats, notamment en matière de renseignement numérique. C'est pourquoi, cette étude a pour objet principal le cadre juridique français.

¹ Règlement (UE) 2021/821 instituant un régime de l'UE de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage.

² A ce sujet, voir G. Rapaille, *Approche comparée des droits du renseignement (Belgique/Europe)*, in *Le droit du renseignement*, op. cit., p. 47 et suivantes.

³ Sur la légalisation du renseignement, voir B. Warusfel, « *Le renforcement du cadre juridique des services de renseignement* », *L'ENA hors les murs*, juin 2014.

⁴ Loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.

⁵ Articles L801-1 à L898-1 du code de la sécurité intérieure (CSI).

⁶ Titre III du Livre VIII du CSI, « De la Commission nationale de contrôle des techniques de renseignement » (articles L831-1 à L833-11 du CSI).

Depuis les années 1990, les évolutions du droit du renseignement français ont porté, pour une grande partie, sur le renforcement de l'encadrement de la montée en puissance des moyens technologiques¹. La loi du 10 juillet 1991 sur le secret des correspondances², premier texte consacré aux activités des services de renseignement, a d'abord encadré la pratique des écoutes téléphoniques. Par la suite, deux lois de 2006 et de 2013 sont notamment venues compléter le dispositif de la loi de 1991 en intégrant la possibilité pour les services de collecter des données techniques de connexion pour les besoins de la lutte anti-terroriste³. A partir de 2015, les différents textes juridiques relatifs au renseignement installent progressivement un dispositif de régulation et de contrôle de la numérisation du renseignement à travers l'encadrement des moyens numériques de collecte des renseignements et de traitement de ces derniers. Soulignons que ce dispositif porte aussi bien sur la surveillance numérique sur le territoire national⁴ que sur la surveillance des communications électroniques internationales⁵, prenant ainsi en considération le caractère transnational du numérique.

Au-delà du droit du renseignement, d'autres réglementations de droit interne concernent également l'encadrement de la numérisation du renseignement. En effet, le droit des données à caractère personnel organise, par exemple, un système de contrôle des fichiers de renseignement et de police avec la Commission nationale de l'informatique et des libertés (CNIL)⁶. En outre, le droit pénal français applicable à la lutte contre la cybercriminalité peut être invoqué pour réprimer les dérives des services de renseignement et, plus généralement,

¹ En ce sens, voir B. Warusfel, *Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement*, in *Le droit du renseignement*, op. cit., p. 75 et suivantes.

² Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

³ Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers et la 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.

⁴ Loi n° 2015-912 du 24 juillet 2015 relative au renseignement et les dispositions relatives à la surveillance de certaines communications hertziennes de la Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

⁵ Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

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

tout acte de cyber-renseignement non légalement autorisé¹. Par ailleurs, il peut être également mentionné des règles nationales relatives à la sécurité des systèmes numériques qui peuvent intéresser le renseignement. On mentionnera le droit de la cyberdéfense qui a été consacré par les lois de programmation militaire (LPM) de 2013 et 2018. Il s'agit également de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) qui consacre la liberté de chiffrement en France². En outre, le caractère sensible des systèmes utilisés par les services de renseignement implique pour ces derniers et leurs partenaires de se conformer à certaines règles spécifiques aux mesures de sécurité des systèmes numériques. On peut citer par exemple les mesures de sécurité relatives aux systèmes d'information protégés par le droit du secret de la défense nationale (l'IGI 1300)³ ou encore l'organisation d'une procédure de qualification pour les produits de sécurité et les prestataires de services de confiance qui permet de répondre aux demandes de l'Etat et des services de renseignement en matière de numérisation⁴.

§3. Une dualité droit du renseignement/droit du numérique

Parmi les sources juridiques précédemment mentionnées, le droit du renseignement s'impose comme le droit le plus directement invocable pour répondre aux enjeux de la numérisation du renseignement. Cependant, les règles que nous avons évoquées qui sont relatives à la protection des données personnelles et au secret des correspondances électroniques, qui incarnent le droit au respect de la vie privée numérique, ainsi que celles qui encadrent l'économie numérique, la cybersécurité, la cyberdéfense ou encore la lutte contre la cybercriminalité tendent à être aujourd'hui rattachées au droit du numérique

¹ A titre d'exemple, les articles 323-1 et suivants du Code pénal répriment les atteintes aux systèmes de traitement automatisé de données comme les intrusions informatiques ou l'utilisation de logiciel malveillant. Notons que les sanctions prévues par ces textes ont été alourdies par la loi du 24 juillet 2015 relative au renseignement (article 4).

² Voir la rubrique du site web de l'ANSSI, *Sécurité, secret et légalité*, <https://www.ssi.gouv.fr/particulier/bonnes-pratiques/crypto-le-webdoc/securite-secret-et-legalite/>.

³ JORF n° 0277 du 15/11/2020, Arrêté du 13 novembre 2020 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, Annexe, Sécurité des systèmes d'informations classifiés, p. 86 et suivantes.

⁴ Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

qui apparaît alors constituer un second droit régulateur de la numérisation du renseignement¹.

On peut alors émettre l'hypothèse selon laquelle les enjeux juridiques de la numérisation du renseignement trouvent leurs réponses à la fois dans le droit du renseignement et dans le droit du numérique. Toutefois, l'articulation entre ces deux droits n'apparaît pas évidente et peut poser des difficultés. En effet, droit dérogatoire régalien par excellence, le droit du renseignement suit une logique juridique publiciste affirmée de protection de l'Etat, de ses agents et de ses secrets. A l'inverse, le droit du numérique est davantage construit dans une logique privatiste protectrice du droit de propriété et des libertés individuelles et des entreprises puisqu'il s'applique majoritairement à la société civile qui domine l'économie numérique.

Dans ces conditions, l'application du droit du numérique au renseignement interroge mais aussi la possibilité pour le droit du renseignement d'intégrer des principes ou des règles du droit du numérique. On peut également s'interroger sur les risques d'incohérence et d'opposition dans leur conciliation qui pourraient s'avérer une source d'insécurité juridique tant pour l'Etat que pour la société civile, notamment lorsque le droit accuse d'un certain retard face à l'innovation technologique.

La dualité entre le droit du renseignement et le droit du numérique dans la régulation de la numérisation du renseignement fait pourtant sens. Après s'être substitué au « droit de l'informatique », le droit du numérique est conduit à être de plus en plus transversal entre le droit public et le droit privé pour s'adapter aux enjeux du cyberspace².

Par ailleurs, ces deux droits ont des points communs qui sont au cœur des enjeux de la numérisation du renseignement : d'une part, ils sont particulièrement attachés à la sauvegarde des mêmes droits et libertés fondamentales, à savoir le

¹ En ce sens, voir notamment les ouvrages juridiques suivants : M. Quémener, *Ecosystème numérique : défis juridiques et sociétaux*, Gualino, Hors collection, 4 avril 2023 ; *Le Lamy droit du numérique*, par M. Vivant, P. Vivant, B. Warusfel, N. Mallet-Poujol et L. Costes ; C. Féral-Schuht, *Cyberdroit*, Praxis Dalloz, 2020 ; L. Crynbaum, C. Le Goffic et L. -H. Morlet, *Droit des activités numériques*, Précis, juin 2014. Voir également l'article de F. Pellegrini et S. Canevet, *Le droit du numérique : une histoire à préserver. Vers un Musée de l'Informatique et de la Société Numérique en France ?*, Conservatoire National des Arts et Métiers, Nov 2012, Paris, France. pp.61-76.

² Sur la transversalité du droit du numérique, voir notamment B. Warusfel, *La transversalité du droit du numérique*, Études en l'honneur du Professeur Jérôme Huet, LGDJ, pp.412-423, 2017.

respect du droit à la vie privée ou encore les libertés d'expression, de communication et du commerce et de l'industrie ; d'autre part, ils sont empreints de la discipline du management des risques qui est propre à l'activité de renseignement et à l'innovation technologique¹.

Enfin, un défi commun rapproche le droit du renseignement et le droit du numérique, celui du contrôle de la circulation des données et des innovations permettant leur captation et leur exploitation dans un cyberspace mondial aux « internets alternatifs »², pour reprendre l'expression du Professeur Sébastien-Yves Laurent qui nous alertait sur l'existence d'un « monde anomique de données »³.

Analysant chacune des règles du droit du renseignement trouvant à s'appliquer aux activités numériques des services de renseignement et du droit du numérique qui impactent ces derniers, tant dans leur organisation que leur fonctionnement, notre étude met en lumière une articulation nuancée entre le droit du renseignement et le droit du numérique dans leurs réponses aux enjeux juridique de la numérisation du renseignement. Deux affirmations en apparence opposées mais qui se complètent en réalité peuvent être soutenues :

- d'abord, notre analyse semble faire émerger une autonomisation du droit du renseignement numérique par rapport au droit du renseignement lui-même et par rapport au droit du numérique (**Première partie**) ;
- ensuite, le droit du numérique apparaît s'affirmer dans son application au renseignement pour compléter l'appréhension encore limitée du cyberspace par le droit du renseignement numérique (**Seconde partie**).

¹ Sur ce point, voir notamment A. Latil, *Le droit du numérique. Une approche par les risques*, Hors collection Dalloz, mars 2023.

² Cf. S. -Y. Laurent, *Chapitre 1. Les Etats-Unis, les Etats et les faux-semblants de la fin de l'internet mondial*, in *Conflits, crimes et régulations dans le cyberspace*, vol. 4, ISTE, 2021, p. 34.

³ Cf. S. -Y. Laurent, *Liberté et sécurité dans un monde anomique de données*, 22^{ème} rapport d'activité de la CNCIS, 2013-2014, p. 11 à 18.

PREMIERE PARTIE

UNE AUTONOMISATION DU DROIT DU RENSEIGNEMENT NUMERIQUE

« Big Brother is watching you »

1984, George Orwell

La fameuse expression de George Orwell ne peut que nous venir à l'esprit lorsque l'on évoque l'idée d'un droit du renseignement numérique autonome en droit français, notamment parce que cette idée se traduit dans les faits par le renforcement continu des moyens numériques de surveillance depuis les années 1990 (**Titre I**). Pour autant, il convient de souligner que l'émergence d'un droit du renseignement numérique apporte également des garanties juridiques spécifiques pour concilier des missions secrètes de sécurité nationale avec le respect du droit à la vie privée à l'ère du numérique (**Titre II**).

TITRE I

LE RENFORCEMENT DES MOYENS NUMERIQUES DE RENSEIGNEMENT

Dans le domaine du numérique, les évolutions du droit du renseignement ont permis de renforcer significativement les moyens techniques d'investigation des services de renseignement. Plus particulièrement, le droit du renseignement tend à devenir le cadre juridique général de la légalisation des moyens de recherche des renseignements (**Chapitre I**) et des moyens d'exploitation des renseignements (**Chapitre II**).

CHAPITRE I

LA RECHERCHE NUMERIQUE DES RENSEIGNEMENTS

La loi du 24 juillet 2015 relative au renseignement a marqué un véritablement tournant dans le dispositif légal de recherche et de collecte des renseignements par des moyens numériques. On peut observer une nette augmentation des capacités numériques entre le dispositif antérieur à la loi relative au renseignement (**Section I**) et celui postérieur à 2015 (**Section II**)

SECTION I : L'insuffisant dispositif antérieur à 2015

Considérée comme « l'acte 1 » de l'encadrement des activités de renseignement en France¹, la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques est également le premier texte à consacrer juridiquement des techniques de renseignement. Ce texte est venu encadrer les « interceptions de sécurité », c'est-à-dire les écoutes des conversations des communications électroniques² et, plus particulièrement pour l'époque, les écoutes téléphoniques (les « zonzons » ou « zonz » en jargon policier ou du renseignement)³.

Bien que les dispositions de la loi du 10 juillet 1991 aient été adaptées, autant que possible, dans leur application aux évolutions technologiques dans le domaine des communications (§1), les développements du numérique et la poussée du terrorisme à partir des années 2000 ont conduit à remettre progressivement en cause les limites du dispositif législatif mis en place depuis

¹ En ce sens, voir O. Forcade, *Retour historique sur les institutions et les pratiques du renseignement français de 1991 à 2015*, in *Le droit du renseignement*, op. cit., p. 22 et suivantes.

² « On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique » (article L. 32-1° du code des postes et des communications électroniques).

³ A ce sujet, voir H. Moutouh et J. Poirot, *Ecoute*, in *Dictionnaire du renseignement*, op. cit., p.323 et suivantes.

1991 jusqu'à l'adoption des lois relatives au renseignement des 24 juillet¹ et 30 novembre 2015² (§2).

§1. L'adaptation de la loi du 10 juillet 1991 aux développements des communications électroniques

Dans un contexte de généralisation des communications électroniques, la légalisation des « interceptions de sécurité » était devenue une incontournable. Cependant, les dispositions consacrées par la loi du 10 juillet 1991 ont dû être interprétées dans leur application pour répondre aux évolutions technologiques sans réellement parvenir à faire face à la numérisation.

A – La légalisation incontournable des « interceptions de sécurité »

La pratique des écoutes est aussi ancienne que le développement du téléphone et il n'a pas fallu attendre la loi du 10 juillet 1991 pour qu'elle fasse l'objet d'un encadrement en France³. En effet, la généralisation des écoutes dans les services de renseignement dans les années 1960 a incité le gouvernement de l'époque à les centraliser auprès d'un service placé sous la responsabilité du Premier ministre et à organiser un « *processus d'autorisation préalable* » par le cabinet de ce dernier⁴. Ainsi, par une décision non publiée n° 1E du 28 mars 1960 du Premier ministre⁵, Michel Debré, le « Groupement interministériel de contrôle » (GIC)⁶ s'est alors vu chargé de la mise en œuvre des « écoutes administratives », par opposition aux « écoutes judiciaires » qui sont réalisées dans le cadre de la procédure pénale. Notons qu'à cette époque, les écoutes

¹ Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

² Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

³ A ce sujet, voir H. Moutouh et J. Poirot, op. cit., p.323 et suivantes.

⁴ A ce sujet, voir B. Warusfel, *La légalisation du renseignement en France (1991-2015)*, in Sébastien Laurent & Bertrand Warusfel, Transformations et réformes de la sécurité et du renseignement en Europe, Presses Universitaires de Bordeaux, 2016, pp. 187-213.

⁵ Sur ce point, voir Commission nationale de contrôle des interceptions de sécurité, *1er rapport d'activité 1991-1992*, La documentation Française, 1993, pp. 13 à 15.

⁶ Sur le GIC, voir notamment H. Moutouh et J. Poirot, *GIC (Groupement Interministériel de contrôle)*, op. cit., p.433 et suivantes.

judiciaires n'étaient également pas reconnues par la loi mais leur existence légale s'était peu à peu affirmée par la jurisprudence judiciaire¹.

Cependant, qu'elles soient administratives ou judiciaires, les écoutes demeuraient dans un « vide législatif »² difficilement tenable. Pour les services de renseignement, cette situation pouvait, par exemple, exposer leurs agents à des poursuites pénales sur le fondement de l'article 368 de l'ancien code pénal sanctionnant les écoutes « sauvages » portant atteinte à la vie privée³. Plus inquiétant, la situation apparaissait contradictoire avec la jurisprudence de la Cour européenne des droits de l'homme (CEDH) sur la protection de la vie privée. En 1978, la Cour a d'abord reconnu que les écoutes secrètes des télécommunications réalisées par les autorités allemandes constituaient une ingérence dans le respect du droit à la vie privée et des correspondances garanti par l'article 8 de la Convention européenne des droits de l'homme (Conv.EDH)⁴. Par la suite, dans un arrêt du 2 août 1984 condamnant les interceptions des télécommunications prévues en droit anglais et gallois⁵, la Cour a pu préciser sa position en affirmant la nécessité d'encadrer les écoutes par une loi suffisamment claire sur les « circonstances » et les « conditions » qui permettent à la puissance publique de s'ingérer dans la vie privée et dans les correspondances des personnes surveillées⁶.

Conscient de la nécessité de remédier au vide législatif français, les praticiens et la doctrine de l'époque s'étaient montrés pourtant favorables à l'élaboration d'une loi⁷. Dès 1973, un rapport présidé par le sénateur Pierre Marcilhacy sur les « services administratifs procédant aux écoutes téléphoniques » préconisait ainsi de « *légaliser les écoutes administratives* » et

¹ En ce sens, voir L. -E. Pettiti, *A propos de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications*, AJDA 1992, p. 35.

² En ce sens, voir A. Coeuret, *Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications*, RTD Civ. 1991, p. 824.

³ Ibid.

⁴ CEDH, Plén., 6 septembre 1978, *affaire Klass et autres c. Allemagne* (Requête n° 5029/71).

⁵ CEDH, Plén., 2 août 1984, *affaire Malone c. Royaume-Uni* (Requête n° 8691/79).

⁶ Ibid., § 67.

⁷ A ce sujet, voir J. Pradel, *Un exemple de restauration de la légalité criminelle : le régime des interceptions de correspondances émises par la voie des télécommunications*, Recueil Dalloz 1992, p. 49.

d'instituer « *un contrôle a priori exercé par des autorités judiciaires* »¹. Cependant, aucune suite n'a été donnée à ces propositions. Il en a été de même pour le rapport non public de 1982 de la commission Schmelck² dont les préconisations législatives ont été tout de même reprises lors de l'adoption de la loi du 10 juillet 1991.

Il a fallu attendre, trente ans après la création du GIC, deux arrêts de la CEDH du 24 avril 1990 pour que la France décide de réellement légaliser les interceptions des télécommunications. Dans les affaires *Huvig* et *Kruslin*, la Cour de Strasbourg a réaffirmé sa jurisprudence sur les écoutes en condamnant les insuffisances du droit français en matière d'écoutes judiciaires³. Un an après les deux arrêts, le gouvernement du Premier ministre, Michel Rocard, décide de légiférer et souhaite tirer toutes les conséquences de la condamnation de la CEDH en déposant un projet de loi portant non seulement sur les écoutes judiciaires mais aussi sur les écoutes administratives. Discuté en procédure d'urgence, le projet est adopté sous la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications⁴.

Tout en garantissant le secret des correspondances électroniques dans son premier article⁵, la loi consacre un cadre juridique pour les écoutes administratives dans ses dispositions relatives aux « interceptions de sécurité »⁶. Selon la loi, ces dernières sont soumises à un régime d'autorisation préalable du

¹ Cf. P. Marcilhacy, Président, et R. Monory, Rapporteur, *Rapport fait au nom de la Commission de contrôle des services administratifs procédant aux écoutes téléphoniques*, Sénat, 23 octobre 1973, p. 57 et suivantes.

² Dans deux lettres de mission du 21 juillet et 1^{er} octobre 1981, le Premier ministre Pierre Mauroy a chargé Robert Schmelck, Premier président de la Cour de cassation, de rendre un rapport sur les écoutes judiciaires, administratives et sauvages. Le 25 juin 1982, le rapport fut remis au Premier ministre et a fait l'objet d'une première publication dans le 1^{er} rapport d'activité (1991-1992) de la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

³ CEDH, 24 avril 1990, *affaires Huvig c. France* (Requête n° 11105/84) et *Kruslin c. France* (Requête n° 11801/85).

⁴ Voir le dossier législatif « *Droits de l'homme et libertés publiques* » du Sénat relatif à la loi du 10 juillet 1991, <http://www.senat.fr/dossier-legislatif/a90912068.html>.

⁵ Notons qu'en 1991 les correspondances visées par la loi concernaient les correspondances téléphoniques par poste fixe, radiotéléphone, visiophone ou encore par télécopie, transmission de données informatiques par câble coaxial, fibres optiques ou voie hertzienne (cf. M. Rudloff, *Rapport sur le projet de loi, adopté par l'Assemblée nationale après déclaration d'urgence, relatif au secret des correspondances émises par la voie des télécommunications*, Sénat, 19 juin 1991, p. 5).

⁶ Articles 3 à 19 de la loi du 10 juillet 1991 codifiés en 2012 au sein du code de la sécurité intérieure par l'ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure aux articles L241-1 et suivants et finalement abrogés par la loi n° 2015-912 du 24 juillet 2015.

Premier ministre et à l'avis d'une autorité administrative indépendante (AAI) spécialement créée pour le contrôle des écoutes administratives, la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Plus concrètement, les services de renseignement des ministères de la défense, de l'intérieur et des douanes (économie) souhaitant mettre en œuvre des écoutes devaient en faire la demande auprès de leur ministre de tutelle en justifiant le caractère exceptionnel de la mesure et sa finalité qui devait avoir pour objet la recherche « *des renseignements intéressant 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* »¹. La demande était ensuite transmise par le ministre concerné au Premier ministre qui en accordait ou non l'autorisation après avis de la CNCIS². Comme prévu depuis 1960, la loi a centralisé l'exécution des interceptions auprès du Premier ministre et donc du GIC³.

Les opérations nécessaires à la mise en œuvre des interceptions de sécurité au sein des entreprises de télécommunications devaient être réalisées par leurs « agents qualifiés » sur ordre du ministre chargé des communications électroniques⁴. La loi du 10 juillet 1991 a ainsi juridiquement affirmé la collaboration entre les acteurs des télécommunications et le renseignement français.

Par ailleurs, soulignons que la loi du 10 juillet 1991 a également consacré deux autres mesures de surveillance en lien avec les interceptions des communications électroniques. D'une part, l'article 20 de la loi a prévu une « exception hertzienne » aux régimes judiciaire et administratif des écoutes. Cette exception avait pour objet de permettre aux services de renseignement, seulement « *aux fins de défense des intérêts nationaux* », de surveiller et de contrôler, sans autorisation ni contrôle préalable, des transmissions empruntant les ondes

¹ Articles 3 et 4 de la loi du 10 juillet 1991.

² Si les dispositions de la loi du 10 juillet 1991 ne prévoyaient pas un avis préalable de la CNCIS, ce dernier s'est imposé dans la pratique du contrôle de la Commission jusqu'à l'adoption de la loi renseignement de 2015 (cf CNCIS, *23^{ème} rapport d'activité 2014-2015*, p. 74).

³ Décret n° 2002-497 du 12 avril 2002 relatif au groupement interministériel de contrôle.

⁴ Article 11 de la loi du 10 juillet 1991.

électromagnétiques¹. Elle se justifiait du fait de la difficulté d'intercepter ce type de communications en raison du « *caractère aléatoire des fréquences utilisées* », ce qui ne permettait pas de les considérer comme des communications individualisables au même titre que celles concernées par le régime des écoutes judiciaires ou administratives².

D'autre part, l'article 22 de la loi du 10 juillet 1991 permettait aux services de renseignement de recueillir « *les informations ou documents* » nécessaires à la « *réalisation et l'exploitation des interceptions autorisées par la loi* ». Ces informations ou documents recueillis auprès des acteurs concernés correspondent aux données techniques des communications.

Pendant dix ans, les dispositions législatives relatives aux techniques de renseignement issues de la loi de 1991 resteront inchangées mais leur application ne manquera pas de faire l'objet d'une « jurisprudence » tenant compte des évolutions technologiques.

B – L'application des dispositions de la loi de 1991 aux évolutions technologiques

La multiplication des différents moyens de communications électroniques a rapidement conduit la CNCIS à préciser dans sa « jurisprudence » « *que les garanties et les droits prévues par la loi du 10 juillet 1991 sont attachées à la personne et non à ses moyens de communications* », c'est-à-dire que l'autorisation d'une interception de sécurité devait faire référence à des personnes ciblées et non à des moyens de communications³. On notera que cette solution a eu pour avantage de ne pas augmenter le contingentement des écoutes et de maintenir leur caractère exceptionnel.

La « jurisprudence » de la CNCIS a également permis d'adapter les dispositions de la loi de 1991 au déploiement des communications hertziennes et de la téléphonie mobile. D'abord, elle a indiqué que la « surveillance hertzienne » se rattachait uniquement à une mission générale de police des ondes (1er rapport

¹ Cf. CNCIS, 20^{ème} rapport d'activité 2011-2012, p. 43.

² En ce sens, voir P. Chambon, *Analyse et commentaire de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications*, Recueil Dalloz 1991, p. 173.

³ En ce sens, voir CNCIS, 22^{ème} rapport d'activité années 2013-2014, La documentation Française, 2015, p. 75.

d'activité 1991-1992) et qu'elle ne pouvait être utilisée à des fins d'interceptions de sécurité¹. Ensuite, face à la généralisation des téléphones portables, la CNCIS a tenu à affirmer, dès 1998, la « *primauté du principe de libertés publiques sur l'évolution technique* » en considérant que les communications sans fil qui n'entraient pas dans le champ d'application de l'exception hertzienne étaient soumises au régime des interceptions de sécurité². En 2009-2010, la CNCIS a également fait part tant aux opérateurs qu'aux services de renseignement de sa position sur l'irrecevabilité des demandes fondée sur les dispositions de l'article 20 pour collecter les relevés téléphoniques d'une personne suite à une demande formulée en ce sens par l'ancien directeur de la Direction centrale du renseignement intérieure (DCRI), Bernard Squarcini, dans le cadre de l'affaire dite des « fadettes »³. Ce dernier a d'ailleurs été condamné par le Tribunal correctionnel de Paris en 2014 pour collecte déloyale de données personnelles, le juge pénal confortant alors la position de la CNCIS⁴. Même si la Commission a su préciser les contours de l'article 20, il n'en demeure pas moins que « l'affaire des fadettes » témoigne du flou qui entourait le régime de la surveillance hertzienne de la loi du 10 juillet 1991. Il n'est alors pas surprenant que, dans son dernier rapport annuel 2013-2014, la CNCIS s'est montrée très critique à l'égard de ce type de surveillance au point de recommander sa suppression en jugeant le dispositif obsolète⁵.

Enfin, les dispositions de l'article 22 de la loi de 1991 relatives aux données techniques des communications ont fait l'objet d'une interprétation pragmatique pour répondre aux besoins des services de renseignement. On notera préalablement que le législateur de 1991 avait pris soins de préciser que ce recueil de données ne constituait pas une violation de la protection des données personnelles garantie par la loi informatique et libertés de 1978⁶. Néanmoins, ce

¹ Cf. CNCTR, *1^{er} rapport d'activité annuel 2015-2016*, p. 48 à 51.

² Cf. CNCIS, *19^{ème} rapport d'activité 2010*, p. 15 et 16.

³ Sur cette affaire, voir H. Moutouh et J. Poirit, *Fadette*, in *Dictionnaire du renseignement*, op. cit., p. 377 et suivantes.

⁴ Jugement du tribunal correctionnel de Paris du 8 avril 2014, n° 110010023019.

⁵ Cf. CNCIS, *22^{ème} rapport d'activité 2013-2014*, p. 128 à 130.

⁶ Al. 2 de l'article 22 de la loi du 10 juillet 1991 : « *La fourniture des informations ou documents visés à l'alinéa précédent ne constitue pas un détournement de leur finalité au sens de l'article 44 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* ».

recueil a pu apparaître comme un empiètement dans la protection des données personnelles voire comme une atténuation de la protection¹. Pour autant, le dispositif de la loi du 10 juillet 1991 prévoyait en réalité que l'autorisation d'interception – judiciaire ou administrative – valait autorisation de recueil des données techniques des communications concernées. Dans son application, le dispositif permettait aux services de renseignement de recueillir les données dans deux cas de figure² :

- dans le cadre d'un projet d'interception de sécurité afin de confirmer ou d'exclure la mesure de surveillance. Ici, la CNCIS admettait seulement le recueil des données d'identification et de trafic. Soulignons que ce cas de figure était particulièrement utile en raison du contingentement des interceptions prévu par la loi³ ;
- durant toute la durée d'une interception de sécurité autorisée pour son exploitation comme explicitement prévu par la loi. Dans ce cas, l'ensemble des données connexion pouvaient être recueillies.

Sur recommandations de la CNCIS, le recueil a été confié au GIC, qui avait pour rôle de centraliser, traiter et contrôler *a priori* les demandes des services, et la CNCIS assurait le contrôle *a posteriori* dans les mêmes conditions que pour les interceptions⁴.

Ces adaptations du cadre juridique des moyens de recherche des renseignements à l'évolution technique ne suffiront pas à pallier les limites du dispositif prévu par la loi de 1991 face à la numérisation.

¹ En ce sens, voir A. Coeuret, *Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications* op. cit., p. 824.

² Cf. CNCIS, *20^{ème} rapport d'activité 2011-2012*, p. 63 et suivantes.

³ Article 5 de la loi du 10 juillet 1991 : « Le nombre maximum des interceptions susceptibles d'être pratiquées simultanément en application de l'article 4 est arrêté par le Premier ministre. La décision fixant ce contingent et sa répartition entre les ministères mentionnés à l'article 4 est portée sans délai à la connaissance de la Commission nationale de contrôle des interceptions de sécurité ».

⁴ Cf. CNCIS, *22^{ème} rapport d'activité 2013-2014*, p. 93 et suivantes.

C – Les limites de la loi du 10 juillet 1991 face à la numérisation

Bien que la loi du 10 juillet 1991 ait constitué une avancée majeure dans l'encadrement des moyens techniques d'enquête et, plus largement, dans l'encadrement des activités du renseignement, elle ne permettait pas d'appréhender les développements de la numérisation des années 2000.

Cependant, la France a attendu les attentats de Madrid de mars 2004 et de Londres en juillet 2005 pour véritablement admettre que la loi de 1991 se révélait insuffisante pour répondre aux besoins des services de renseignement confrontés à la montée en puissance du terrorisme international et de l'utilisation d'Internet.

En 2001, dans le tumulte des attentats du 11 septembre qui ont bouleversé les Etats-Unis, le législateur français s'était pourtant efforcé de s'adapter, aussi vite que possible, au « virage numérique » des années 2000 en matière pénale. Anticipant l'entrée en vigueur de la Convention sur la cybercriminalité de Budapest¹, la LSQ du 15 novembre 2001 a ainsi organisé la mise à disposition des « données de trafic »² conservées par les opérateurs et fournisseurs d'accès à Internet (FAI) à l'autorité judiciaire, en dehors d'une interception, et « *pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales* » selon l'article L. 32-3-1 du code des postes et télécommunications³.

En revanche, rien n'a été prévu pour organiser la collecte de ces données par le renseignement, le législateur persistant ainsi son retard dans ce domaine. On pouvait comprendre la volonté de l'Etat de conserver un usage discrétionnaire du renseignement mais, en ne reconnaissant légalement que les interceptions de sécurité, il n'était pas certain que la situation soit de nature à sécuriser

¹ Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest, le 23 novembre 2001, et entrée en vigueur le 1^{er} juin 2006 en France.

² Les données de trafic désignent ici celles définies par la Convention sur la cybercriminalité de 2001 de Budapest, c'est à dire « *toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent* » (d de l'article 1). De manière assez semblable, l'article L. 32-18° du code des postes et des communications électroniques pose la définition suivante : « *on entend par données relatives au trafic toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* ».

³ En ce sens, voir B. Warusfel, op. cit., Droit et Défense, 2002/1, pp. 17-22.

juridiquement les activités des services ni à garantir les libertés à l'heure de l'Internet¹.

§2. La remise en cause progressive du dispositif antérieur à 2015

Malgré les interventions du législateur pour compléter le dispositif de 1991 afin de faire face à la numérisation des sociétés, il a été jugé nécessaire d'adopter une véritable loi relative au renseignement, notamment pour encadrer les nouveaux moyens numériques de collecte de données.

A – Les dispositions complémentaires au dispositif de 1991

Dans trois lois, le législateur est venu compléter le dispositif de 1991 en adoptant des dispositions portant sur le déchiffrement des communications et les données de connexion.

1. La loi du 15 novembre 2001 relative à la sécurité quotidienne

On relèvera tout d'abord que le législateur a tenu à adapter les interceptions de sécurité à la libéralisation du chiffrement des communications². En effet, les dispositions de la loi du 15 novembre 2001 relative à la sécurité quotidienne (LSQ) ont inséré une obligation de remise de clé de chiffrement ou, si possible, de déchiffrement à la charge des fournisseurs de prestations de cryptologie³. Ainsi, l'encadrement des interceptions de sécurité s'est accompagné d'une réglementation spécifique au renseignement applicable aux acteurs des télécommunications qui est autonome du droit du numérique.

2. La loi du 23 janvier 2006 relative à la lutte contre le terrorisme

Ensuite, le législateur a surtout tenu à permettre aux services de renseignement de collecter les données de connexion. De manière générale, ces données regroupent l'ensemble des traces d'une communication électronique, c'est-à-dire les informations sur « l'émetteur et le destinataire d'une

¹ En ce sens, voir B. Warusfel, *Le renseignement, dimension majeure de l'action publique dans une société d'information*, in *Le renseignement contemporain – Aspects politiques et juridiques*, Éditions L'Harmattan, 2003, pp. 9-35.

² En ce sens, voir B. Warusfel, *"Procédure pénale et technologies de l'information : de la Convention sur la Cybercriminalité à la Loi sur la sécurité quotidienne"*, Droit et Défense, 2002/1, pp. 17-22.

³ Article 11-1 de la loi du 10 juillet 1991 créé par l'article 31 de la loi n° 2001-1062 du 15 novembre 2001.

*communication ainsi que sa date, son heure et sa durée, les numéros de téléphones appelés ou les sites consultés, ou encore l'équipement utilisé ainsi que le numéro de téléphone correspondant, l'adresse IP ou la géolocalisation »*¹. Elles ne portent donc pas sur le contenu d'une correspondance électronique ou sur des informations consultées en ligne. L'accès à ces données pour les services de renseignement s'est révélé indispensable pour s'adapter à l'utilisation croissante des outils numériques et de l'Internet par les réseaux terroristes², ce qui a conduit le législateur à consacrer, à titre expérimental³, cette technique de collecte des renseignements à l'article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

Uniquement prévu pour la prévention des actes de terrorismes, l'autorisation de cette collecte s'organisait selon deux types de mesures :

- une première mesure portait sur la collecte des « *données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* »⁴. Elle concernait les traditionnels opérateurs de communications électroniques et les FAI mais aussi les professionnels offrant au public une connexion à Internet⁵, ce qui impliquait les « cybercafés » et les « bornes Wi-Fi »⁶ accessibles dans des hôtels, des restaurants ou des aéroports par exemple ;

¹ A ce sujet, voir H. Moutouh et J. Poirot, *Données de connexion*, op. cit., p. 289 et suivantes.

² En ce sens, voir E. Diard, rapporteur, et J. Dray, co-rapporteur, *Rapport d'information sur la mise en application de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, Assemblée nationale, 5 février 2008, p. 17 et suivantes.

³ Article 32 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

⁴ Al. 2 de l'article L. 34-1-1 du code des postes et des communications électroniques.

⁵ Al. 1 de l'article L. 34-1-1 du code des postes et des communications électroniques.

⁶ Circulaire du 21 juillet 2006 relative à l'application de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relative à la sécurité et aux contrôles frontaliers.

- une seconde mesure portait sur la collecte des données de connexion permettant d'identifier les personnes à l'origine d'un contenu mis en ligne qui sont conservées par les FAI et les hébergeurs¹.

En dépit du fait que la mise en œuvre de la seconde mesure a été retardée jusqu'en 2011², en raison notamment des difficultés liées à la définition des données concernée³, les deux mesures étaient mises en œuvre dans les mêmes conditions. Les textes organisaient une procédure d'approbation préalable des demandes d'accès aux données de connexion par une décision d'une « personnalité qualifiée » du ministère de l'intérieur ainsi qu'un contrôle *a posteriori* exercé par la CNCIS⁴.

Les demandes, qui devaient émaner des agents habilités des services anti-terroristes du renseignement intérieur⁵, étaient centraliser dans une plateforme technique de l'Unité de coordination de la lutte anti-terroriste (UCLAT)⁶. Cette dernière était chargée d'effectuer un premier examen des demandes avant de les soumettre à la personnalité qualifiée qui prenait une décision de nature contraignante soit favorable, soit défavorable, soit pour demander des informations complémentaires. En cas d'approbation, l'UCLAT saisissait les acteurs du numérique concernés qui étaient tenus de lui transmettre les données demandées sans délai et de manière sécurisée. Cette transmission pouvait être prévue par convention ou par arrêté. Par ailleurs, notons que les surcoûts supportés par les acteurs du numérique pour satisfaire les demandes d'accès aux données pouvaient faire l'objet d'une compensation financière par l'Etat. Les données recueillies étaient ensuite transmises par l'UCLAT au service demandeur

¹ II bis de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

² Décret n° 2011-219 du 25 février 2011 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.

³ A ce sujet, voir E. Diard, rapporteur, et J. Dray, co-rapporteur, op. cit., Assemblée nationale, 5 février 2008, p. 26 et suivantes.

⁴ Décret n° 2006-1651 du 22 décembre 2006 pris pour l'application du I de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers et Décret n° 2011-219 du 25 février 2011.

⁵ Les services de renseignement légalement autorisés à demander des accès aux données de connexion étaient notamment la DST, les RG, puis la DCRI à partir de 2008, et la DRPP.

⁶ Arrêté du 31 mars 2006 pris pour l'application de l'article 33 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

qui pouvait les exploiter selon la finalité justifiant leur collecte. Elles étaient également enregistrées et conservées pendant trois ans maximums dans des fichiers du ministère de l'intérieur¹.

Le dispositif prévu par la loi de 2006 a été jugé satisfaisant dans son ensemble, tant du point de vue du droit que dans de la pratique. En effet, le Conseil constitutionnel, saisi par soixante sénateurs, avait d'abord considéré que les dispositions de l'article 6 n'étaient pas contraire à la Constitution en raison de leur utilité dans la lutte contre le terrorisme et des garanties qu'elles présentaient en matière de protection de la vie privée². Notons toutefois que la Conseil constitutionnel a censuré l'empiètement du pouvoir de police administrative dans celui du pouvoir judiciaire prévu par la référence à la « répression » des actes de terrorisme dans la rédaction initiale de l'article 6. Ensuite, il a été relevé que la rapidité et la réactivité du dispositif mis en place répondait aux besoins des services tout en assurant une qualité des relations entre l'UCLAT et les acteurs du numérique³. Ces considérations expliquent notamment que l'application de l'expérimentation du dispositif jusqu'au 31 décembre 2008 fut prorogée une première fois jusqu'au 31 décembre 2012⁴, puis une seconde fois jusqu'au 31 décembre 2015⁵.

Il reste que l'application des modalités des accès aux données de connexion ont tout de même fait l'objet de critiques. A plusieurs reprises, la CNIL n'a pas manqué d'observer que le dispositif de 2006 présentait des carences en matière de protection des données personnelles. Elle avait notamment relevé que les textes ne prévoyaient pas d'habilitation des employés des acteurs du numérique

¹ Seul le ministère de l'intérieur est ici mentionné par souci de simplification. Initialement, les données recueillies étaient enregistrées et conservées dans des fichiers du ministère de l'intérieur et du ministère de la défense selon que les demandes émanaient des services de police ou de gendarmerie nationales (Décret n°2006-1651 du 22 décembre 2006). Cette distinction a été abandonnée (Décret n° 2010-774 du 8 juillet 2010 modifiant les parties réglementaires du code des postes et des communications électroniques, du code de la route et du code monétaire et financier) suite à la loi n° 2009-971 du 3 août 2009 relative à la gendarmerie nationale qui a rattaché cette dernière au ministère de l'intérieur.

² Décision n° 2005-532 DC du 19 janvier 2006.

³ Sur ce point, voir E. Diard, rapporteur, et J. Dray, co-rapporteur, op. cit., Assemblée nationale, 5 février 2008, p. 25 et 26.

⁴ Loi n° 2008-1245 du 1er décembre 2008 visant à prolonger l'application des articles 3,6 et 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

⁵ Loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme.

impliqués dans la collecte des données de connexion¹. Elle s'était également inquiétée de l'absence de déclaration préalable des fichiers mis en œuvre par les acteurs du numérique et le ministère de l'intérieur dans l'application du dispositif de 2006².

Le principal point de crispation a concerné la collecte des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. L'application de cette mesure a été attaquée devant le Conseil d'Etat dans le cadre d'un recours pour excès de pouvoir par des acteurs du numérique dont la société française d'hébergement OVH. Les requérants soutenaient notamment que la mesure méconnaissait les règles relatives à la protection des données personnelles, ce que le Conseil d'Etat a rejeté, dans une décision de 2013, en qualifiant la conservation et la communication des données concernées de traitement intéressant la sûreté de l'Etat³. La haute juridiction administrative a ainsi considéré que les dérogations aux règles relatives à la protection des données personnelles prévues par la mesure étaient justifiées. Notons qu'en 2011, le Conseil d'Etat avaient également rejeté une requête en « référé liberté » qui soutenait que la mesure portait une atteinte à la liberté d'expression, à la liberté d'opinion et à la liberté d'entreprendre⁴.

Remettant particulièrement en cause l'anonymat sur Internet pour les besoins de la lutte anti-terroriste, l'introduction des accès aux données de connexion par la loi du 23 janvier 2006 a suscité des inquiétudes sur les risques d'un passage progressif vers un « *Big Brother* »⁵. Ces inquiétudes se sont d'ailleurs renouvelées lors de l'adoption de la loi de programmation militaire du 18 décembre 2013 qui a simplifié et renforcé le régime juridique des accès aux données de connexion pour les services de renseignement.

¹ Délibération 2006-219 du 28 septembre 2006 portant avis sur le projet de décret pris pour l'application des I et II de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

² Sur ce point, voir E. Diard, rapporteur, et J. Dray, co-rapporteur, op. cit., Assemblée nationale, 5 février 2008, p. 24 et 27.

³ CE, 20 novembre 2013, *M. J...* (requête n° 347349), *association Internet sans frontière* (requête n° 348851) et *société OVH* (requête n° 348891).

⁴ CE, 21 mars 2011, *M. Joseph A* (requête n° 347350).

⁵ En ce sens, voir E. A. Caprioli, *Lutte contre le terrorisme – Les technologies de l'information et la lutte anti-terroriste*, Communication Commerce électronique n° 5, Mai 2006.

3. La loi de programmation militaire du 18 décembre 2013

Tout en consacrant la « politique publique du renseignement »¹, la loi de programmation militaire (LPM) de 2014 à 2019 du 18 décembre 2013 a continué de renforcer le régime juridique des accès administratifs aux données de connexion en permettant notamment aux services de renseignement de recourir à la géolocalisation en temps réel. Initialement, l'encadrement de cette dernière technique constituait la seule mesure prévue par le projet de loi de 2013 en matière de recueil des données de connexion². Si la loi du 23 janvier 2006 avait prévu la possibilité de recueillir les données techniques de localisation d'un appareil, ce recueil s'effectuait cependant en temps différé. Le dispositif de 2006 ne pouvait donc pas servir de fondement à la géolocalisation en temps réel, d'autant plus que la CEDH avait rappelée en 2010 que cette technique devait faire l'objet d'une « *loi particulièrement précise* »³. Suivant les préconisations de clarification du rapport d'information sur l'évaluation du cadre juridique des services de renseignement des députés Jean-Jacques Urvoas et Patrice Verchère⁴, l'article 13 du projet de loi de 2013 a ainsi souhaité mentionner précisément le recueil en temps réel des données de géolocalisation dans le dispositif de 2006⁵. Cependant, le projet fut amendé par le Sénat pour finalement « *refondre le régime*

¹ Article 12 de la loi n° 2013-1168 du 18 décembre 2013.

² Sur ce point, voir J. - L. Carrère, *Rapport fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur le projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, Sénat, 8 octobre 2013, p. 176 et suivantes.

³ CEDH, 2 septembre 2010, *affaire Uzun c. Allemagne* (requête n° 35623/05).

⁴ Cf. J. - J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, Assemblée nationale, 14 mai 2013, p. 48 et 49.

⁵ Article 13 du projet de loi : « I. - Le code des postes et des communications électroniques est ainsi modifié : 1° Au V de l'article L. 34-1, après les mots : « et du IV » sont ajoutés les mots : « du présent article et du premier alinéa de l'article L. 34-1-1 » ; 2° Le premier alinéa de l'article L. 34-1-1 est remplacé par un alinéa ainsi rédigé : « Afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au II de l'article L. 34-1 la communication des données traitées par les réseaux ou les services de communications électroniques de ces derniers, après conservation ou en temps réel, impliquant le cas échéant une mise à jour de ces données. » II. - Au premier alinéa du II bis de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, sont ajoutés les mots : « après conservation de ces données ou en temps réel ». III. - Aux articles L. 222-2 et L. 222-3 du code de sécurité intérieure, après les mots : « données conservées » sont ajoutés les mots : « et traitées ».

juridique de l'accès administratif aux données de connexion en le rapprochant de celui relatif aux interceptions de communication issu de la loi du 10 juillet 1991 »¹.

En effet, deux régimes d'accès administratifs aux données de connexion coexistaient en 2013 :

- le régime de l'article 22 de la loi du 10 juillet 1991² qui autorisait l'accès aux données d'identification et de trafic, sur décision du Premier ministre, pour l'ensemble des services de renseignement et pour les mêmes finalités que les interceptions de sécurité ;
- le régime de la loi du 23 janvier 2006 qui autorisait l'accès à l'ensemble des données de connexion, sur décision de la « personnalité qualifiée » du ministère de l'intérieur, pour le renseignement intérieur et pour les seuls besoins de la prévention du terrorisme.

Notons que lors des débats parlementaires sur la loi du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme, il avait été déjà émis le souhait d'un alignement des deux régimes sur celui de l'article L. 244-2 et donc d'une unification du régime des interceptions et des accès aux données de connexion (centralisation auprès du GIC et contrôle transverse de la CNCIS)³. Ces préconisations ont été reprises dans différents rapports parlementaires de 2013 relatifs au cadre juridique du renseignement⁴. Néanmoins, cette solution n'a pas été entièrement retenue par la loi de programmation militaire de 2013.

L'article 20 de la loi de programmation militaire de 2013, qui remplace l'article 13 du projet de loi, est donc venu mettre un terme à l'expérimentation de la loi du 23 janvier 2006 en aménageant un tout nouveau dispositif d'accès administratif aux données de connexion dont l'entrée en vigueur était prévue pour le 1^{er} janvier 2015. Ce nouveau dispositif, codifié aux articles L. 246-1 à L. 246-5

¹ Cf. J. -L. Carrère, *Rapport sur le projet de loi, modifié par l'Assemblée nationale, relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, Sénat, 4 décembre 2013, p. 15 et 16.

² Dispositions codifiées à l'article L. 244-2 du code de la sécurité intérieure.

³ Débats au Sénat du 16 octobre 2012 et à l'Assemblée nationale du 27 novembre 2012 sur la loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme.

⁴ Cf. C. Cavard, président, et J. -J. Urvoas, rapporteur, *Rapport fait au nom de la commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés*, Assemblée nationale, 24 mai 2013, p. 50 à 52 et J. -J. Urvoas et P. Verchère, op. cit., Assemblée nationale, 14 mai 2013, p. 22 et suivantes.

du code de la sécurité intérieure, a opéré une nouvelle distinction entre deux régimes d'accès aux données de connexion : les accès « en temps différé » et ceux « en temps réel » pour la géolocalisation.

Reprenant l'idée admise par la CEDH¹ selon laquelle les accès aux données de connexion constituent une ingérence moins importante dans la vie privée que les interceptions de correspondances, la loi de programmation militaire de 2013 a élargi le dispositif de 2006 aux services de renseignement des ministères de l'intérieur, de la défense et de l'économie qui pouvaient désormais, pour les mêmes finalités que les interceptions de sécurité, être autorisés à accéder aux données de connexion, en temps différé, sur décision d'une « personnalité qualifiée » placée cette fois-ci auprès du Premier ministre. S'agissant de la géolocalisation en temps réel qui a été considérée comme plus intrusive que les accès en temps différé, l'article L. 246-3 du code de la sécurité intérieure a aligné son régime juridique sur celui des interceptions de sécurité. Autrement dit, la géolocalisation en temps réel était soumise aux mêmes conditions d'autorisation et de contrôle que les interceptions de sécurité (autorisation du Premier ministre et contrôle de la CNCIS).

En pratique, deux systèmes de recueil des données ont été mis en place dans le cadre du décret d'application du 24 décembre 2014². Le recueil des données en temps différé était réalisé par les opérateurs, FAI, professionnels offrant au public un accès à Internet et les hébergeurs. Les données collectées étaient transmises au GIC qui les mettait à disposition des services demandeurs pour exploitation.

En matière de géolocalisation en temps réel, l'article 20 de la loi de programmation militaire et son décret d'application prévoyaient un recueil sur « sollicitation du réseau » des opérateurs et une « transmission en temps réel » des données au GIC qui se chargeait, là aussi, de mettre les données à disposition des services demandeurs. La sollicitation du réseau était effectuée par l'opérateur exploitant qui adressait « *des messages « invisibles » au terminal mobile placé sous surveillance afin que celui-ci se manifeste et indique l'antenne du réseau mobile à*

¹ CEDH, 2 septembre 2010, *affaire Uzun c. Allemagne* (requête n° 35623/05), §66.

² Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.

laquelle il est rattaché à un instant « *t* »¹. Les données de localisation transmises au GIC correspondent à celles de l'antenne, ce qui implique une géolocalisation approximative du terminal de la personne surveillée. Si cette technique facilite la filature d'une personne à distance, son efficacité doit être relativisée. En effet, l'attachement de cette technique à l'appareil de la personne surveillée et l'approximation de la géolocalisation de ce dernier supposent d'accompagner la mesure d'une surveillance physique². Pour exemple, on retrouve cette combinaison de la surveillance numérique et humaine en matière de filature dans l'affaire Uzun contre Allemagne de 2010 dans laquelle la CEDH avait noté que le requérant avait fait l'objet d'une « surveillance par GPS » et d'une « surveillance visuelle » par des agents du ministère de la Protection de la Constitution de la Rhénanie-du-Nord-Westphalie et par des fonctionnaires de l'Office fédéral de la police judiciaire³. Par ailleurs, notons que si la collecte en temps réel des données de connexion a été justifiée pour les besoins de la géolocalisation afin notamment de pouvoir suivre des terroristes « *qui ne sortent de l'ombre qu'au moment de commettre un attentat* »⁴, la CNIL avait relevé que le périmètre de cette collecte ne se limitait pas seulement aux données techniques de localisation d'un terminal mais s'étendait à l'ensemble des données de connexion⁵. A ce sujet, le Secrétariat général de la Défense et de la Sécurité nationale (SGDSN) avait répondu que cette possibilité prévue par les textes avait pour objet de permettre l'adaptation des dispositions aux évolutions technologiques sans plus de précisions⁶. La CNIL avait alors regretté ce choix. En outre, elle avait tenu à souligner que le recueil sur « sollicitation du réseau » des opérateurs interdisait une collecte massive et

¹ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, 11 juin 2020, p. 81 et 82.

² A ce sujet, voir H. Moutouh et J. Poirrot, *Filature*, op. cit., p. 384 et 385.

³ CEDH, 2 septembre 2010, *affaire Uzun c. Allemagne* (requête n° 35623/05), §79.

⁴ Sur ce point, voir A. Marsaud, *rapport fait au nom de la commission des Lois de l'Assemblée nationale sur le projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, 16 novembre 2005, p. 59.

⁵ Délibération n° 2014-484 du 4 décembre 2014 portant avis sur un projet de décret relatif à l'accès administratif aux données de connexion et portant application de l'article L. 246-4 du code de la sécurité intérieure (demande d'avis n° AV 14027710).

⁶ On peut émettre l'hypothèse selon laquelle la collecte en temps réel des données de connexion envisagée par la loi de programmation militaire de 2013 aurait par exemple non seulement prévu la géolocalisation en temps réel d'une personne surveillée mais également la possibilité de connaître ses communications durant sa filature numérique.

directe des données par les services de renseignement. Cependant, les modifications apportées par la loi de programmation militaire ont suscité de vives polémiques sur la surveillance d'Internet, notamment dans un contexte marqué par les révélations d'Edward Snowden sur le programme PRISM de la *National Security Agency* (NSA)¹.

Parlementaires, institutions numériques comme le Conseil national du numérique (CNNum) ou la CNIL, entreprises privés du numérique tels que l'Association des sites internet communautaires, l'Interactive advertising Bureau (IAB) regroupant les acteurs de la publicité sur internet, la fédération Syntec² ou encore le think tank Renaissance numérique ou même le Mouvement des entreprises de France (Medef)³ n'ont pas hésité à s'opposer à l'évolution de la surveillance numérique proposées par la loi de programmation militaire. De manière générale, ils ont critiqué :

- le manque de concertation des institutions et acteurs du numérique dans l'élaboration de la loi ;
- l'élargissement de la collecte des données de connexion à l'ensemble des services de renseignement et en temps réel ainsi que l'insuffisance du contrôle ; ou encore,
- le renforcement de la participation des opérateurs et prestataires de l'Internet dans la surveillance et les risques que cette participation implique pour la confiance dans l'économie numérique française.

D'un point de vue juridique, la loi de programmation militaire a pu être considéré comme liberticide en ayant fait le choix de faire prévaloir la sécurité sur la liberté à travers l'élargissement de la surveillance numérique⁴. Pour autant, le Conseil constitutionnel n'a pas été saisi de la loi par les parlementaires. S'agissant du décret d'application, il a été critiqué comme laissant « *une trop grande liberté à*

¹ A ce sujet, voir G. Greenwald, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, Friday 7 jun 2013 et T. Berthemet, *Edward Snowden, l'homme qui fait trembler le gouvernement américain*, Le Figaro, 10 juin 2013.

² Sur ce point, voir C. Guerrier, *Les interceptions et la loi de programmation militaire*, Revue Le Lamy Droit de l'immatériel, n° 104, 1^{er} mai 2014.

³ Sur ce point, voir Q. Girard, *Vos mails, SMS, connexions internet, légalement surveillés ?*, Libération, 10 décembre 2013.

⁴ En ce sens, voir L. Marino, *Surveillance du net : un Patriot Act à la française ?*, Recueil Dalloz 2014, p. 360.

l'administration sans possibilité de contrôle effectif d'un juge »¹. Le décret fut d'ailleurs attaqué en annulation pour excès de pouvoir devant le Conseil d'Etat par les associations French Data Network, La Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs² ainsi que l'association Reporters sans frontières³. Dans cette affaire, les associations d'acteurs du numérique ont, dans un premier temps, contesté la constitutionnalité des dispositions de l'article 20 de la loi de programmation militaire de 2013 dans une question prioritaire de constitutionnalité (QPC) jugée recevable en juin 2015 par le Conseil d'Etat⁴.

Dans sa décision du 24 juillet 2015, le Conseil constitutionnel a déclaré les dispositions de la loi de programmation militaire relatives aux accès administratifs aux données de connexion conformes à la Constitution⁵. Il a ainsi jugé que le législateur avait suffisamment défini les données susceptibles d'être collectées en précisant que cette collecte porte sur les données de connexion et non pas sur les « données de contenu » d'une communication. Les Sages ont également validé la procédure de collecte des données de connexion prévue par la loi. En ce qui concerne le recueil en temps réel, le Conseil a notamment relevé, comme la CNIL, que le dispositif n'autorisait pas les services de renseignement à accéder directement au réseau des opérateurs. Par ailleurs, le Conseil constitutionnel a considéré, de manière générale, que le dispositif ne présentait pas « *une atteinte disproportionnée au droit au respect de la vie privée, aux droits de la défense, au droit à un procès équitable, y compris pour les avocats et journalistes* » (considérant 19). En ce sens, le législateur n'était pas tenu de prévoir des garanties spécifiques de nature à protéger le secret professionnel des avocats et des journalistes, d'autant plus que le Conseil a considéré que les accès aux données de connexion ne sauraient constituer une atteinte au droit au secret des correspondances et à la liberté d'expression. Notons qu'un jour auparavant, le Conseil avait validé le nouveau régime d'accès aux données de connexion issu de la loi relative au

¹ En ce sens, voir L. Milano, *Surveillance sur le net : du nouveau avec le décret du 24 décembre 2014*, Recueil Dalloz 2015, p. 616.

² Requête et mémoires n° 388134 enregistrés le 19 février et le 15 avril 2015 et le 22 janvier 2016 au secrétariat du contentieux du Conseil d'Etat.

³ Requête et mémoire n° 388255 enregistrés le 24 février et le 6 novembre 2015.

⁴ CE, 5 juin 2015, *Association French Data Network et autres* (requête n° 388134).

⁵ Décision n° 2015-478 QPC du 24 juillet 2015, *Association French Data Network et autres*.

renseignement dans sa décision n° 2015-713 DC du 23 juillet 2015. Le législateur de 2015 n'avait donc pas pu bénéficier des retours du Conseil constitutionnel sur le dispositif de 2013 mais cela n'a finalement pas posé de problème.

Dans un deuxième temps, les associations requérantes ont surtout contesté la conventionnalité du régime des accès administratifs aux données de connexion au regard du droit européen¹. Elles soutenaient que le dispositif prévu par le décret d'application du 24 décembre 2014 portait une atteinte disproportionnée au droit au respect à la vie privée, au droit à la protection des données personnelles et à la liberté d'expression garantis par les articles 8 et 10 de la Conv. EDH et les articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne (UE). Plus particulièrement, les associations soutenaient que le droit de l'Union européenne, notamment la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques², s'opposait à une « *conservation préventive des données de connexion en vue de leur réquisition administrative* »³. Ces griefs avaient pour fondement l'arrêt *Digital Rights Ireland Ltd* du 8 avril 2014 de la Cour de justice de l'Union européenne (CJUE)⁴. Dans cette décision, la CJUE avait ainsi invalidé la directive 2006/24/CE sur la conservation des données chez les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications⁵. La Cour avait considéré que la conservation généralisée et indifférenciée des données prévue par la directive litigieuse constituait « *une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans que cette ingérence soit limitée* ».

¹ Sur ce point, voir O. Henrard, *Accès aux données de connexion, blocage et déréférencement des sites : l'administration pourra agir sans recourir au juge*, Observations sous Conseil d'État, 12 février 2016, n° 388134 et n° 388255, *Association French Data Network et autres* et Conseil d'État, 15 février 2016, n° 389140 et n° 389896, *Association French Data Network et autres*, Dalloz IP/IT 2016, p. 313.

² Directive 2002/58/CE du Parlement européen et du Conseil 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 (directive vie privée et communications électroniques).

³ Sur ce point, voir O. Henrard, *op. cit.*

⁴ CJUE, 8 avril 2014, *affaires jointes C-293/12 et C-594/12 Digital Rights Ireland et Seitlinger e.a.*

⁵ Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

au strict nécessaire »¹. Cependant, le Conseil d'Etat a finalement rejeté les requêtes des associations par un arrêt du 12 février 2016². Le juge administratif a tout simplement jugé que le droit de l'Union européenne n'interdisait pas, en principe, une conservation des données pour les besoins du renseignement d'Etat et que les modalités d'accès aux données de connexion et de contrôle prévues par le droit français présentaient des garanties suffisantes au regard du droit européen.

Si la loi du 18 décembre 2013 a constitué une amélioration significative du régime des accès administratifs aux données de connexion, il reste que cette réforme était inaboutie. En effet, elle laissait perdurer deux régimes juridiques distincts selon que la demande d'accès était relative à une interception de sécurité ou non, ce qui pouvait entraîner des « *risques de contradiction et d'incohérence* »³. Ce dualisme des procédures et du contrôle prendra fin avec l'adoption de la loi relative au renseignement du 24 juillet 2015. Au-delà des accès aux données de connexion, cette dernière loi et celle du 30 novembre 2015 sur les communications internationales ont revu l'ensemble du dispositif des techniques de renseignement mises en œuvre depuis la loi du 10 juillet 1991.

B – La nécessité d'une loi relative au renseignement

Le dispositif légal de recherche et de collecte numérique des renseignements mis en place de 1991 jusqu'en 2015 reposait sur deux catégories principales de techniques :

- les interceptions de sécurité qui regroupaient les écoutes de correspondances individualisables et la surveillance et le contrôle des transmissions empruntant la voie hertzienne ;
- les accès administratifs aux données de connexion qui pouvaient être soit en temps différé, soit en temps réel (géolocalisation).

Un an après l'adoption de la loi de programmation militaire de 2013, ce dispositif a été jugé trop faible par la DPR « *pour affronter la mutation des*

¹ CJUE, communiqué de presse n° 54/14, 8 avril 2014.

² CE, 12 février 2016, *Association French Data Network et autres* (requêtes n° 388138 et n° 388255).

³ Sur ce point, voir CNCIS, *23^{ème} rapport d'activité 2014-2015*, p. 104 et suivantes.

menaces » dans son rapport d'activité pour l'année 2014¹. Cette dernière proposait d'ailleurs de permettre aux services de renseignement de recourir à de nouvelles techniques déjà consacrées en matière de police judiciaire. Il s'agissait notamment des capacités de sonorisation et de fixation d'images dans des lieux privés (microphones et caméras de surveillance par exemple)² ou encore de captation des données informatiques³.

Sur cette dernière technique, notons que le rapport de la DPR soulignait qu'il ne s'agissait pas d'un piratage informatique du système de la personne surveillée étant donné que la technique ne vise pas à contrôler le système ou à en vérifier le contenu. En effet, la mise en œuvre de cette technique vise à implanter un logiciel dédié permettant « *d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques* »⁴. Or, contrairement à ce que soulignait le rapport, le procédé constitue bien un piratage informatique au sens de l'article 323-1 du code pénal qui réprime « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement de données* ».

En outre, on peut une nouvelle fois constater le retard du renseignement sur la police judiciaire en matière de légalisation des moyens numériques d'enquête. Par ailleurs, suites aux attentats du début d'année 2015 qui ont touché la France⁵, il a été de nouveau dénoncé le manque de moyens légaux d'enquêtes

¹ Cf. J. – J. Urvoas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, DPR, 18 décembre 2014, p. 75 et suivantes.

² Ces techniques ont été introduites en procédure pénale par la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité ou dite « Perben II ».

³ La captation de données informatiques a été consacrée en procédure pénale par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure ou dite « LOPPSI 2 ».

⁴ Article 706-102-1 du code de procédure pénale.

⁵ Attentats de janvier 2015 à Paris, Montrouge et Dammarville-en-Goële et de février 2015 à Nice.

pour les services de renseignement dans le cadre de la commission d'enquête du Sénat sur l'organisation et les moyens de la lutte contre les réseaux djihadistes¹.

Toutefois, parallèlement aux demandes de renforcement des moyens du renseignement, les craintes d'une surveillance de masse suscitées par les révélations Snowden de 2013 se sont accentuées. Il est vrai que le cadre juridique américain du renseignement a considérablement renforcé les pouvoirs de surveillance numérique de la NSA depuis les attentats du 11 septembre 2001. En effet, l'*USA Patriot Act* du 26 octobre 2001 et d'autres textes ultérieurs comme le *FISA Amendments Act* de 2008 ont modifié le *Foreign Intelligence Surveillance Act* de 1978 afin de permettre, sans véritable contrôle préalable, la collecte massive de données de personnes suspectées de relations avec le terrorisme international ou une puissance étrangère ainsi que l'interception des communications internationales. Ce cadre juridique a permis, sur autorisation de l'*US Foreign Intelligence Surveillance Court* (FISC ou FISA Court), la mise en œuvre du programme PRISM de la NSA d'accès direct aux données hébergées par Google, Apple, Facebook, Amazone ou encore Microsoft (GAFAM). Si l'encadrement du dispositif américain de surveillance a fait l'objet de contestations, il n'a toutefois pas été remis en cause par la justice américaine².

Ces pratiques de surveillance ont provoqué l'indignation et des réactions de la part des autorités européennes³. En octobre 2013, peu de temps après les révélations Snowden, le Parlement européen a ainsi adopté une résolution visant à suspendre l'accord sur les transferts de données depuis l'Europe vers les Etats-Unis dans le cadre du programme de surveillance du financement du terrorisme (accord TFTP) du fait de la surveillance exercée par la NSA⁴. Une seconde résolution du Parlement du 12 mars 2014 a également dénoncé les actions de la NSA et appelé à une meilleure protection des données dans l'Union européenne

¹ A ce sujet, voir N. Goulet et A. Reichardt, co-présidents, et J. -P. Sueur, rapporteur, *Rapport fait au nom de la commission d'enquête sur l'organisation et les moyens de la lutte contre les réseaux djihadistes en France et en Europe*, Sénat, 1^{er} avril 2015, p. 65 et 66.

² A ce sujet, voir C. Guerrier, *PRISM est-il conforme au droit ?*, Revue Lamy Droit de l'immatériel, n° 97, 1^{er} octobre 2013.

³ A ce sujet, voir B. Fauvarque-Cosson, *Les données et la loi française*, CNCIS, 23^{ème} rapport d'activité 2014-2015, p. 50 et suivantes.

⁴ Résolution du Parlement européen du 23 octobre 2013 sur la suspension de l'accord TFTP du fait de la surveillance exercée par l'agence nationale de sécurité américaine (NSA).

ainsi qu'à un plus grand contrôle démocratique des services de renseignement à l'ère numérique¹. Un mois après cette seconde résolution, la CJUE rendait sa décision *Digital Rights Ireland* condamnant le principe de conservation généralisée et indifférenciée des données. De son côté, le « G29 », qui regroupe les autorités européennes de protection des données, a adopté une déclaration en novembre 2014 jugeant la surveillance de masse secrète des personnes en Europe contraire aux Traités et législations de l'Union européenne et éthiquement inacceptable².

A la même période, le Conseil d'Etat ne manquait pas de souligner le caractère essentiel de la surveillance numérique secrète pour « *la stratégie de défense et de sécurité de la France* » tout en suggérant de renforcer les garanties encadrant notamment les accès aux données de connexion et les interceptions des communications à l'étranger³. Ces préoccupations ont été au cœur des lois relatives au renseignement adoptées en juillet et novembre 2015.

Présenté en procédure accélérée en mars 2015, le projet de loi relatif au renseignement a eu pour ambition de poser un cadre juridique unique aux services de renseignement et à leurs activités⁴. Soulignant la prévalence de l'Etat de droit, le projet n'avait pas seulement pour objet les techniques de renseignement mais aussi la définition des missions des services de renseignement, la protection des agents, le contrôle des services ou encore le contentieux du renseignement⁵. Il s'agissait également d'assurer la protection des libertés fondamentales face à l'action de l'Etat ou, autrement dit, de « sortir de la raison d'Etat »⁶. Le projet de loi

¹ Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures.

² Déclaration commune adoptée par le G29 en séance plénière du 25 novembre 2014 et présentée lors de l'évènement *The European Data Governance Forum* organisé le 8 décembre 2014 à Paris (UNESCO).

³ Cf. CE, *Le numérique et les droits fondamentaux*, étude annuelle 2014, p. 194 et suivantes.

⁴ Cf. J. -J. Urvoas, *Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, après engagement de la procédure accélérée, sur le projet de loi relatif au renseignement*, Assemblée nationale, 2 avril 2015, p. 15 et suivantes.

⁵ En ce sens, voir F. Vadillo, *Quand l'Etat de droit rencontre l'Etat secret : cadre et garanties du recours aux techniques de recueil de renseignement*, in *Le droit du renseignement*, op. cit., 8 février 2019, p. 87 et suivantes.

⁶ En ce sens, voir O. Chopin, *Renseignement, sécurité et libertés fondamentales*, in *Le droit du renseignement*, op. cit., p. 201 et suivantes.

a néanmoins mobilisé la contestation de la société civile et des acteurs de l'Internet qui percevaient le texte comme une énième loi sécuritaire visant à étendre toujours plus les moyens des services de renseignement¹, notamment après les attentats de janvier 2015. Il reste que le texte n'était pas une « loi de circonstance » mais le fruit d'une longue réflexion initiée dès 2011 sur l'encadrement des services de renseignement, ce qui a été rappelé avec constance lors des débats parlementaires² et par les commentateurs de la loi relative au renseignement³.

Promulguée le 24 juillet 2015, la loi relative au renseignement consacre un véritable « droit du renseignement » qui demeure toutefois très concentré sur l'encadrement des moyens numériques de renseignement⁴. Prenant en considération les attentes techniques des services, le texte met en place un nouveau dispositif de techniques de renseignement avec l'introduction de nouvelles mesures dont la possibilité de surveiller des communications internationales.

¹ Voir O. Chopin, *Renseignement, sécurité et libertés fondamentales*, in *Le droit du renseignement*, op. cit., p. 201 et suivantes.

² Cf. J. -J. Urvoas, op. cit., Assemblée nationale, 2 avril 2015, p. 84.

³ Voir par exemple les interventions d'Olivier Forcade et de Florian Vadillo dans les actes du colloque sur le droit du renseignement organisé par l'Académie du renseignement à l'Ecole militaire, le 8 février 2018.

⁴ En ce sens, voir B. Warusfel, *Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement*, in *Le droit du renseignement*, op. cit., p. 67 et suivantes.

SECTION II : L'exorbitant dispositif postérieur à 2015

Les lois relatives au renseignement, dont les dispositions sont codifiées dans le Livre VIII du code de la sécurité intérieure¹, instituent un dispositif légal unifié encadrant les techniques de recueil de renseignement soumises à autorisation du Premier ministre et à un contrôle préalable de la Commission nationale de contrôle des techniques de renseignement (CNCTR)² ainsi que des règles plus libérales pour certaines techniques numériques particulières. Sans entrer dans le détail des garanties entourant les techniques numériques de recueil de renseignement³, nos propos s'attacheront, ici, à une analyse du panorama de ces techniques légalisées depuis 2015.

Tout d'abord, il convient d'examiner les modifications apportées sur les techniques déjà consacrées. Le législateur a largement étendu leurs capacités (§1). Ensuite, le nouveau dispositif transpose en droit du renseignement certaines techniques de police judiciaire spécifiques à l'environnement numérique (§2). Enfin, il affirme des mesures numériques de renseignement extérieur (§3).

§1. L'extension des techniques numériques déjà consacrées

Le dispositif issu de 2015 n'a pas mis fin à la distinction entre les interceptions de sécurité et les accès administratifs aux données de connexion⁴, qui sont désormais, sauf pour « l'exception hertzienne », soumis à autorisation du Premier⁵. Par ailleurs, il a été décidé de renforcer le régime des réquisitions des conventions de déchiffrement des données.

A- Les accès administratifs aux données de connexion

La loi du 24 juillet 2015 relative au renseignement a réaffirmé le recueil en temps différé et en temps réel des données de connexion. Cette distinction a été reprise, conformément à la délibération n° 1/2016 du 14 janvier 2016 de la

¹ Articles L. 801-1 à L. 898-1 du code de la sécurité intérieure.

² La loi relative au renseignement a remplacé la CNCIS par la CNCTR qui est chargée de contrôler l'ensemble des techniques de renseignement soumises à autorisation.

³ Voir à ce sujet le Titre II de la Ière Partie.

⁴ Article 5 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

⁵ La loi relative au renseignement a notamment mis fin à la « la personnalité qualifiée » placée sous l'autorité du Premier ministre issue de la loi de programmation militaire de 2013.

CNCTR, par le décret du 29 janvier 2016 relatif aux techniques de renseignement¹ qui précise les modalités d'application des accès aux données de connexion². Ainsi, l'article L. 851-1 du code de la sécurité intérieure a repris les dispositions prévues dans le dispositif de 2013 (ancien article L. 246-1) pour le premier type de recueil³. En pratique, le décret de 2016 a donc prévu que le GIC centralise l'exécution du recueil en temps différé qui est réalisé par les acteurs du numérique sur des données qu'ils conservent, ce qui ne permet pas de recourir aux mesures techniques prévues pour le recueil en temps réel⁴.

En revanche, pour ce qui concerne ce second type de recueil, la loi a entièrement réorganisé la collecte des données en légalisant notamment de nouveaux moyens.

1. Les « sondes » mises en œuvre sur les réseaux

La loi relative au renseignement de 2015 a légalisé la mise en œuvre de « sondes » sur les réseaux des opérateurs permettant de recueillir directement les données de connexion d'une personne préalablement identifiée comme présentant une menace. Introduite uniquement pour la prévention du terrorisme à l'article L. 851-2 du code de la sécurité intérieure, cette technique a pour objectif « *la détection précoce d'actes de terrorisme* »⁵. Cependant, soulignons que l'article 15 de la loi du 21 juillet 2016⁶ prorogeant l'état d'urgence face à la menace terroriste a modifié les dispositions de l'article L. 851-2 relatives aux personnes surveillées. Désormais, les personnes en question ne sont plus celles préalablement identifiées comme présentant une menace mais celles susceptibles d'être en lien avec une menace, ce qui peut élargir le nombre de personnes soumises à la surveillance. En outre, le législateur a élargi l'autorisation

¹ Décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

² Notons qu'avant la publication du décret n° 2016-67 du 29 janvier 2016, le dispositif du décret n° 2014-1576 du 24 décembre 2014 continuait à s'appliquer après la promulgation de la loi relative au renseignement (cf J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, DPR, 25 février 2016, p. 38).

³ Sur ce point, voir J. -J. Urvoas, *Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, après engagement de la procédure accélérée, sur le projet de loi relatif au renseignement*, Assemblée nationale, 2 avril 2015, p. 194.

⁴ En ce sens, voir CNCTR, 1^{er} rapport annuel (2015-2016), p. 37 et suivantes.

⁵ Cf. Etude d'impact, *Projet de loi relatif au renseignement*, 18 mars 2015, p. 71 et 72.

⁶ Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.

individuelle du recueil des données en temps réel à l'entourage de la personne surveillée s'il y a des raisons sérieuses de penser qu'une ou plusieurs personnes sont susceptibles de fournir des informations relevant de la finalité motivant l'autorisation initiale¹. Notons que les parlementaires n'ont pas retenu deux propositions de la DPR qui visaient à élargir l'autorisation prévue à l'article L. 851-2 à des listes de personnes préalablement identifiées et à introduire la notion d'entourage dans l'article L. 851-4 relatif à la géolocalisation². Ces propositions qui concernent davantage les personnes que les données semblent aller dans le sens de la surveillance de masse.

2. Les algorithmes de détection d'une menace terroriste

En amont des sondes de l'article L. 851-2 et par renvoi implicite à cette technique³, la loi de 2015 a consacré, à titre expérimental⁴, un nouvel article L. 851-3 du code de la sécurité intérieure qui permet : dans un premier temps, d'imposer aux opérateurs la mise en œuvre sur leurs réseaux d'algorithmes paramétrés pour « *recueillir, traiter, analyser et recouper un grand nombre d'éléments techniques anonymes* » afin de détecter, dans l'immensité d'Internet, des signaux faibles susceptibles de révéler une menace terroriste⁵ ; et, dans un second temps, de lever l'anonymat sur les données de connexion ayant fait l'objet d'une alerte de l'algorithme.

Cette nouvelle technique a rapidement suscité des inquiétudes. Sur le plan technique, l'INRIA a tenu à rappeler les risques de « faux-positifs » pouvant entraîner l'identification de personnes sans intention terroriste dans l'application

¹ Notons que la notion d'entourage avait déjà été introduite par le législateur en 2015 pour les interceptions de sécurité de l'article L. 852-1 (cf. infra. *L'élargissement des interceptions de sécurité*).

² La DPR avait proposé d'autoriser le recueil en temps réel pour une liste de personnes préalablement identifiées pour faire face à une augmentation possible de suspects potentiels détectés par l'algorithme de l'article L. 851-3. Pour l'entourage en matière de géolocalisation, la DPR souhaitait pouvoir suivre les personnes de l'entourage d'une cible revenue d'une « zone de djihad » pour commettre un attentat en France et ainsi la localiser (cf. P. Adam, op. cit., DPR, 2 mars 2017, p. 77 à 79).

³ En ce sens, voir P. Adam et P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, DPR, 2 mars 2017, p. 77 et 78.

⁴ L'article 25 de la loi relative au renseignement de 2015 est venu préciser que les dispositions de l'article L. 851-3 ne sont applicables que jusqu'au 31 décembre 2018.

⁵ Cf. Etude d'impact, op. cit., 18 mars 2015, p. 72.

de l'article L. 851-3¹. En outre, l'Institut a relevé que la plupart des données recherchées sont stockées en dehors du territoire ou de la juridiction française et échappent donc au traitement prévu par l'article L. 851-3². Par ailleurs, il a été pointé que le texte de l'article L. 851-3 pourrait s'interpréter d'une manière extensive comme « *un mécanisme de big data gouvernemental assurant une surveillance très fine des échanges numériques de la population* », ce qui serait toutefois contraire à l'objectif recherché par le législateur de 2015³.

Si les modalités d'exécution ne sont pas prévues ni par la loi ni par décret, une délibération classifiée du 28 juillet 2016 de la CNCTR portant sur un projet d'architecture générale a rappelé « *que la loi fait obstacle à ce que les agents des services de renseignement puissent accéder aux données collectées tant que le Premier ministre n'a pas autorisé l'identification d'une personne* »⁴. Précisons qu'en 2016, aucun algorithme n'était mis en œuvre chez les opérateurs. Par la suite, l'article 17 de loi n° 2017-510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (SILT) a prolongé jusqu'en 2020 l'expérimentation de l'article L. 851-3. Cette prolongation s'explique par le fait que l'efficacité de cette technique n'a pu être véritablement vérifiée en raison de sa mise en œuvre tardive⁵. En effet, ce n'est que le 27 avril 2017 qu'une première décision classifiée du Premier ministre est venue définir l'architecture des algorithmes et leurs conditions de mise en œuvre en conformité avec la position de la CNCTR⁶. L'architecture générale a été ainsi placée sous la responsabilité du GIC, ce qui semble cohérent au regard de l'ensemble du dispositif issu de la loi relative au renseignement de 2015. Par la suite, une première demande de mise en œuvre d'un algorithme a été soumise, le 18 juillet 2017, à la CNCTR qui a cependant émis un avis défavorable. Notons que la CNCTR avait estimé possible de réaliser des

¹ Cf. INRIA, *Eléments d'analyse technique du projet de loi relatif au renseignement*, Note interne, 30 avril 2015.

² La plupart des informations, documents et données relatives à l'usage d'Internet sont traitées et stockées par les géants du numérique comme les GAFAM américains par exemple.

³ En ce sens, voir B. Warusfel, *Les enjeux du nouveau cadre juridique du renseignement*, 3^{ème} colloque annuel de l'Association française de droit de la sécurité et de la défense (AFDSD), septembre 2015, p. 405 à 423.

⁴ En ce sens, voir CNCTR, 1^{er} rapport annuel (2015-2016), p. 39 et 40.

⁵ Sur point, voir C. Cambon, op. cit., DPR, 11 juin 2020, p. 69 et suivantes.

⁶ Cf. CNCTR, 2^{ème} Rapport d'activité 2017, p. 16 et suivantes.

tests préalables sur des données fictives¹. A notre sens, cette position laisse entrevoir les débuts d'un régime de recherche-développement en renseignement. La CNCTR a finalement approuvé le même algorithme dans le cadre d'une demande rectificative du 25 septembre 2017. Le premier algorithme n'a donc été autorisé par le Premier ministre que le 12 octobre 2017. Il a été renouvelé en décembre 2017 pour deux mois sur avis favorable de la CNCTR et à nouveau renouvelé pour quatre mois². En 2018, deux nouveaux algorithmes ont été autorisés. Sur les trois algorithmes, deux sont prévus pour la DGSI et un pour la DGSE et leur mise en œuvre a bien été confiée au GIC et pour les seuls besoins de la lutte anti-terroriste³. La même année, le Conseil d'Etat statuait sur une seconde affaire portant sur un recours pour excès de pouvoir sur le décret de 2016⁴.

Malgré des résultats discutables depuis leur mise en œuvre en 2017-2018⁵, les algorithmes de l'article L. 851-3 ont été prolongés jusqu'au 31 décembre 2021⁶. Observons que les algorithmes produisent des alertes portant « *sur un nombre relativement faible de données de connexion* » entraînant alors des demandes systématiques d'identification par les services⁷. Dans ce cas, l'intérêt de la distinction introduite par la loi entre les demandes portant sur l'algorithme et celles sur l'identification des personnes semble alors réduit. Néanmoins, la distinction demeure pertinente, à notre sens, compte tenu d'une augmentation toujours possible des données traitées. Il reste à savoir pour les services comment distinguer une alerte méritant une demande d'identification d'une alerte n'en nécessitant pas sans avoir un minimum d'indices préalables sur les données traitées afin de savoir si elles sont réellement « *susceptibles de caractériser*

¹ Cf. CNCTR, 2^{ème} Rapport d'activité 2017, p. 17.

² A ce sujet, voir G. Larrivé, président, et L. Kervran et J. -M. Mis, rapporteurs, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, Assemblée nationale, 10 juin 2020, p. 38 et suivantes.

³ A ce sujet, voir C. Cambon, op.cit., DPR, 11 juin 2020, p. 70.

⁴ Requête n° 397851.

⁵ En ce sens, voir C. Cambon, op. cit., DPR, 11 juin 2020, p. 69 et suivantes.

⁶ Loi n° 2020-1671 du 24 décembre 2020 relative à la prorogation des chapitres VI à X du titre II du livre II et de l'article L. 851-3 du code de la sécurité intérieure.

⁷ Sur ce point, voir G. Larrivé, président, et L. Kervran et J. -M. Mis, op. cit., Assemblée nationale, 10 juin 2020, p. 190 et suivantes.

l'existence d'une menace à caractère terroriste »¹. A ce sujet, les rapports parlementaires et de la CNCTR restent muets. Toutefois, il semblerait que « *le dispositif tourne, sous le contrôle de la CNCTR* »² qui pourrait, selon cette formulation du directeur du GIC, avoir accès aux données traitées par l'alerte afin de caractériser l'existence d'une menace terroriste justifiant une demande d'identification. Cette interprétation serait cependant contraire à la lettre de la loi et placerait la CNCTR dans une position ambiguë au regard de son rôle de contrôleur. Afin d'améliorer les résultats des algorithmes, la question s'est posée d'étendre cette technique au-delà de la seule finalité de la prévention du terrorisme et des données de connexion, notamment en permettant le traitement des adresses web URL (*Uniform Resource Locator*) qui pourrait également s'étendre à l'article L. 851-2³. Finalement, la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement est venue pérenniser le dispositif de l'article L. 851-3 et a étendu son champ d'application ainsi que celui de l'article L. 851-2 aux adresses URL complètes⁴. Cette extension soulève une difficulté d'ordre constitutionnel du fait de la caractérisation juridique incertaine des URL qui sont notamment considérées par la CNCTR comme des données mixtes, c'est-à-dire des données pouvant être assimilées à des données de connexion mais aussi à des données de contenu⁵. Or, l'intégration de ces données mixtes dans le champ des techniques d'accès aux données de connexion tend à remettre en question la délimitation consacrée par le Conseil constitutionnel entre les deux catégories de données⁶. Plus encore, l'extension ainsi prévue pourrait entraîner un basculement du domaine de la surveillance algorithmique vers une interception des contenus plus attentatoire pour les libertés individuelles⁷. Conscient de la sensibilité des URL, le législateur a souhaité

¹ IV. de l'article L. 851-3 du code de la sécurité intérieure.

² Cf. G. Larrivé, président, et L. Kervran et J. -M. Mis, op. cit., Assemblée nationale, 10 juin 2020, p. 190.

³ Ibid, p. 191.

⁴ Articles 15 et 16 de la loi n° 2021-998 du 30 juillet 2021.

⁵ Cf. CNCTR, délibération n° 1/2016 du 14 janvier 2016.

⁶ Cf. infra. Titre II de la Ière Partie.

⁷ En ce sens, voir F. Safi, *La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Entre pérennisation et extension de l'exception...*, La Semaine Juridique Edition Générale n° 40, 4 octobre 2021, 1012.

les distinguer des données de connexion en fixant la durée maximale de conservation des URL à 120 jours au lieu de la limite de 4 ans (article L. 822-2 du code de la sécurité intérieure)¹. Si cette intégration des URL nous apparaît logique en raison de l'intérêt que présente l'utilisation du web pour l'efficacité des techniques de sonde et algorithmiques qui ont vocation à traiter des données massives, une telle évolution pourrait s'interpréter comme une collecte disproportionnée des données susceptible d'une censure constitutionnelle dans le cadre d'une QPC ou encore comme une violation de la protection du secret des correspondances prévue à l'article L. 851-7 du code de la sécurité intérieure². On peut regretter que les parlementaires n'aient pas saisi le Conseil constitutionnel de cette question. De manière restrictive, la CNCTR avait considéré en 2016 que le recueil d'URL devait être limité aux seuls éléments « *qui déterminent le chemin utilisé pour échanger des correspondances ou consulter des informations* »³. Plus en accord avec le législateur, il aurait pu être fait le choix d'introduire une nouvelle demande d'autorisation spécifique pour les données mixtes.

3. La géolocalisation en temps réel et le balisage

S'agissant de la géolocalisation en temps réel, la loi réintroduit à l'article L. 851-4 du code de la sécurité intérieure le suivi d'un équipement terminal sur sollicitation du réseau des opérateurs (ancien article L. 246-3). En outre, elle a élargi les possibilités de la filature numérique en légalisant le recours au balisage d'une personne, d'un véhicule ou d'un objet à l'article L. 851-5. Déjà prévue en matière judiciaire⁴, cette technique permet notamment aux services de renseignement le suivi dynamique d'une cible et de disposer d'une « *capacité de pénétration discrète* » dans des milieux ou zones difficilement accessibles « *sans éveiller des interrogations ou des soupçons* »⁵.

¹ Sur ce point, voir R. Gauvain et L. Kervran, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, Assemblée nationale, 20 mai 2021, p. 91.

² Cf. infra. Titre II de la Ière Partie.

³ Délibération n° 1/2016 du 14 janvier 2016.

⁴ Le balisage a été légalisé en matière de police judiciaire par la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation et codifié à l'article 230-32 du code de procédure pénale.

⁵ Cf. Etude d'impact, op. cit., 18 mars 2015, p. 70 et 71.

En dehors des sondes et algorithmes, la DPR s'est également interrogée en 2020 sur la possibilité d'étendre la technique de géolocalisation de l'article L. 851-4 à l'entourage de la personne surveillée en introduisant un contingentement conformément à la position du Conseil constitutionnel¹. Elle s'est également interrogée sur un possible ajustement du cadre légal de l'article L. 851-4 en rapport avec la notion de « sollicitation du réseau » sans pour autant apporter plus de précision en raison du secret de la défense nationale². Il pourrait s'agir par exemple d'un ajustement technique permettant d'améliorer la précision et l'efficacité de la filature numérique via de nouvelles techniques de géolocalisation qui sollicitent par exemple les réseaux WI-FI ou Bluetooth ou par recueil des données de connexion en temps réel des pages web HTML5 ou de réseaux sociaux³. Ces nouvelles techniques permettent notamment de géolocaliser un équipement terminal à l'intérieur d'un bâtiment en sollicitant le réseau WI-FI d'un aéroport par exemple. Elles nécessiteraient sans doute d'étendre la notion de « sollicitation du réseau » aux autres acteurs du numérique que les opérateurs de télécommunication (FAI, fournisseurs de services en ligne au public et hébergeurs).

Enfin, on notera que si l'exécution de la géolocalisation en temps réel est centralisée par le GIC, le balisage est, quant à lui, directement mis en œuvre par les agents des services de renseignement comme pour la possibilité nouvelle de recourir à des dispositifs de proximité de recueil des données de connexion.

4. L'utilisation d'un « dispositif technique de proximité »

Dans le but d'identifier les différents moyens de communication d'une cible lors d'une surveillance physique ou pour préparer d'autres investigations⁴, l'article L. 851-6 du code de la sécurité intérieure permet désormais l'utilisation d'un « dispositif technique de proximité » (ou dit « *IMSI-catcher* ») pour recueillir

¹ En revanche, la Délégation a estimé « *plus fragile sur le plan constitutionnel* » l'extension de la notion d'entourage à la technique de balisage (L. 851-5) qui peut constituer une ingérence disproportionnée « *pour des individus qui ne présentent pas, comme le Conseil constitutionnel a déjà eu l'occasion de le rappeler, de lien nécessairement étroit avec la menace* » (cf. C. Cambon, op. cit., DPR, 11 juin 2020, p. 81).

² Cf. C. Cambon, op. cit., DPR, 11 juin 2020, p. 81.

³ En ce sens, voir Observatoire du monde cybernétique, *Nouvelles techniques de géolocalisation et risques cyber*, Lettre n°67, octobre 2017.

⁴ Cf. Etude d'impact, op. cit., 18 mars 2015, p. 72 et 73.

des données d'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ou des données de géolocalisation¹.

Toutefois, le développement de la 5G a suscité des interrogations sur l'avenir de l'utilisation des « *IMSI-catcher* »². En effet, cette technologie devrait complexifier les connexions entre les objets connectés et rendre ainsi difficile voire impossible l'interception des données via les fausses antennes relais des services, notamment avec le développement d'identifiants terminaux temporaires³. Afin d'identifier correctement les terminaux mobiles ciblés, la loi relative au renseignement du 30 juillet 2021⁴ a étendu la possibilité pour les services de renseignement de recourir à l'assistance des acteurs du numérique pour l'utilisation des « *IMSI-catcher* »⁵. Si la loi relative au renseignement de 2015 avait opéré une distinction entre les techniques nécessitant le concours des acteurs du numérique et celles pouvant être directement mises en œuvre par les services, la loi relative au renseignement de 2021 réaffirme le rôle majeur de ces acteurs dans le renseignement numérique. Par conséquent, on ne peut que constater la place grandissante qu'occupe le droit du renseignement dans les activités des acteurs du numérique depuis 1991 et, inversement, la nécessité d'élaborer un régime juridique spécifique applicable à ces derniers en dehors du droit du numérique. En pratique, la nouvelle participation des acteurs du numérique dans l'utilisation des « *IMSI-catcher* » ne devrait pas nécessiter une conservation de données ni une transmission de données aux services, ce qui devrait donc exclure l'application du droit de l'Union européenne issue de la jurisprudence de la CJUE sur la conservation des données par les opérateurs du numérique⁶. Pour des raisons de clarification, il aurait pu être précisé cette

¹ Le dispositif technique de l'article L. 851-6 consiste à utiliser une fausse antenne relais portative à proximité de la personne surveillée afin de capter les données transmises par l'équipement terminal de la cible à la véritable antenne relais des opérateurs (cf. délibération de la CNIL 2015-078 du 5 mars 2015).

² A ce sujet, voir G. Larrivé, président, et L. Kervran et J. -M. Mis, rapporteurs, op. cit., Assemblée nationale, 10 juin 2020, p. 108 et suivantes.

³ Sur ce point, voir R. Gauvain et L. Kervran, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, op. cit., p. 74 et suivantes.

⁴ Article L. 871-6 du code de la sécurité intérieure.

⁵ En ce sens, voir P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement. Commentaire de la loi n° 2021-998 du 30 juillet 2021*, Droit pénal n° 10, Octobre 2021, étude 18.

⁶ En ce sens, voir Etude d'impact, *Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative*, 11 mai 2021, p. 161.

absence de collecte et de transmission des données dans les opérations matérielles réalisées par les opérateurs.

On précisera enfin que l'élargissement du champ de réquisition des opérateurs de communications n'a pas concerné l'utilisation des « *IMSI-catcher* » en matière d'interception de sécurité puisque la loi relative au renseignement de 2015 qui a consacré cette technique l'avait déjà introduite dans les dispositions de l'article L. 871-6 du code de la sécurité intérieure.

5. La validité des nouveaux accès aux données de connexion

Cette extension des accès aux données de connexion a été largement discutée durant les débats législatifs de 2015. Les inquiétudes se sont principalement portées sur les techniques des articles L. 851-2, L. 851-3 et L. 851-4 du code de la sécurité intérieure. A cet égard, on peut mentionner tout particulièrement les remarques soulevées par la CNIL et l'Autorité de régulation des communications électroniques et des postes (ARCEP). La CNIL a considéré que l'utilisation des sondes, algorithmes et « *IMSI-catcher* » bouleverse la nature des mesures de surveillance en France et permet de collecter des données de manière massive et directe par les services de renseignement¹. De son côté, l'ARCEP n'a pas manqué de signaler que les nouvelles techniques mises en œuvre chez les opérateurs peuvent, d'une part, avoir un impact sur l'intégrité et la disponibilité des réseaux et, d'autre part, entraîner des risques d'erreurs dans la gestion des demandes administratives et judiciaires de recueil des données du fait de l'augmentation des sollicitations prévues par la loi². L'INRIA a également précisé que les nouvelles techniques d'accès aux données de connexion pouvaient être facilement contournées par les internautes³. Il semblerait que la loi relative au renseignement accusait alors un certain retard vis-à-vis des pratiques de l'Internet.

¹ Délibération 2015-078 du 5 mars 2015.

² Avis n° 2015-0291 de l'Autorité de régulation des communications électroniques et des postes en date du 5 mars 2015 sur le projet de loi relatif au renseignement.

³ La collecte de données de connexion peut être contournée par exemple par l'utilisation d'une connexion chiffrée vers un opérateur ou un hébergeur situé en dehors du territoire national ou échappant à la juridiction française grâce à un *Virtual Private Network* (VPN) ou la mise en place d'un « proxy ». En outre, des mesures de perturbation ou de brouillage (attaques DDoS) des connexions à des sites web considérés comme suspects par les services de renseignement peuvent être mis en œuvre pour déjouer les mesures de surveillance numérique.

Pour autant, le législateur de 2015 a estimé nécessaire de légaliser les nouvelles techniques d'accès aux données de connexion. Il a été soutenu que la loi n'organisait pas une surveillance de masse indifférenciée puisqu'elle prévoit une collecte précise et ciblées des données relatives à des personnes représentant une menace avérée¹. Saisi par le Président de la République et des députés, le Conseil constitutionnel a validé l'ensemble des techniques d'accès aux données de connexion dans sa décision du 23 juillet 2015². Considérant que ces techniques étaient assorties de garanties suffisantes, le Conseil a jugé que la collecte des données était ciblée en référence à la distinction opérée par le législateur entre les données de connexion et les données de contenu. S'agissant particulièrement de l'article L. 851-3, il a approuvé la distinction faite entre le traitement des données et l'identification des personnes en réponse aux critiques des députés sur les « faux positifs » (considérants 59 et 60).

La position du Conseil constitutionnel n'a cependant pas convaincu l'ensemble de la doctrine. En effet, un certain nombre d'auteurs ont affirmé que les nouvelles techniques d'accès aux données de connexion permettent bien une collecte massive des données³. Plus encore, d'autres auteurs ont même précisé que les équipements pouvant être utilisés par les services sont « *des équipements de surveillance de masse* »⁴ et qu'ils « *semblent favoriser une surveillance élargie* »⁵.

A notre sens, la loi consacre des outils techniques permettant la collecte massive des données mais s'efforce de cibler la surveillance des personnes. Cependant, le législateur français glisse peu à peu vers l'élargissement de la surveillance des personnes, en contradiction parfois avec l'évolution de la protection des libertés à l'ère du numérique. Dès 2016, la conventionnalité des

¹ Sur ce point, voir J. -J. Urvoas, op. cit., Assemblée nationale, 2 avril 2015, p. 41 et suivantes.

² Décision n° 2015-713 DC du 23 juillet 2015.

³ En ce sens, voir W. Mastor, *La France, Etat de surveillance ?*, AJDA 2015, p. 2018 ; N. Catelan, *Les nouveaux textes relatifs au renseignement : un moindre mal*, RSC 2015, p. 922 ; L. Christine, et H. Henrion-Stoffel, « *Politique criminelle, renseignement et droits de l'homme. A propos de la loi du 24 juillet 2015 relative au renseignement* », *Revue de science criminelle et de droit pénal comparé*, vol. 3, no. 3, 2015, pp. 761-775 ; R. Parizot, *Surveiller et prévenir... à quel prix ?*, *La Semaine Juridique Edition Générale* n° 41, 5 octobre 2015.

⁴ En ce sens, voir M. -H. Gozzi, *Sed quis custodiet ipsos custodes ? A propos de la loi du 24 juillet 2015 relative au renseignement*, *La Semaine Juridique Edition Générale* n° 38, 14 septembre 2015.

⁵ A ce sujet, voir X. Latour, *La loi relative au renseignement : un Etat de surveillance ?*, *La Semaine Juridique Administrations et Collectivités territoriales* n° 40, 5 octobre 2015.

accès aux données de connexion de la loi relative au renseignement a été mise en doute face à l'arrêt *Tele2 Sverige*¹ de la CJUE du 21 décembre 2016². Confirmant la jurisprudence de 2014 sur la conservation des données³, la décision pouvait notamment s'interpréter comme remettant en cause les accès en temps différé prévus par l'article L. 851-1⁴. En outre, les contentieux les textes portant sur les accès aux données de connexion adoptés la même année que l'arrêt de la CJUE feront ressortir la contradiction précédemment évoquée. Le décret de 2016 a été contesté devant le Conseil d'Etat dans deux affaires, ce qui a abouti à différentes prises de positions de la part du Conseil constitutionnel, du Conseil d'Etat et de la CJUE sur l'évolution des accès aux données de connexion.

Dans le cadre d'une première affaire portant sur la décision de refus du Premier ministre d'abroger le décret contesté⁵, le Conseil d'Etat a, le 17 mai 2017, fait droit à une demande de QPC relative aux nouvelles dispositions de l'article L. 851-2, notamment « *eu égard à l'ampleur des modifications législatives intervenues depuis la déclaration de conformité prononcée par la décision du Conseil constitutionnel du 23 juillet 2015* »⁶. Dans sa décision QPC du 4 août 2017⁷, le Conseil constitutionnel a validé le recueil en temps réel des données d'un individu susceptible d'être en lien avec une menace. En revanche, il a déclaré contraire à la Constitution la notion d'entourage telle qu'introduite par la loi du 21 juillet 2016, conditionnant cette extension de l'article L. 851-2 à un contingentement du nombre d'autorisations simultanées (considérant 11). Cette censure s'inscrit, en toute logique, dans la continuité de la position du Conseil constitutionnel sur la notion d'entourage dégagée dans sa décision n° 2015-713 DC du 23 juillet 2015 dans le cadre du contrôle des dispositions relatives aux interceptions de sécurité

¹ CJUE, 21 décembre 2016, *affaires jointes C-203/15 Tele2 Sverige AB/ Post-och telestyrelsen et C-698/15 Secretary of State for the Home Department/Tom Watson e.a*

² A ce sujet, voir A. -S. Chavent-Leclère, *La surveillance : une pratique encadrée ? renseignement, écoute, vidéo-protection...*, Procédures n°1, Janvier 2016.

³ CJUE, 8 avril 2014, *Digital Rights Irland et Seitlinger e.a.* (affaires jointes C-293/12 et C-594/12, voir CP n° 54/14).

⁴ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 88 et suivantes.

⁵ Requête n° 405792.

⁶ CE, 17 mai 2017, *La Quadrature du Net et autres* (requête n° 405792).

⁷ Décision 2017-648 QPC - 04 août 2017 - *La Quadrature du Net et autres*.

de l'article L. 852-1 (considérants 64 à 67). On peut saluer, ici, le souci des Sages d'assurer la cohérence de la notion d'entourage dans le droit du renseignement, ce qui contribue à une meilleure sécurité juridique en la matière. Le législateur a alors revu sa copie en inscrivant les préconisations du Conseil constitutionnel dans la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (SILT)¹.

Par ailleurs, la loi SILT a supprimé, suivant les préconisations de la CNCTR dans sa délibération du 9 juin 2017 sur le projet de loi, l'article L. 871-2 du code de la sécurité intérieure qui prévoyait un pouvoir de réquisition du Premier ministre des données de connexion pour la réalisation et l'exploitation des interceptions. Survivance du dispositif antérieur à 2015, ce pouvoir de réquisition avait été jugé obsolète par la CNCTR dans une délibération classifiée du 28 avril 2016 et le gouvernement de Manuel Valls s'était engagé à ne plus recourir à ce type de réquisition dans une note du 20 mai 2016².

Dans une décision du 26 juillet 2018³, le Conseil d'Etat a été amené à se prononcer sur la conventionnalité des accès aux données de connexion au regard notamment du droit de l'Union européenne⁴ et de la jurisprudence de la CJUE⁵. A cette occasion, la haute juridiction administrative a mis hors de cause les techniques de balisage⁶ et de « *IMSI-catcher* »⁷ considérant qu'elles n'étaient pas soumises au droit de l'Union européenne étant directement mises en œuvre par les services de renseignement sans passer par les acteurs du numérique. En

¹ Article 15 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

² Cf. CNCTR, 2^{ème} *Rapport d'activité 2017*, p. 40 et suivantes.

³ CE, 26 juillet 2018, *La Quadrature du Net et autres* (requête n° 394922).

⁴ Directive 2002/58/CE du Parlement européen et du Conseil 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 et Charte des droits fondamentaux de l'UE, notamment ses articles 7, 8 et 11.

⁵ CJUE, 8 avril 2014, *Digital Rights Ireland e.a* ; CJUE, 21 décembre 2016, *Tele2 Sverige et Watson e.a* ; CJUE, 2 octobre 2018, *Ministerio Fiscal*.

⁶ Article L. 851-5 du code de la sécurité intérieure.

⁷ Article L. 851-6 du code de la sécurité intérieure.

revanche, le recueil en temps différé¹, le recueil en temps réel², les algorithmes³ et la géolocalisation sur sollicitation des réseaux⁴ ont été considérés comme pouvant se heurter au droit de l'Union européenne, ce qui a abouti à un renvoi préjudiciel à la CJUE sur ces techniques. Le Conseil d'Etat a notamment interrogé la Cour sur la question de savoir si la conservation généralisée et indifférenciée des données ne pouvait pas s'entendre comme une ingérence justifiée au regard des besoins de la sécurité nationale, c'est-à-dire pour les besoins de l'article L. 851-1. Pour le Conseil d'Etat, cette conservation présente une « *utilité sans équivalent* » (considérant 23). Il a alors interrogé la CJUE sur la possibilité de justifier la conservation des données en droit de l'Union européenne sur le fondement du droit à la sûreté garanti par l'article 6 de la Charte des droits fondamentaux et de l'article 4 du traité sur l'Union européenne (TUE) qui prévoit que les exigences de sécurité nationale relèvent de la responsabilité des Etats membres. Cette position a pu être regardée comme une invitation du Conseil d'Etat à la CJUE de revoir sa jurisprudence⁵. S'agissant des techniques de recueil en temps réel nécessitant une intervention chez les acteurs du numérique⁶, le Conseil d'Etat a soulevé la question de savoir si elles sont autorisées par le droit de l'Union européenne car présentant, selon le juge administratif, « *une utilité opérationnelle sans équivalent* » (considérant 27). Par un arrêt très attendu du 6 octobre 2020, la CJUE a réaffirmé le principe de non-conservation généralisée et indifférenciée des données et précisé les dérogations autorisées par le droit de l'Union européenne en matière d'accès aux données de connexion⁷. Dans sa réponse, la Cour n'a pas remis en cause la légalisation des techniques des articles L. 851-1 à L. 851-4 tout en ne manquant pas de préciser les garanties exigées par le droit européen, ce qui a conduit à revoir

¹ Article L. 851-1 du code de la sécurité intérieure.

² Article L. 851-2 du code de la sécurité intérieure.

³ Article L851-3 du code de la sécurité intérieure.

⁴ Article L. 851-4 du code de la sécurité intérieure.

⁵ En ce sens, voir M. -C. de Montecler, *Techniques de renseignement : quand le Conseil d'Etat invite la CJUE à revoir sa jurisprudence*, Dalloz actualité, 7 septembre 2018.

⁶ Article L. 851-2, L. 851-3 et L. 851-4 du code de la sécurité intérieure.

⁷ CJUE, 6 octobre 2020, affaire C-623/17 *Privacy International* et dans les affaires jointes C-511/18 *La Quadrature du Net e.a.* et C-512/18, *French Data Network e.a.*, ainsi que C-520/18 *Ordre des barreaux francophones et germanophone e.a.*

certaines garanties en droit interne¹. Dans le prolongement de cette décision, le Conseil d'Etat a opéré une délicate conciliation dans son arrêt *French Data Network* d'avril 2021² entre les exigences européennes et constitutionnelles permettant de maintenir les dispositifs d'accès aux données de connexion³.

B - Les interceptions de communications

Depuis 2015, les interceptions de sécurité ont été élargies, la surveillance des communications hertziennes réorganisée et une surveillance des communications satellitaires a été consacrée.

1. L'élargissement des interceptions de sécurité

Comme pour les accès aux données de connexion, la loi du 24 juillet 2015 relative au renseignement a maintenu et étendu, dans une moindre mesure, les interceptions de sécurité. Désormais, les interceptions traditionnelles exécutées par le GIC et nécessitant le concours des opérateurs sont prévues à l'article L. 852-1 du code de la sécurité intérieure (ancien article L. 241-2)⁴. Cependant, le législateur de 2015 n'a pas jugé nécessaire de réinscrire le caractère exceptionnel des interceptions dans le texte au regard des garanties entourant ce type de technique et de son contingentement prévu par la loi, ce que la CNIL n'a pas remis en cause⁵. Cette dernière avait néanmoins regretté le maintien du recueil systématique des données de connexion pour l'exécution et l'exploitation des interceptions en estimant que ce type de recueil devrait s'apprécier au cas par cas⁶. Le législateur n'a pas suivi la CNIL sur ce point en inscrivant ce recueil systématique de données à l'article L. 852-1-III⁷. En outre, il a apporté deux innovations notables :

¹ Cf. Titre II de la Ière Partie.

² Conseil d'Etat, 21 avril 2021, *French Data Network* (n° 393099).

³ A ce sujet, voir Section II du Chapitre I du Titre I de la Seconde Partie sur l'impact du droit européen sur le droit du renseignement.

⁴ Selon le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement, le GIC est toujours chargé de centraliser l'exécution des interceptions de sécurité.

⁵ Délibération 2015-078 du 5 mars 2015.

⁶ Ibid.

⁷ On notera que la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste est venue modifier ces dispositions en précisant que les données de connexion recueillies ne sont plus celles nécessaires à l'exécution de l'interception et à son exploitation mais

- d'une part, le législateur a étendu l'autorisation de recourir aux interceptions à l'entourage de la personne surveillée lorsqu'il existe des raisons sérieuses de croire que ce dernier est susceptible de fournir des informations relatives à l'autorisation initiale d'interception. Soulignons que cette position entraîne l'abandon de la « jurisprudence » constante de la CNCIS qui exigeait « *une présomption d'implication directe et personnelle* » de la cible dans les menaces relevant des finalités du renseignement¹ ; et,
- d'autre part, le législateur a consacré la possibilité pour les services de directement réaliser des interceptions opérées par « *IMSI-catcher* » pour les seules finalités prévues aux 1°, 4° et a du 5° de l'article L. 811-3 du code de la sécurité intérieure².

Ni la notion d'entourage ni l'utilisation des « *IMSI-catcher* » n'ont été remis en question par le Conseil constitutionnel dans sa décision du 23 juillet 2015³. Pourtant, parmi les innovations de l'article L. 852-1, la notion d'entourage a particulièrement attiré l'attention des commentateurs. Tout en rappelant que la CNCIS avait tenté de limiter cette extension, il a pu être relevé que les nouvelles dispositions relatives aux interceptions pourraient favoriser l'élargissement de la surveillance en France⁴. Plus particulièrement, des inquiétudes ont été émises sur les limites de la notion d'entourage et sur les risques d'extension de la surveillance à l'entourage de l'entourage de la personne initialement surveillée⁵. Notons néanmoins que la notion d'entourage vise, selon les parlementaires, les personnes « *susceptibles de jouer un rôle d'intermédiaire, volontaire ou non, pour le compte de* »

celles qui y sont associées, ce qui semble être une formulation plus appropriée au regard de l'évolution des accès aux données de connexion et des interceptions de sécurité.

¹ Sur ce point, voir P. Bas, *Rapport sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif au renseignement et sur la proposition de la loi organique présentée par MM. J. -P. Raffarin et P. Bas, relative à la nomination du président de la CNCTR*, Sénat, 20 mai 2015, p. 76 et suivantes.

² Les finalités concernées sont : l'indépendance nationale, l'intégrité du territoire et la défense nationale ; la prévention du terrorisme ; la prévention des atteintes à la forme républicaine des institutions.

³ Décision n° 2015-713 DC du 23 juillet 2015 (considérants 64 à 67).

⁴ En ce sens, voir X. Latour, *La loi relative au renseignement : un Etat de surveillance ?*, op. cit.

⁵ En ce sens, voir O. Desaulnay, *Le renseignement français n'est plus hors-la-loi – Commentaire de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement*, Droit pénal n° 9, Septembre 2015.

la personne surveillée¹. Dès lors, il nous apparaît que cette notion semble, en principe, exclure la possibilité d'autoriser des interceptions pour l'entourage de l'entourage de la personne surveillée.

2. La réorganisation de la surveillance des communications hertziennes

En ce qui concerne la « surveillance hertzienne » issue de l'article 20 de la loi du 10 juillet 1991, aucun changement n'a été apporté à cette mesure d'exception par la loi relative au renseignement. Les dispositions ont simplement été déplacées à l'article L. 811-5 du code de la sécurité intérieure (ancien article L. 241-3).

Cependant, la DPR s'était montrée prudente sur le maintien d'une « exception hertzienne » et sur le droit applicable lorsque ce type d'interception est réalisé à partir du territoire national². Saisi d'une QPC par le Conseil d'Etat, en juillet 2016, dans le cadre du contentieux des décrets d'application de la loi relative au renseignement³, le Conseil constitutionnel a eu finalement l'occasion de se prononcer sur la « surveillance hertzienne » dans une décision du 21 octobre 2016.

Considérant que le législateur n'a aucunement défini les conditions de fond et de procédure applicables à la surveillance hertzienne et que son régime juridique n'exclut pas clairement l'interception de communications individualisables ou n'interdit pas son utilisation à des fins plus larges que la défense des intérêts nationaux, le Conseil constitutionnel a jugé contraire à la Constitution les dispositions de l'article L. 811-5⁴. On peut relever, ici, que les motivations de la décision du Conseil ne sont pas sans rappeler « l'affaire des fadettes » de 2014⁵. Si Cette décision n'a pas eu d'effet sur le contentieux porté

¹ Sur ce point, voir P. Bas, *Rapport sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif au renseignement et sur la proposition de la loi organique présentée par MM. J. -P. Raffarin et P. Bas, relative à la nomination du président de la CNCTR*, op. cit., p. 77.

² Cf. J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, DPR, 25 février 2016, p. 71 à 73.

³ CE, 22 juillet 2016, *La Quadrature du Net et autres* (requête n° 394922).

⁴ Décision n° 2016-590 QPC du 21 octobre 2016, *La Quadrature du Net et autres*.

⁵ Cf. supra. §1 de la Section I du Chapitre I du Titre I.

devant le Conseil d'Etat à l'origine de la QPC¹, l'abrogation immédiate des dispositions litigieuses aurait entraîné des « *conséquences manifestement excessives* » pour les pouvoirs publics. Le Conseil a alors différé dans le temps l'effet de sa décision jusqu'au 31 octobre 2017 pour « *permettre au législateur de remédier à l'inconstitutionnalité constatée* » (considérant 11). En outre, le juge constitutionnel n'a pas manqué l'occasion de poser les bases d'un nouveau régime de la surveillance hertzienne en précisant que l'article L. 811-5 ne peut servir de fondement à des mesures relevant des techniques de renseignement soumises à autorisation et que la CNCTR doit être « *régulièrement informée sur le champ et la nature des mesures prises en application de cet article* » (considérant 12). Le Conseil confirme ainsi la doctrine constante de la CNCIS reprise par la CNCTR². Comme le soulignait le sénateur Michel Boutant, il nous paraît juste de rappeler que cette censure du Conseil constitutionnel contribue à garantir l'Etat de droit dans la légalisation des capacités de surveillance numérique des services de renseignement³.

Afin d'assurer le droit transitoire applicable à l'article L. 811-5, la CNCTR a recommandé au gouvernement, dans une délibération n°2/2016 du 10 novembre 2016, de définir par instructions des ministres concernés les conditions de mise en œuvre des mesures de surveillance hertzienne (champ et nature des mesures ainsi que les motifs pour y recourir). La CNCTR a également recommandé qu'elle puisse contrôler la conformité des mesures de surveillance à la réserve d'interprétation du Conseil constitutionnel et de saisir le Conseil d'Etat en cas de contentieux. Sur le plan organisationnel, ces modifications ont principalement impacté le ministère de la défense et, plus particulièrement, la Direction du renseignement militaire (DRM) qui dispose d'antennes d'interception des

¹ CE, 26 juillet 2018, *La Quadrature du Net et autres* (requête n° 394922).

² Cf. CNCTR, 1^{er} rapport annuel (2015-2016), p. 48 à 51.

³ Cf. M. Boutant, *Avis présenté au nom de la commission des affaires étrangères, de la défense et des forces armées sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, Sénat, 12 juillet 2017, p. 18.

communications hertziennes internationales pouvant être installées sur le territoire national¹. Sur le plan technique, il a fallu distinguer² :

- les communications satellites qui se rattachent, en dehors de la diffusion audiovisuelle, aux communications internationales individualisables et dont l'interception depuis le territoire national doit entrer dans le champ d'application de la loi relative à la surveillance des communications internationales de 2015³ ;
- les communications radio exclusivement hertziennes qui ne sont pas identifiable par un opérateur à un destinataire individualisable et dont les interceptions sur le territoire national ne sont encadrées par aucun texte depuis la décision QPC du 21 octobre 2016 ;
- les communications hertziennes permettant d'accéder au réseau d'un opérateur ou à un réseau privatif dont les interceptions sur le territoire national entrent dans le champ d'application des techniques soumises à autorisation de la loi relative au renseignement de 2015.

Reprenant les préconisations de la DPR dans son rapport d'activité pour l'année 2016, le gouvernement du Premier ministre Edouard Philippe a fait le choix de maintenir la surveillance hertzienne dans son projet de loi SILT de juin 2017 tout en tenant compte du caractère privé ou confidentiel ou ouvert au public des communications concernées, renonçant ainsi au critère du caractère individualisable de la communication⁴. Il convient de noter que cette solution nous apparaît plus protectrice pour les libertés et moins sujette à caution pour caractériser des communications qui utilisent nécessairement le domaine public. Il ressort de l'étude d'impact⁵ et de l'avis du sénateur Michel Boutant sur le projet

¹ A ce sujet, voir P. Adam, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016, DPR, 2 mars 2017, p. 74.

² Ibid, p. 72 à 75.

³ Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

⁴ Cf. Etude d'impact, *Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, 21 juin 2017, p. 74 à 76.

⁵ Ibid, p. 71 à 81.

de loi SILT¹ que le maintien de la surveillance hertzienne s'explique pour des raisons opérationnelles qui nous apparaissent justifiées au regard des missions de contre-ingérence ou de lutte anti-terrorisme des services de renseignement et des forces armées. En effet, les communications hertziennes sont, par exemple, utilisées par les services de renseignement étrangers et forces armées étrangères, les groupes armés non étatiques ou des organisations terroristes. Ces communications présentent notamment l'avantage d'être difficilement individualisables, conférant ainsi un certain anonymat à leur utilisateur qui souhaiterait, par exemple, échapper à la surveillance des communications acheminées par les opérateurs. Finalement, la solution retenue par la loi SILT du 30 octobre 2017 distingue deux types de surveillance hertzienne² :

- le « hertzien privatif » : la loi a introduit une nouvelle technique soumise à autorisation à l'article L. 852-2 du code de la sécurité intérieure visant les interceptions sur le territoire national des communications exclusivement hertziennes utilisant un réseau conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs et n'impliquant pas un opérateur³. A la différence des dispositions de l'article L. 852-1 qui renvoient à la surveillance des personnes à partir de leurs équipements terminaux, celles prévues à l'article L. 852-2 visent des réseaux privés. Si cette référence au réseau pourrait être perçue comme une surveillance non ciblée, il n'en demeure pas moins que l'article L. 852-2 s'inscrit dans une recherche de conciliation entre le respect des libertés et les particularités de la surveillance hertzienne, notamment en intégrant dans le régime d'autorisation les transmissions entre objets connectés pouvant

¹ Cf. M. Boutant, *Avis présenté au nom de la commission des affaires étrangères, de la défense et des forces armées sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, op. cit., p. 13 et suivantes.

² Article 15 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

³ Les communications hertziennes concernées par l'article L. 852-2 sont par exemple : le trafic WI-FI non connecté à internet (réseau interne d'une entreprise ou à un domicile familial) et le trafic entre téléphone sans fil en mode « interphone » ; les « *private mobile radiocommunications* » (PMR) ; les communications satellitaires exclusivement hertziennes ne passant pas par un opérateur et qui sont rattachables au territoire national ; le trafic relevant du protocole Bluetooth, NFC ou RFID (objets connectés) en raison de leur faible portée. Précisons que les signaux hertziens GPS sont considérés comme des balises au sens de l'article L. 851-5 (Cf. Etude d'impact, *Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, op. cit., p. 71 à 81).

n'appartenir qu'à une seule personne¹. Par ailleurs, notons que les moyens d'interception visés par l'article L. 852-2 renvoient implicitement à ceux visés à l'article 226-3 du code pénal sur la captation ou la détection à distance de conversations ou de données informatiques ;

- le « hertzien ouvert » : la loi a maintenu le régime d'exception hertzienne dans les articles L. 855-1 A à L. 855-1 C du code de la sécurité intérieure pour les communications qui n'impliquent pas un opérateur et qui n'entrent pas dans le champ d'application des techniques soumises à autorisation, notamment du nouvel article L. 852-2². Là aussi, les moyens d'interception renvoient à ceux visés à l'article 226-3 du code pénal mais également aux moyens militaires tels que les antennes de la DRM opérant depuis le territoire national.

S'agissant plus particulièrement du « hertzien ouvert », la loi SILT a, comme souhaité par le gouvernement et approuvé par la CNCTR³, autorisé ce type de surveillance dans le code de la défense pour les unités militaires chargées de la dissuasion nucléaire et des missions d'action de l'Etat en mer⁴ ainsi que pour les tests des matériels militaires d'interception réalisés par certains services des armées dont la Direction générale à l'armement (DGA)⁵. Dans ce dernier cas, l'exploitation des renseignements recueillis n'est pas autorisée en raison du risque d'interception de communications privées.

En plus d'opérer une distinction entre la « surveillance administrative » relevant du code de la sécurité intérieure et la « surveillance militaire » relevant du code de la défense, la loi SILT semble consacrer une distinction légale entre les opérations de renseignement et la recherche-développement en renseignement dans le domaine numérique. Notons d'ailleurs que l'article 36 de la LPM 2019-2025 du 13 juillet 2018 a étendu l'autorisation des tests pour les essais de

¹ Délibération n° 4/2017 du 9 juin 2017 de la CNCTR.

² Les communications hertziennes concernées par l'article L. 855-1 A sont par exemple : le trafic des radioamateurs ; les Citizen-band (CB ou cibistes) ; les talkies-walkies analogiques ; les communications radio VLF et HF ainsi que les moyens militaires tactiques V/UHF (Cf. Etude d'impact, *Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, op. cit., p. 71 à 81).

³ Délibération n° 4/2017 du 9 juin 2017 de la CNCTR.

⁴ Article L. 2371-1 du code de la défense.

⁵ Article L. 2371-2 du code de la défense.

systèmes d'arme intégrant les techniques de renseignement des articles L. 851-6, L. 852-1 II, L. 852-2 du code de la sécurité intérieure et des moyens de surveillance des communications internationales prévus à l'article L. 854-1 du même code¹. Il s'agissait notamment de sécuriser juridiquement l'acquisition, la détention et les essais des matériels en question pour les militaires contre les risques de poursuites sur le fondement de l'article 226-3 du code pénal². Par la suite, un arrêté du 3 janvier 2019 signé par la ministre des armées, Florence Parly, est venu renforcer le cadre légal des essais³, notamment en ajoutant que ces derniers « *couvrent les travaux de recherche et développement, de vérification, de validation ou de qualification de ces appareils ou dispositifs techniques* »⁴, ce qui tend à confirmer textuellement une légalisation de la recherche-développement en renseignement numérique mais qui reste néanmoins circonscrite à la « surveillance militaire ». Il nous apparaît alors logique de permettre ces essais pour la « surveillance administrative » comme le suggère la DPR dans son rapport pour les années 2019-2020⁵. Cette dernière préconise d'autoriser des essais pour l'ensemble des techniques de renseignement pour les services spécialisés de renseignement et le GIC.

3. La consécration d'une surveillance des communications satellitaires

Toujours dans l'idée de permettre aux services de renseignement de faire face aux avancées des nouvelles technologies numériques, la loi du 30 juillet 2021 relative au renseignement a consacré, à titre expérimental jusqu'en juillet 2025, une nouvelle technique d'interception portant sur des communications satellitaires⁶. Introduite à l'article L. 852-3 du code de la sécurité intérieure, cette

¹ Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

² En ce sens, voir Etude d'impact, *Projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*, 6 février 2018, p. 138 et suivantes.

³ Délibération n° 4/2018 du 8 novembre 2018 de la CNCTR.

⁴ Arrêté du 3 janvier 2019 relatif aux essais de matériels de renseignement réalisés en application de l'article L. 2371-2 du code de la défense.

⁵ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 82 à 84.

⁶ Sur ce point, voir P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement. Commentaire de la loi n° 2021-998 du 30 juillet 2021*, op. cit.

nouvelle technique vise à utiliser sur le territoire national un appareil ou un dispositif technique similaire à un « *IMSI-catcher* » relevant de l'article 226-3 du code pénal pour intercepter des correspondances acheminées par des satellites de télécommunications qui relèvent notamment d'opérateurs étrangers non assujettis aux obligations légales françaises. Il s'agit de prendre en compte les évolutions de l'internet spatial portées essentiellement par les acteurs américains du « *New Space* »¹. Dans ce contexte, il était donc nécessaire d'adopter un cadre distinct des réquisitions pouvant être autorisées dans le cadre du I de l'article L. 852-1 du code de la sécurité intérieure. Le législateur n'a pas non plus souhaité reprendre le cadre adopté au II du même article concernant le recours au « *IMSI-catcher* », considérant que le dispositif d'interception satellitaire ne présenterait pas à court terme le même niveau d'utilisation². Dans l'incertitude des évolutions techniques et juridiques à prévoir, il a été décidé que la mise en œuvre de ce nouveau type d'interception sera autorisée par un décret en Conseil d'Etat après avis de la CNCTR pour les seules finalités prévues aux 1°, 2°, 4° et 6° de l'article L. 811-3 du code de la sécurité intérieure³. L'autorisation ne pourra être délivrée que pour une durée maximale de 30 jours et permettra le recueil des données de connexion associées à l'interception. Si les interceptions sont directement réalisées par les services, elles doivent être immédiatement centralisées au GIC qui est chargé de mettre à disposition les renseignements collectés. En cas d'impossibilité technique, les données recueillies devront être chiffrées jusqu'à leur centralisation au GIC. Un contingentement des autorisations est également prévu. Conformément aux remarques soulevées par la CNCTR⁴, cette nouvelle technique présente un caractère subsidiaire par rapport aux interceptions du I de l'article L. 852-1, c'est-à-dire qu'elle ne pourra être autorisée que s'il n'est pas techniquement possible de recourir à l'assistance des opérateurs ou si cette assistance soulève un problème de confidentialité par la nécessité de révéler à des

¹ A ce sujet, voir Observatoire du monde cybernétique, *Le New Space et la course à l'Internet spatial*, 7 septembre 2020.

² Cf. R. Gauvain et L. Kervran, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, op. cit., p. 79.

³ Les finalités sont l'indépendance nationale, la prévention du terrorisme, la promotion et la défense des intérêts majeurs de la politique étrangère et la lutte contre la criminalité organisée.

⁴ Délibération n° 3/2021 du 14 avril 2021.

opérateurs étrangers l'identité des cibles des services¹. Ce nouveau dispositif juridique expérimental à caractère subsidiaire devrait cependant être amené à évoluer car, en l'état actuel des capacités techniques des services, il conduit à une interception de toutes les correspondances satellitaires pouvant être détectées par l'outil de surveillance, le ciblage n'étant opéré qu'*a posteriori* au sein du GIC². Dans ces conditions, il est vrai que l'on peut s'interroger sur le caractère raisonnable de cette nouvelle mesure et, plus largement, sur une banalisation des atteintes à la vie privée³.

Une autre évolution pourrait être à prévoir concernant l'avenir du recours au « *IMSI-catcher* » en matière d'interception⁴. Cette technique pourrait être remise en cause par le renforcement du chiffrement du contenu des correspondances avec le déploiement de la 5G⁵, ce qui nous amène à évoquer les dispositions du droit du renseignement relatives aux réquisitions des conventions de déchiffrement des données.

C - Les réquisitions des conventions de déchiffrement des données

La loi du 24 juillet 2015 relative au renseignement n'a pas manqué de reprendre l'obligation prévue par la loi de 1991⁶ imposant aux prestataires de cryptologie la remise des conventions de déchiffrement des données sur demande des services de renseignement⁷. Le dispositif a été légèrement renforcé avec la fixation d'un délai de 72 heures accordé aux prestataires pour la remise des conventions ou pour procéder au déchiffrement des données et un rehaussement des peines d'amende en cas d'obstruction aux réquisitions (de 30 000 et 7 500 euros à 150 000 euros), ce qui assure effectivement une meilleure sécurité

¹ Sur ce point, voir R. Gauvain et L. Kervran, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, op. cit., p. 79.

² Avis n° 402562 du Conseil d'Etat sur un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, 21 avril 2021 ; CNCTR, Délibération n° 3/2021 du 14 avril 2021.

³ En ce sens, voir F. Safi, *La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Entre pérennisation et extension de l'exception...*, op. cit.

⁴ Article L. 852-1 II du code de la sécurité intérieure.

⁵ En ce sens, voir G. Larrivé, président, et L. Kervran et J. -M. Mis, rapporteurs, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 108 et suivantes.

⁶ Article L. 871-1 du code de la sécurité intérieure.

⁷ Sur ce point, voir X. Latour, *La loi relative au renseignement : un État de surveillance ?*, op. cit.

juridique pour les services¹. De leur côté, les prestataires se voient garantis que « *l'intégralité des frais liés à la mise en œuvre de l'obligation prévue par l'article L. 871-1 est prise en charge, sur la base des frais réellement exposés par le fournisseur et dûment justifiés par celui-ci, par le budget des services du Premier ministre* »².

En pratique, les réquisitions résultent d'une décision écrite et motivée du Premier ministre³ qui indique les personnes concernées et les modalités des opérations devant être réalisées⁴. Les prestataires visés sont notifiés de la décision sans délai et la décision est communiquée à la CNCTR⁵. Il convient de préciser que les conventions de déchiffrement « *s'entendent des clés cryptographiques ainsi que de tout moyen logiciel ou de toute autre information permettant la mise au clair de ces données* »⁶. A cet égard, on notera que la jurisprudence de la Cour de cassation s'est expressément appuyée sur cette définition pour étendre la qualification de convention de déchiffrement au code de déverrouillage d'un smartphone dès lors que ce dernier est équipé d'un moyen de cryptologie chiffrant les données à l'occasion de son verrouillage⁷. Bien que cette précision jurisprudentielle ne concerne que la police judiciaire, elles apportent un éclairage sur l'application de notions définies en droit du renseignement.

Le renforcement du régime des réquisitions des conventions de déchiffrement pourrait s'avérer limité dans les années à venir face à la libéralisation et au perfectionnement des outils de chiffrement sans que pour autant « une réponse juridique certaine » puisse être apportée aujourd'hui⁸.

¹ En ce sens, voir *La loi n° 2015-912 du 24 juillet 2015 relative au renseignement. 3 questions à Jean-Jacques Urvoas, député (PS) du Finistère, président de la commission des lois de l'Assemblée nationale*, Communication Commerce électronique n° 10, Octobre 2015, entretien 9.

² Article R. 873-1 du code de la sécurité intérieure.

³ Article R. 871-1 du code de la sécurité intérieure.

⁴ Article R. 871-4 du code de la sécurité intérieure.

⁵ Article R. 871-2 du code de la sécurité intérieure.

⁶ Article R. 871-3 du code de la sécurité intérieure.

⁷ Sur la qualification de convention de déchiffrement d'un code de déverrouillage d'un smartphone, voir S. Fucinile, *Code d'accès d'un téléphone : une convention de déchiffrement ?*, Dalloz Actualité, 20 octobre 2020 ; J. Buisson, *Téléphones portables et convention secrète de déchiffrement*, Procédures n° 1, Janvier 2021, alerte 1 ; E. A. Caprioli, *Clé de déchiffrement. Assimilation du code de déverrouillage du téléphone portable à un moyen de cryptologie*, Communication Commerce électronique n° 12, Décembre 2022, comm. 89.

⁸ Sur ce point, voir G. Larrivé, président, et L. Kervran et J. -M. Mis, rapporteurs, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 112.

Néanmoins, le débat sur l'installation des « portes dérobées » (ou « *backdoors* » en anglais) dans les systèmes numériques pour contourner le chiffrement pourrait se renouveler même si cette solution n'avait pas été retenue en raison de ces risques pour la sécurité de l'économie numérique¹. Pour notre part, nous rejoignons la position de certains commentateurs qui s'opposent ouvertement à l'introduction de « portes dérobées »².

§2. La transposition de certaines techniques de police judiciaire

Reprenant les propositions du rapport de la DPR pour l'année 2014 sur les techniques de police judiciaire³, la loi du 24 juillet 2015 a consacré la possibilité pour les services de renseignement de recourir, d'une part, aux techniques de sonorisation et de captation d'images et, d'autre part, à la captation de données informatiques sur le territoire national⁴. Ces nouveaux moyens directement mis en œuvre par les services entrent dans le champ des techniques soumises à autorisation mais ne peuvent être autorisées qu'à titre subsidiaire du fait de leur caractère très intrusif dans la vie privée des personnes⁵. Les dispositifs et appareils utilisés renvoient à ceux envisagés par l'article 226-3 du code pénal dont la liste est fixée par arrêté⁶. Parfois déployées à proximité de leur cible, ces techniques peuvent nécessiter pour les agents des services de s'introduire dans un véhicule ou dans un lieu privé. La loi relative au renseignement a ainsi prévu une autorisation spécifique pour ce type d'opération à l'article L. 853-3 du code de la sécurité intérieure. Cette dernière peut également concerner le balisage⁷. Notons que la CNCTR a précisé que si l'introduction dans un véhicule ou un lieu privé nécessite une autorisation spécifique, cette mesure constitue un moyen de mettre

¹ A ce sujet, voir S. Sontag Koenig, *Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel*, AJ Pénal 2016, p. 238.

² En ce sens, voir notamment F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, Livret #12, L'Hétairie, 9 mars 2020.

³ Cf. supra. §2 de la Section I du Chapitre I du Titre I de la Ière Partie.

⁴ Article 6 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

⁵ Cf. Titre II de la Ière Partie.

⁶ Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal.

⁷ Article L. 851-5 du code de la sécurité intérieure.

en place des techniques et n'est pas une technique à proprement parler¹. Au-delà d'un renforcement des moyens qui n'a pas reçu d'opposition de principe par la CNIL², il s'agissait de sécuriser juridiquement sur le fondement de l'article 122-4 du code pénal³ les actions des agents des services opérant sur le territoire national au plus près de la population sans avoir besoin de leur accorder une immunité pénale spécifique⁴. En dehors du régime des techniques soumises à autorisation, le législateur de 2015 a introduit une autre technique d'enquête également connue du monde judiciaire : les « cyber-patrouilles »⁵.

A - La sonorisation et la captation d'images

Codifiées à l'article L. 853-1 du code de la sécurité intérieure, les dispositions relatives à la sonorisation et à la captation d'images reprennent, de manière plus simplifiée, celles de l'article 706-96 du code de procédure pénale. Les deux textes prévoient pour les services de renseignement et de police judiciaire la possibilité d'utiliser des dispositifs techniques de captation, de fixation, de transmission et d'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé. Sur le plan technique, il s'agit d'utiliser des enregistreurs, des microphones et des caméras⁶. En pratique, ces techniques trouvent particulièrement à s'appliquer en matière de contre-espionnage ou de contre-ingérence ainsi qu'en matière de terrorisme et de criminalité organisée⁷. Les micros et caméras espions présentent l'intérêt d'entendre et/ou de voir une ou des cibles qui sont habituées à déjouer les dispositifs de surveillances numériques et physiques. Juridiquement, la sonorisation et la captation d'images dans le domaine du renseignement n'ont pas été remises en question par le Conseil

¹ Cf. CNCTR, *1^{er} rapport annuel* (2015-2016), p. 42.

² Délibération 2015-078 du 5 mars 2015.

³ « *N'est pas pénalement responsable la personne qui accomplit un acte prescrit ou autorisé par des dispositions législatives ou réglementaires. N'est pas pénalement responsable la personne qui accomplit un acte commandé par l'autorité légitime, sauf si cet acte est manifestement illégal* ».

⁴ Sur ce point, voir Etude d'impact, *Projet de loi relatif au renseignement*, 18 mars 2015, p. 65.

⁵ Article 8 de la loi n° 2015-912 du 24 juillet 2015.

⁶ Sur ce point, voir J. -J. Urvoas, *Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, après engagement de la procédure accélérée, sur le projet de loi relatif au renseignement*, op. cit., p. 213.

⁷ Sur la pratique, voir Etude d'impact, *Projet de loi relatif au renseignement*, op. cit., p. 64 à 67.

constitutionnel dans sa décision du 23 juillet 2015¹ et n'ont pas présentées de difficultés particulières en matière de recherche et de collecte des renseignements. En revanche, la distinction opérée par la loi entre la sonorisation et la captation d'images a présenté des difficultés en matière de conservation des données obtenues².

B - La captation de données informatiques

Initialement, l'article L. 853-2 du code de la sécurité intérieure a distingué deux types de techniques : le recueil de données informatiques stockées dans un système d'information³ et la captation de données informatiques sous forme de flux, c'est-à-dire les données s'affichant sur un écran, introduites par saisie de caractères ou reçues et émises par des périphériques audiovisuels⁴. Ces techniques consistent à utiliser des logiciels espions ou « mouchards » qui ont par exemple pour fonction d'enregistrer les frappes sur un clavier d'ordinateur (« *keylogger* » en anglais) ou de réaliser une capture d'écran⁵. La captation de données informatique apparaît comme une solution de secours aux interceptions de sécurité face à la diversité des moyens numériques de communication et qui sont de plus en plus protégés par le chiffrement⁶. Pour autant, bien que le législateur de 2015 ait souhaité éviter l'obsolescence de l'article L. 853-2 au regard de la technologie en s'attachant à la finalités des techniques de captation de données informatiques⁷ et que la rédaction de cet article ait été jugé conforme à la Constitution par le Conseil constitutionnel dans sa décision du 23 juillet 2015⁸, il n'en demeure pas moins que des problèmes de conformité du droit à la réalité

¹ Décision n° 2015-713 DC du 23 juillet 2015 (considérants 69 à 75).

² Cf. infra. Titre II de la Ière Partie.

³ Article L. 853-2-1° du code de la sécurité intérieure.

⁴ Article L. 853-2-2° du code de la sécurité intérieure.

⁵ En ce sens, voir J. -J. Urvoas, *Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, après engagement de la procédure accélérée, sur le projet de loi relatif au renseignement*, op. cit., p. 213 et suivantes.

⁶ En ce sens, voir Etude d'impact, *Projet de loi relatif au renseignement*, op. cit., p. 64 à 67.

⁷ En ce sens, voir J. -J. Urvoas, *Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, après engagement de la procédure accélérée, sur le projet de loi relatif au renseignement*, op. cit., p. 215.

⁸ Décision n° 2015-713 DC du 23 juillet 2015 (considérants 69 à 75).

technologique se sont révélées dans l'application de cette nouvelle technique de renseignement.

Une première difficulté a concerné la technique définie dans les dispositions de l'article L. 853-2-2°. Dans leur rédaction initiale, ces dispositions limitaient notamment la captation de données informatiques reçues et émises par des périphériques aux seuls périphériques audiovisuels. Or, cette limitation avait pour conséquence de ne pas prendre en compte le partage de données avec d'autres périphériques, notamment les objets connectés qui n'entrent pas nécessairement dans la catégorie des périphériques audiovisuels¹. Afin de tenir compte de la diversité des objets connectés et de leurs évolutions, l'article 15 de la loi SILT du 30 octobre 2017 a donc supprimé le mot « audiovisuels » à la fin de l'article L. 853-2-2°. Au-delà d'assurer la pérennité dans le temps du dispositif, cette clarification a eu « *en pratique pour effet d'intégrer le recueil de certaines transmissions hertziennes, notamment les transmissions par protocoles de communication sans fil tels que le wifi, dans le champ d'application de la technique de captation de données informatiques* »². Autrement dit, les services de renseignement peuvent être autorisés à pirater des objets connectés pour accéder aux données qu'ils reçoivent ou transmettent par voie hertzienne sur le fondement l'article L. 853-2. Notons que cette nouvelle possibilité ne remet pas en question les distinctions entre le « hertzien ouvert »³, le « hertzien privatif »⁴ et les communications hertziennes relevant des opérateurs⁵. En effet, les communications hertziennes pouvant être concernées par l'article L. 853-2 sont toutes celles qui entrent dans le champ d'application des interceptions de sécurité des articles L. 852-1 et L. 852-2 du code de la sécurité intérieure⁶. Précisons également que le recours à l'article L. 853-2 n'est possible qu'à la condition que les

¹ On peut citer par exemple les bracelets connectés équipés de capteurs liés à la mobilité des personnes ou à leur état de santé ou encore les objets de maison connectée tels que les serrures connectées ou les robots de cuisine ou d'entretien ménager.

² Sur ce point, voir R. Gauvain, *Rapport sur le projet de loi, adopté par le Sénat après engagement de la procédure accélérée, renforçant la sécurité intérieure et la lutte contre le terrorisme*, Assemblée nationale, 14 septembre 2017, p. 240 et 241.

³ Article L. 855-1 A du code de la sécurité intérieure.

⁴ Article L. 852-2 du code de la sécurité intérieure.

⁵ Article L. 852-1 du code de la sécurité intérieure.

⁶ Cf. Etude d'impact, *Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, op. cit., p. 77 à 79.

interceptions de sécurité ne permettent pas en pratique d'accéder aux contenus des communications hertziennes surveillées. Par exemple, le recours à la captation de données informatiques prévu par le législateur de 2017 pourrait être autorisé pour contourner le chiffrement d'une communication hertzienne¹, ce qui pourrait d'ailleurs entraîner à l'avenir une augmentation du recours à cette technique pour faire face au déploiement de la 5G². Relevons que cette modification constitue un progrès pour deux raisons :

- d'une part, elle a pour effet de mieux cibler les mesures de surveillance en permettant aux services de ne recourir qu'à la captation des seules données émises ou reçues par des objets connectés lorsqu'une interception de sécurité ne permet pas en pratique d'accéder à ces données et sans avoir à solliciter le recueil de l'ensemble des données stockées dans les objets connectés visés³ ;
- d'autre part, cette modification renforce l'encadrement de la surveillance hertzienne dans le cadre du recours à l'article L. 853-2 qui ne peut être autorisé qu'à titre subsidiaire⁴.

Soulignons que si le Conseil constitutionnel n'a pas eu l'occasion de se prononcer sur cette modification, il a validé en mars 2019 la même modification opérée par le législateur pour les captations de données en matière judiciaire dans la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice⁵.

La seconde difficulté tient à la complexité de la mise en œuvre des techniques de captation de données informatiques, que ce soit en matière judiciaire ou de renseignement. En cybersécurité, le recours à des logiciels espions renvoie généralement à des attaques informatiques, baptisés par les analystes

¹ Cf. Etude d'impact, *Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, op. cit., p. 77 à 79.

² Cf. supra. §1 de la Section II du Titre I de la Ière Partie.

³ Cf. Etude d'impact, *Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*, op. cit., p. 79.

⁴ Délibération de la CNCTR n° 4/2017 du 9 juin 2017.

⁵ Décision n° 2019-778 DC du 21 mars 2019, *Loi de programmation 2018-2022 et de réforme pour la justice* (considérant 167).

américains APT (Advanced Persistent Threat)¹, qui sont des « *attaques sophistiquées et furtives, avec un fort degré d'anticipation et de préparation* » et qui sont menées dans la durée². Le haut niveau de technicité requis pour la captation de données informatiques a pu alors expliquer le retard opérationnel souligné en 2015 dans la mise en œuvre de cette technique en matière judiciaire³. Plus particulièrement, l'impossibilité pour les solutions de cybersécurité d'opérer une distinction entre les logiciels espions cybercriminels et ceux des services de police a soulevé une question pratique⁴. Dès lors, on pourrait imaginer, dans ce cas, une régulation des solutions de cybersécurité au regard des besoins cyber-policiers ou de cyber-renseignement, ce qui serait toutefois problématique pour la protection l'économie numérique à l'instar de la polémique du chiffrement et des portes dérobées⁵.

Dans le domaine du renseignement, les services se sont progressivement approprié les nouvelles techniques dont celles de l'article L. 853-2⁶. La captation informatique est notamment utilisée par la DGSI, la DGSE et la DNRED pour la surveillance du cyberespace et les besoins de la cyberdéfense⁷. Néanmoins, la distinction prévue par la loi relative au renseignement entre le recueil des données de informatiques (RDI)⁸ et la captation de ces données (CDI)⁹ a tout de même fait l'objet d'une critique. Dès 2016, la DPR a constaté qu'en pratique la technique utilisée par les services était la technique de RDI qui peut être autorisé pour une durée de 30 jours à la différence de la CDI qui peut l'être pour une durée de deux

¹ Voir à ce sujet la sous rubrique « *Espionnage* » de la rubrique « *Principales menaces* » du site web de l'ANSSI ([Espionnage | Agence nationale de la sécurité des systèmes d'information \(ssi.gouv.fr\)](https://ssi.gouv.fr/)).

² Sur ce point, voir L. Gautier, *Cyber : les enjeux pour la défense et la sécurité des Français*, Politique étrangère, vol. Été, no. 2, 2018, pp. 29-42.

³ En ce sens, voir M. Quémener, *Les techniques spéciales d'enquête en matière de lutte contre la cybercriminalité*, AJ Pénal 2015 p.403.

⁴ Ibid.

⁵ En ce sens, voir Conseil national du numérique, *Prédictions, chiffrement et libertés*, op. cit., p. 6.

⁶ Depuis 2015, les rapports successifs de la CNCTR font état d'une appropriation croissante de la maîtrise des nouvelles techniques dont celles de l'article L. 853-2 (cf. CNCTR, *4^{ème} rapport d'activité 2019*, p. 50 à 52).

⁷ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 266 à 268.

⁸ Article L. 853-2-1° du code de la sécurité intérieure.

⁹ Article L. 853-2-2° du code de la sécurité intérieure.

mois¹. A ce titre, les parlementaires ont proposé d'aligner sur la durée des deux mois les autorisations de RDI et de CDI pour plus de cohérence avec la réalité technologique. Cette proposition a été réitérée par le rapport « Larrivé » du 10 juin 2020 sur l'évaluation de la loi relative au renseignement². Dans son rapport d'activité de 2020, la DPR va plus loin en recommandant une simplification de l'article L. 853-2 pour ne retenir qu'une seule définition de l'accès aux données informatiques et qu'une seule durée d'autorisation de deux mois³. Dans le cadre de la loi du 30 juillet 2021, le législateur a finalement procédé à une fusion des deux techniques RDI et CDI⁴. Comme recommandé, il a ainsi harmonisé le délai d'autorisation sur celui de deux mois et supprimer la distinction entre RDI et CDI, l'autorisation valant alors pour les deux techniques⁵. Cette proposition va à l'encontre de ce qu'avait préconisé l'étude d'impact de l'exécutif qui n'avait pas souhaité remettre en question cette distinction afin d'obliger les services à motiver leur demande sur l'une ou l'autre des techniques⁶. L'harmonisation des délais ne devrait pas présenter de difficulté de nature constitutionnelle selon l'étude d'impact⁷ et elle nous semble cohérente au regard des caractéristiques des logiciels espions. En revanche, la fusion des deux techniques nous apparaît moins protectrice pour le respect du droit à la vie privée puisqu'elle pourrait avoir pour effet de généraliser l'utilisation de la technique de RDI, ce qui pourrait être également perçu comme un pas de plus vers une collecte de masse et

¹ Cf. P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 78.

² Cf. G. Larrivé, président, et L. Kervran et J. -M. Mis, rapporteurs, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 184.

³ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 66.

⁴ Sur ce point, voir P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement. Commentaire de la loi n° 2021-998 du 30 juillet 2021*, op. cit.

⁵ En ce sens, voir R. Gauvain et L. Kervran, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, op. cit., p. 74.

⁶ Cf. Etude d'impact, *Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative*, op. cit., p. 156.

⁷ « Dans sa décision rendue sur la loi relative au renseignement de 2015 (décision n° 2015-713 DC du 23 juillet 2015), le Conseil constitutionnel, se prononçant sur la conformité à la Constitution des dispositions de l'article L. 853-2 du code de la sécurité intérieure, s'est borné à relever que « que l'autorisation est délivrée pour une durée de deux mois ou de trente jours selon la technique utilisée » sans que l'on puisse déduire de cette incise qu'une uniformisation de ces durées d'autorisation serait de nature à heurter un principe constitutionnel, notamment le droit au respect de la vie privée et l'inviolabilité du domicile ». (Cf Etude d'impact, *Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative*, op. cit., p. 156).

indifférenciée des données alors que la loi du 24 juillet 2015 avait justement organisé une collecte ciblée des données. Par ailleurs, le choix du législateur de 2021 serait de nature à remettre en cause la « neutralité technologique » recherchée par le législateur de 2015¹. Pour notre part, il conviendrait de conserver la distinction entre les deux techniques, notamment dans les cas où les logiciels espions seraient en mesure de cibler uniquement des données émises ou reçues par des composantes informatiques.

La loi du 30 juillet 2021 a également élargi le champ de réquisition des opérateurs de communications² aux techniques de captation de données informatiques « *afin notamment d'éviter que les opérateurs, dans le cadre de la protection de leurs réseaux, ne fassent involontairement échec à leur mise en œuvre* »³. Autrement dit, il semblerait que l'assistance des opérateurs viserait à restreindre ou remettre en cause leurs efforts en matière de cybersécurité pour ne pas compromettre l'efficacité d'une cyberopération de renseignement. Il ne s'agit donc pas d'opérations matérielles de collecte ou de transmission de données aux services par les opérateurs, ce qui devrait exclure l'application du droit de l'Union européenne⁴. Comme pour la technique du « *IMSI-catcher* », le texte aurait pu préciser qu'il ne s'agit pas d'opérations matérielles visant à collecter et transmettre des données. Le législateur aurait pu même prévoir une distinction de principe entre les opérations matérielles relatives aux techniques de recueil de données via les opérateurs et celles relatives aux techniques mises en œuvre directement par les services.

¹ A ce sujet, voir F. Vadillo, *Quand l'Etat de droit rencontre l'Etat secret : cadre et garanties du recours aux techniques de recueil de renseignement*, in *Le droit du renseignement*, op. cit., p. 97 et 98.

² Article L. 871-6 du code de la sécurité intérieure.

³ Sur ce point, voir R. Gauvain et L. Kervran, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, op. cit., p. 74 et suivantes ; P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement. Commentaire de la loi n° 2021-998 du 30 juillet 2021*, op. cit.

⁴ En ce sens, voir Etude d'impact, *Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative*, op. cit., p. 161.

C - Les « cyber-patrouilles »

Technique d'infiltration numérique, les « cyber-patrouilles » ont été introduites, pour la première fois, en 2007 dans le code de procédure pénale sous les termes de « l'enquête sous pseudonyme »¹. Le champ d'application de cette technique s'est progressivement étendu avant d'être généralisé dans les enquêtes de police judiciaire en matière de criminalité organisée par la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme². Il s'agit pour des officiers et les agents habilités de police judiciaire de pouvoir participer, sous pseudonyme, à des échanges électroniques avec des personnes suspectes et de collecter des données sur ces dernières ou de partager avec elles, en réponse à une demande expresse, des contenus illicites sans être pénalement responsable et à la condition de ne pas inciter à la commission d'une infraction³.

Avec le développement des réseaux sociaux et des « réseaux souterrains numériques » comme le Darkweb, les cyber-patrouilles peuvent se révéler un outil précieux de surveillance en ligne de la criminalité organisée ou encore du terrorisme⁴. D'autant plus lorsque la Cour de cassation considère que la création par les forces de l'ordre, en l'occurrence le FBI américain, d'un site en ligne de surveillance et d'enregistrement des messages électroniques sur les techniques de fraude à la carte bancaire n'est pas constitutif d'une provocation à la commission d'une infraction⁵, méthode qui peut s'avérer également utile en matière de

¹ L'article 35 de la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance a introduit les « cyber-patrouilles » aux articles 706-35-1 et 706-47-3 du code de procédure pénale, pour les infractions relatives à la traite des êtres humains, au proxénétisme et aux atteintes aux mineurs.

² A ce sujet, voir F. -N. Buffet et Y. Détraigne, *Rapport sur le projet de loi de programmation 2018-2022 et de réforme pour la justice et sur le projet de loi organique relatif au renforcement de l'organisation des juridictions*, Sénat, 3 octobre 2018, p. 196 et 197.

³ Article 706-87-1 du code de procédure pénale.

⁴ En ce sens, voir M. Quémener, *Le terrorisme face au cyberspace*, AJ Pénal 2013, p. 446 et M. Quémener, *Enquête dans le Darkweb*, Dalloz IP/IT 2017, p. 83.

⁵ Cass. crim., 30 avr. 2014, n° 13-88.162 : « Attendu que, pour rejeter leurs requêtes, prises de ce que la procédure serait fondée sur un stratagème les ayant provoqués à la commission d'une infraction, l'arrêt énonce, notamment, que M. X... avait déjà manifesté sur d'autres sites son intérêt pour les techniques de fraude à la carte bancaire et pour l'utilisation d'internet à cette fin ; que les juges ajoutent que le site de surveillance et d'enregistrement des messages échangés a seulement permis de rassembler les preuves de la commission de fraudes à la carte bancaire et d'en identifier les auteurs, aucun élément ne démontrant qu'il ait eu pour objet d'inciter les personnes qui l'ont consulté à passer à l'acte ; Attendu qu'en l'état de ces constatations, d'où il résulte qu'il n'y a pas eu, de la part des autorités américaines, de provocation à la commission d'infractions, la chambre de l'instruction, qui

renseignement. Dès 2013, la mission d'évaluation du cadre juridique des services de renseignement de l'Assemblée nationale avait suggéré de transposer cette technique en droit du renseignement¹, ce que la loi du 24 juillet 2015 a concrétisé.

Inséré dans la loi relative au renseignement par amendement², le dispositif de « cyber-patrouilles administratives » a été codifié à l'article L. 863-1 du code de la sécurité intérieure et reprend pour l'essentiel le dispositif prévu en matière de police judiciaire³. Néanmoins, il convient de relever des différences substantielles entre les deux dispositifs.

D'abord, les agents des services de renseignement peuvent entrer en contact en ligne avec des personnes susceptibles de porter atteinte aux intérêts fondamentaux de la Nation relevant des finalités du renseignement⁴ en utilisant une identité d'emprunt ou une fausse qualité sous l'autorité d'un agent chargé de superviser ou de coordonner la mission⁵. Le dispositif de renseignement va plus loin que celui prévu en matière judiciaire qui ne permet que l'usage d'un pseudonyme en ligne et se rapproche alors du dispositif de l'infiltration humaine plus contraignant de l'article 706-81 du code de procédure pénale. Ce dernier prévoit un régime d'autorisation à la différence de l'enquête sous pseudonyme. De son côté, l'article L. 863-1 du code de la sécurité intérieure n'a pas fait entrer les cyber-patrouilles administratives dans le régime des techniques soumises à autorisation du Premier ministre, mais le législateur a considéré que l'intervention d'un agent superviseur ou coordonnateur caractérisait en réalité un régime

a répondu aux articulations essentielles des mémoires dont elle était saisie, a justifié sa décision sans méconnaître les dispositions conventionnelles invoquées ».

¹ Cf. J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 46 et 47.

² Séance du jeudi 16 avril 2016 de l'Assemblée nationale, Amendements n° 243 rectifié, 416 rectifié (sous-amendement).

³ Article L863-1 : « Dans l'accomplissement de leurs missions définies au titre Ier du présent livre, les agents individuellement désignés et habilités des services mentionnés à l'article L. 811-2 ou des services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 peuvent procéder aux actes suivants sans en être pénalement responsables : 1° Être en contact, par le moyen d'échanges électroniques et dans les conditions prévues à l'article L. 861-2, avec des personnes susceptibles de porter atteinte aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ; 2° Extraire, acquérir ou conserver par ce moyen des données sur les personnes mentionnées au 1° du présent article ; 3° Extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie. Ces actes ne peuvent constituer une incitation à commettre des infractions, sous peine d'un an d'emprisonnement et de 30 000 € d'amende ».

⁴ Article L. 811-3 du code de la sécurité intérieure.

⁵ Article L. 861-2 du code de la sécurité intérieure.

d'autorisation¹. Sur ce point, on peut s'interroger de savoir si les actes autorisés à l'article L. 863-1 du code de la sécurité intérieure ne peuvent être réalisés que dans les conditions de l'article L. 861-2 du même code. En outre, la question se pose de savoir si les agents des services de renseignement peuvent procéder à des enquêtes sous pseudonyme, c'est-à-dire sans nécessairement utiliser une identité d'emprunt ou une fausse qualité. On peut soutenir que si les services peuvent faire usage d'une identité d'emprunt, ils peuvent également faire usage d'un pseudonyme selon le proverbe « qui peut le plus peut le moins ». Le législateur de 2015 avait d'ailleurs qualifié de « cyber-patrouilles administratives » le dispositif par renvoi à l'enquête sous pseudonyme prévue en matière de police judiciaire. A notre sens, il nous apparaît également plus logique que le législateur ait souhaité placer dans tous les cas les cyber-patrouilles administratives sous l'autorité d'un agent superviseur ou coordonnateur, que ce soit lors d'une infiltration sous pseudonyme ou faisant usage d'une identité d'emprunt ou d'une fausse qualité. Par ailleurs, on notera que si le législateur de 2015 a envisagé ces dispositions dans un chapitre du code de la sécurité intérieure relatif aux agents des services de renseignement², elles auraient pu tout aussi bien faire l'objet d'un chapitre dans les techniques de recueil de renseignement.

Ensuite, les cyber-patrouilles administratives sont principalement portées sur la prévention du terrorisme en ce que l'article L. 863-1-3° ne permet que l'échange de contenus provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie. On ne peut que regretter cette limitation au regard de l'intérêt que semble présenter cette technique en matière de criminalité organisée. Cette précision permet toutefois aux services de pouvoir consulter régulièrement des sites web et d'échanger « en réponse à une demande expresse » des propos en ligne à caractère terroriste sans être pénalement responsable ou caractériser une incitation à la commission d'infractions. Il reste qu'en dehors des dispositions de l'article L. 863-1-3° les agents des cyber-patrouilles

¹ En ce sens, voir P. Bas, *Rapport sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif au renseignement et sur la proposition de loi organique relative à la nomination du président de la CNCTR*, Sénat, 20 mai 2015, p. 101.

² Chapitre III du Titre VI du Livre VIII du code de la sécurité intérieure.

administratives sont tenus de ne pas inciter à commettre des infractions sous peine d'être pénalement poursuivis.

Ces dernières années, l'extension du recours au dispositif judiciaire d'enquête sous pseudonyme a été contesté, notamment au regard du droit au respect de la vie privée, ce qui pourrait impacter le dispositif retenu en matière de renseignement. Plus particulièrement, l'absence de garanties procédurales dans l'article 706-87-1 du code de procédure pénale a été dénoncée dans le cadre d'une QPC soulevée devant la chambre de l'instruction de la cour d'appel de Paris en novembre 2017. Un an plus tard, la Cour de cassation a cependant refusé de transmettre la QPC jugeant notamment que cette technique ne constitue pas une intrusion dans la vie privée de la personne avec qui l'enquêteur échange des messages puisqu'elle est « *libre de répondre aux dits messages en appréciant librement le contenu de sa réponse* »¹. L'interprétation de la haute juridiction judiciaire n'a pas fait l'unanimité. Il a pu être soutenu que l'absence d'autorisation et de durée maximale dans la collecte des données sur les personnes en contact avec les enquêteurs peuvent constituer une collecte de données personnelles portant atteinte au respect de la vie privée ou encore que l'absence de ces garanties puisse notamment aboutir dans le temps à une provocation à la commission d'une infraction². Rejoignant ces conclusions³, les parlementaires ont finalement décidé de revoir le dispositif judiciaire dans la loi de programmation 2018-2022 et de réforme pour la justice⁴. Désormais, le nouvel article 230-46 du code de procédure pénale prévoit que les actes réalisés sous pseudonyme sont effectués sous le contrôle du procureur de la République ou du juge d'instruction. L'article prévoit également la nécessité d'une autorisation des magistrats pour « *acquérir tout contenu, produit, substance, prélèvement ou service, y compris illicite, ou transmettre en réponse à une demande expresse des contenus illicites* »⁵. Ajoutons

¹ Cass. crim., 7 févr. 2018, n° 17-90.026.

² En ce sens, voir G. Dumenil, *La nécessité urgente d'encadrer procéduralement la mesure de cyber-infiltration*, Droit pénal n° 9, Septembre 2018, étude 22.

³ Cf. F. -N. Buffet et Y. Détraigne, *Rapport sur le projet de loi de programmation 2018-2022 et de réforme pour la justice et sur le projet de loi organique relatif au renforcement de l'organisation des juridictions*, Sénat, 3 octobre 2018, p. 198 et 199.

⁴ Article 45 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

⁵ Article 230-46-3° du code de procédure pénale.

que la solution retenue par les parlementaires a été validée par le Conseil constitutionnel dans sa décision du 21 mars 2019 sur la loi de programmation 2018-2022¹. L'évolution du cadre juridique de l'enquête judiciaire sous pseudonyme pourrait inspirer une modification de l'article L. 863-1 en matière de renseignement. Il pourrait ainsi être envisagé de placer le dispositif sous le contrôle de la CNCTR et de renforcer le rôle de l'agent superviseur ou coordonnateur qui pourrait être, par exemple, plus clairement mentionné à l'article L. 863-1-3° tout en ajoutant les contenus mentionnés à l'article 230-46-3° en plus de ceux à caractère terroriste déjà prévus par le texte.

Notons enfin que si la loi relative au renseignement a transposé des techniques de police judiciaire qui sont applicables sur le territoire national, rien n'empêche pour les cyber-patrouilles d'échanger en ligne avec des personnes situées à l'étranger. On pourrait donc affirmer que les cyber-patrouilles constituent une technique mixte de surveillance pouvant contribuer aux mesures numériques de renseignement extérieur.

¹ Décision n° 2019-778 DC du 21 mars 2019 (considérants 151 à 157).

§3. L'affirmation de mesures numériques de renseignement extérieur

En dehors du « hertzien ouvert » pouvant porter sur la surveillance des ondes à l'international¹, deux types de mesures peuvent être distinguées : les mesures mises en œuvre portant atteintes aux systèmes d'information à l'étranger et les mesures de surveillance des communications électroniques internationales.

A - Les mesures mises en œuvre portant atteintes aux systèmes d'information à l'étranger

Ces mesures ne constituent pas une technique de renseignement proprement dite. En réalité, il s'agit d'une « excuse pénale » spécifique pour les cyberopérations de renseignement extérieur², notamment pour les actions « offensives »³. L'article 18 de la loi relative au renseignement du 24 juillet 2015 a créé un nouvel article 323-8 dans le code pénal qui exclut l'application du chapitre III du titre II du livre III du code pénal relatif aux atteintes aux systèmes d'information à certaines mesures prises par des agents habilités des services de renseignement. Toutefois, l'excuse pénale n'est pas absolue puisqu'elle ne concerne que les infractions d'atteintes aux systèmes d'information⁴. Les conséquences criminelles ou délictuelles d'une attaque informatique à l'étranger commise par un agent (atteinte à la population ou violences involontaires par exemple) pourraient donc engager sa responsabilité pénale conformément à l'article L. 862-2 du code de la sécurité intérieure⁵.

Pour bénéficier des dispositions de l'article 323-8 du code pénal, les mesures concernées doivent répondre à deux conditions :

- elles doivent être mise en œuvre pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'article L.

¹ Cf. supra. §1 de la Section I du Chapitre I du Titre I de la Ière Partie.

² En ce sens, voir J. -J. Urvoas, *Rapport sur le projet de loi relatif au renseignement*, op. cit., p. 49.

³ En ce sens, voir P. Bas, *Rapport sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif au renseignement et sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, op. cit., p. 121.

⁴ En ce sens, voir Etude d'impact, *Projet de loi relatif au renseignement*, op. cit., p. 78.

⁵ L'article L. 862-2 rappelle que « les agents des services spécialisés de renseignement sont pénalement responsables de leurs actes dans les conditions définies au titre II du livre Ier du Code pénal ».

811-3 du code de la sécurité intérieure¹, ce qui comprend les atteintes à des systèmes d'information localisés à l'étranger, peu importe que les mesures aient été prises depuis le territoire national ou non² ;

- elles doivent être mises en œuvre par des agents désignés par le Premier ministre relevant des services de renseignement du premier cercle³. Il devrait s'agir principalement d'agents relevant de la DRM ou de la DGSE qui participent à la cyberdéfense.

Lorsque ces conditions sont réunies, l'article 323-8 offre une protection aux agents concernés contre les risques de poursuites en France sur le fondement des articles 323-1 à 323-7 du code pénal⁴.

Le dispositif a pu être comparé avec la protection pénale des militaires en opération extérieure prévue à l'article L. 4123-12-II du code de la défense⁵. Néanmoins, les conditions entourant l'excuse pénale prévue pour les militaires sont différentes. Elle n'est invocable que lorsque les mesures concernées prises par le militaire étaient nécessaires à l'exécution de sa mission dans le cadre d'une opération militaire se déroulant hors du territoire national et qu'elles étaient mises en œuvre dans le respect des règles du droit international. L'article 323-8 du code pénal est de portée plus générale puisqu'il exclut la compétence de la loi pénale française en matière d'atteintes aux systèmes d'information dès lors que les mesures prises par l'agent habilité visaient à assurer, à l'étranger, la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code de la sécurité intérieure. Il n'est donc pas requis que l'agent ait agi dans le cadre d'une opération déterminée et pour les nécessités de sa mission. Néanmoins, la combinaison des articles 323-8 du code pénal, de L. 811-2 et de L. 811-3 du code de la sécurité intérieure laisse entendre que les mesures concernées doivent

¹ Sur ce point, voir P. Bas, *Rapport sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif au renseignement et sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, op. cit., p. 121.

² En ce sens, voir Etude d'impact, *Projet de loi relatif au renseignement*, op. cit., p. 78.

³ Sur ce point, voir P. Bas, *Rapport sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif au renseignement et sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, op. cit., p. 121.

⁴ Ibid., p. 120 et 121.

⁵ En ce sens, voir Etude d'impact, *Projet de loi relatif au renseignement*, op. cit., p. 78.

s'inscrire dans une mission de recherche, de collecte et d'exploitation des renseignements portant sur les finalités énumérées à l'article L. 811-3. L'excuse pénale ne devrait donc pas être invoquée par les services de renseignement pour une cyberopération offensive visant à détruire des systèmes d'information étrangers, ce type d'opération relevant normalement du Commandement de la cyberdéfense (COMCYBER)¹. Cependant, en vertu de l'article L. 811-2, elle pourrait se voir appliquer aux agents habilités des services de renseignement qui ont contribué par des mesures cyber à l'entrave d'une menace ou d'un risque entrant dans le champ des finalités de l'article L. 811-3, comme par exemple en matière de cyberdéfense en perturbant des systèmes d'information étrangers à l'origine d'une cyberattaque de grande ampleur visant la France. En revanche, on peut regretter l'absence de référence au respect des règles du droit international, notamment au regard des développements du droit international applicable aux cyberopérations².

La création d'une excuse pénale spécifique n'était pas nécessaire pour certains auteurs qui ont souligné que les règles relatives à la protection des agents s'articulent avec « *les conditions normales d'application de la responsabilité pénale* »³ et que l'article 122-4 du code pénal rappelle que les agents ne sont pas pénalement responsables de leurs actes prescrits par la loi ou le règlement ou par une autorité légitime⁴. Quoi qu'il en soit, on relèvera que cette excuse pénale concerne les mesures et non les agents à la différence de celle de l'article L. 4123-12 du code de la défense qui vise directement l'irresponsabilité pénale des militaires. Cette autre différence peut prêter à confusion en laissant penser qu'il s'agit de nouvelles mesures de surveillance pouvant être mises en œuvre sans autorisation et échappant à tout contrôle, notamment celui de la CNCTR.

Cette dernière interprétation a notamment été retenue par les associations *La Quadrature du Net et autres* qui ont contesté le dispositif devant le Conseil d'Etat

¹ Pour en savoir plus, visitez la page dédiée sur COMCYBER du site internet du ministère des Armées : <https://www.defense.gouv.fr/ema/organismes-interarmees/le-comcyber/le-comcyber/comcyber>.

² A ce sujet, voir le Titre II de la Seconde Partie.

³ En ce sens, voir R. Parizot, *Surveiller et prévenir... à quel prix ? Loi n° 2015-912 du 24 juillet 2015 relative au renseignement*, op. cit.

⁴ En ce sens, voir E. Dreyer, *Diversité des atteintes aux « STAD »*, Le Lamy droit pénal des affaires, mis à jour 11/2020.

par voie d'exception d'inconventionnalité lors de leur recours pour excès de pouvoir dirigé contre le décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement¹. Dans sa décision du 26 juillet 2018, le Conseil d'Etat a finalement débouté la demande des associations requérantes au motif que le décret litigieux « *n'a été pris ni sur le fondement ni pour l'application des dispositions de l'article 323-8 du code pénal* »². Cette solution semble logique bien qu'il ait été supposé que la haute juridiction administrative aurait pu contrôler la conventionnalité de l'article 323-8 du code pénal « *qui a pour objet d'organiser une exemption pénale par renvoi à des situations juridique déterminées par la voie réglementaire* »³. En revanche, rappelons que le Conseil d'Etat a considéré le dispositif conforme à la Constitution dans son avis sur le projet de loi relatif au renseignement en raison des conditions, vues précédemment, qui encadrent l'excuse pénale⁴.

Sur les contestations des associations requérantes, ces dernières soutenaient la contrariété de l'article 323-8 du code pénal aux stipulations⁵ :

- de la Convention de Budapest de 2001 sur la cybercriminalité, notamment sur l'interdiction faite aux Etats parties à la convention d'exclure la compétence de la loi pénale pour l'infraction de mise à disposition d'éléments permettant d'accéder à un système d'information (article 6) et sur la nécessité pour les Etats parties souhaitant accéder aux données stockées dans un système d'information localisé dans un autre Etat de recueillir le consentement légal et volontaire de la personne autorisée légalement à divulguer les données concernées (article 32) ;
- de la Conv. EDH sur le respect du droit à la vie privée (article 8) et au droit à un recours effectif (article 13) ainsi que sur le droit au respect de ses biens (article 1 du 1^{er} Protocole additionnel). Considérant notamment que l'article 323-8 du code pénal met en place des mesures de surveillance

¹ Requête n° 394922.

² CE, 26 juillet 2018, *La Quadrature du Net et autres* (requête n° 394922).

³ En ce sens, voir C. Santulli, *Droit administratif et droit international*, RFDA 2018, p. 977.

⁴ Avis du Conseil d'Etat sur le projet de loi relatif au renseignement du 12 mars 2015, p. 4.

⁵ Cf. Observations complémentaires des associations *La Quadrature du Net et autres* sur la requête n° 394.922.

secrètes et de collecte et de partage de données personnelles, les requérants soutenaient que les mesures devaient être, au regard de la jurisprudence de la CEDH¹, assorties de garanties minimales telles que la fixation d'une limite à la durée des mesures ou encore l'établissement de précautions et d'une procédure à suivre concernant le traitement et le partage des données collectées.

En ce qui concerne la Convention sur la cybercriminalité, l'article 323-8 du code pénal ne semble pas se heurter à l'obligation du recueil du consentement imposée à l'article 32 qui concerne, en principe, la coopération internationale en matière pénale et donc l'entraide judiciaire². En revanche, une contradiction apparaît avec les stipulations de l'article 6 en ce que l'inapplicabilité de la loi pénale française s'étend à l'ensemble des dispositions de l'article 323-3-1 du code pénal qui incriminent la mise à disposition d'éléments permettant d'accéder à un système d'information.

Du point de vue la Conv. EDH, le dispositif pourrait particulièrement être sanctionné par les juges de Strasbourg sur le fondement du droit au respect à la vie privée si ces derniers retiennent qu'il s'agit de mesures de surveillance et de collecte de données personnelles, notamment en ce que « *le facteur décisif sera le niveau d'atteinte porté à la vie privée de la personne et non la définition technique de cette atteinte* »³. Dans ce cas, les conditions entourant l'excuse pénale ne nous apparaissent pas suffisantes au regard de la jurisprudence de la CEDH. Aussi, le dispositif pourrait être perçu comme une mesure susceptible d'entraîner une surveillance de masse indifférenciée dans l'hypothèse où l'article 323-8 du code pénal servirait de fondement au piratage d'un opérateur de télécommunication et d'Internet étranger en vue de collecter les données des abonnés. A ce sujet, on rappellera l'affaire du piratage de l'opérateur belge Belgacom ou de « l'Opération Socialist » impliquant la NSA et le GCHQ qui s'est déroulée entre 2011 et 2013⁴. Dans cette affaire, la justice belge soupçonnait la NSA et le GCHQ d'avoir piraté une

¹ CEDH, 29 juin 2006, *Weber et Saravia c. Allemagne* (requête n° 54934/00).

² Article 23 de la Convention sur la cybercriminalité « *Principes généraux relatifs à la coopération internationale* ».

³ CEDH, 25 octobre 2015, *R.E. c. Royaume-Uni* (requête n° 62498/11).

⁴ Sur cette affaire, voir A. Guiton, *Belgacom, ou les aléas du piratage entre amis*, Libération, 2 novembre 2018.

filiale internationale de l'opérateur belge afin d'accéder aux communications transitant par les opérateurs étrangers partenaires de Belgacom, notamment d'Afrique et du Moyen-Orient.

En conclusion, l'article 323-8 du code pénal pourrait faire l'objet de modifications sans toutefois remettre en cause l'inapplicabilité de la loi pénale française aux mesures concernées afin de maintenir une protection des agents contre les risques de poursuites en France ou à l'étranger, notamment dans un contexte d'augmentation des cyberattaques et de risque accru de poursuites judiciaires dans ce domaine au niveau international. Il s'agirait donc de conserver l'excuse pénale tout en renforçant les conditions de son application au regard du droit international et des droits de l'homme. Il pourrait être précisé que l'excuse pénale vise les mesures qui produisent leurs effets hors du territoire national, peu importe qu'elles soient mises en œuvre depuis le territoire national ou l'étranger. Comme actuellement prévu, l'exonération de la responsabilité pénale s'appliquerait aux agents de l'Etat habilités et désignés par arrêté du Premier ministre parmi les services de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure. Cependant, le texte pourrait être complété en disposant que l'agent doit agir pour assurer la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code de la sécurité intérieure dans le respect du droit international et dans l'accomplissement de ses missions définies au titre Ier du livre VIII du même code et les textes réglementaires relatifs à son service d'appartenance. Enfin, la question se pose de modifier l'inapplicabilité du chapitre III du titre II du livre III du code pénal pour tenir compte de l'exception du fait d'offrir, de céder ou de mettre à disposition un mot de passe, un code d'accès ou toute donnée permettant d'accéder à tout ou partie d'un système d'information¹.

¹ A ce sujet, voir le Titre II de la Seconde Partie.

B - Les mesures de surveillance des communications électroniques internationales

L'une des innovations importantes du projet de loi relatif au renseignement a été de proposer un encadrement des interceptions des communications électroniques internationales¹. Suivant les raisonnements du Conseil constitutionnel² et du Conseil d'Etat³ sur les exigences constitutionnelles liées à l'exercice des libertés à l'étranger, le dispositif envisagé organisait un régime dérogatoire de collecte et d'exploitation des renseignements qui se voulait plus souple que pour les techniques mises en œuvre sur le territoire national. Il était prévu de préciser le régime applicable dans deux décrets en Conseil d'Etat soumis à l'avis de la CNCTR. Le décret précisant les modalités de mises en œuvre de la surveillance internationale ne devait d'ailleurs pas être publié pour ne pas dévoiler les capacités techniques françaises dans ce domaine. Cependant, le Conseil constitutionnel a censuré le dispositif, considérant que législateur n'avait pas épuisé sa compétence pour garantir le respect des libertés⁴.

En septembre 2015, deux propositions de loi de l'Assemblée nationale⁵ et du Sénat⁶ reprendront les travaux du projet de loi relatif au renseignement pour « *inscrire au niveau législatif les dispositions qui devaient initialement figurer dans un décret du Conseil d'Etat* »⁷. Comme anticipé par ce dernier lors des débats parlementaires⁸, le Conseil constitutionnel validera finalement les dispositions issues de la proposition de l'Assemblée nationale⁹, celle du Sénat ayant été

¹ En ce sens, voir Etude d'impact, *Projet de loi relatif au renseignement*, op. cit., p. 68 et 69.

² Le Conseil constitutionnel a estimé que certaines obligations constitutionnelles ne s'imposaient pas à l'Etat hors du territoire national (Décision n° 2012-654 DC du 9 août 2012).

³ Le Conseil d'Etat a reconnu un assouplissement possible des garanties pour les personnes situées à l'étranger qui échappent à la juridiction de l'Etat (cf. CE, *Le numérique et les droits fondamentaux*, étude annuelle 2014, p. 214).

⁴ Décision n° 2015-713 DC du 23 juillet 2015 (considérants 76 à 79).

⁵ Cf. P. Adam et P. Nauche, *Proposition de loi relative aux mesures de surveillance des communications électroniques internationales*, Assemblée nationale, 9 septembre 2015.

⁶ Cf. P. Bas, *Proposition de loi relative aux mesures de surveillance des communications électroniques internationales*, Sénat, 21 septembre 2015.

⁷ Cf. P. Adam, *Rapport sur la proposition de loi, après engagement de la procédure accélérée, relative aux mesures de surveillance des communications électroniques internationales*, Assemblée nationale, 16 septembre 2015, p. 6.

⁸ Délibération du Conseil d'Etat du 15 octobre 2015 (n° 390578).

⁹ Décision n° 2015-722 DC du 26 novembre 2015.

abonnée au profit de la première¹. Le dispositif sera enfin consacré avec la promulgation de la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

Prévues au chapitre IV du titre V du livre VIII du code de la sécurité intérieure, les mesures de surveillance portent sur des communications émises ou reçues à l'étranger². Selon les observations complémentaires formulées par le gouvernement devant le Conseil constitutionnel lors de l'examen du projet de loi relatif au renseignement, il s'agit « *des communications dont l'une des terminaisons au moins n'est pas située sur le territoire national* », étant entendu que le terme « terminaison » désigne « *l'extrémité finale d'une communication même si elle emprunte plusieurs nœuds de communication* ». Autrement dit, les terminaisons sont « *les points physiques par lesquels les utilisateurs accèdent à un réseau de communications électroniques ouvert au public* »³.

Dans son rapport d'activité pour l'année 2016, la DPR a tenu à préciser que l'application de la loi du 30 novembre 2015 ne concerne que les communications internationales qui transitent par le territoire national, y compris les communications individualisables relayées par satellites⁴. La possibilité d'intercepter les communications internationales depuis le territoire national a motivé la nécessité d'encadrer cette surveillance par la loi française⁵. On relèvera néanmoins que cette précision n'est pas explicitement affirmée dans les dispositions de la loi du 30 novembre 2015, le texte pouvant alors entretenir la confusion sur les communications concernées. Quoi qu'il en soit, cette précision a pour conséquence d'exclure les communications non rattachables à la France et exclusivement localisées hors du territoire national du champ d'application de la loi française. Les interceptions de ces dernières sont librement mises en œuvre par

¹ Cf. P. Bas, *Rapport sur la proposition de loi, adoptée par l'Assemblée nationale après engagement de la procédure accélérée, relative aux mesures de surveillance des communications électroniques internationales*, Sénat, 21 octobre 2015, p. 16 et suivantes.

² Article L. 854-1 du code de la sécurité intérieure.

³ Article L. 32-3° bis du code des postes et des communications électroniques.

⁴ Cf. P. Adam et P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 71 à 75.

⁵ Cf. Observations complémentaires du gouvernement devant le Conseil constitutionnel lors de l'examen de la loi sur le renseignement.

les services¹. Précisons que c'est dans ce cadre que l'excuse pénale de l'article 323-8 du code pénal a notamment vocation à s'appliquer. Pour autant, ces interceptions doivent être mises en œuvre dans le respect des mesures de surveillance hertzienne lorsque des capacités de renseignement électromagnétique (ROEM) sont utilisées depuis le territoire national ou encore dans le respect du droit international². De même, la loi exclut expressément des mesures de surveillance internationale les communications échangées entre des personnes ou équipements qui sont rattachables à la France par des numéros d'abonnement ou des identifiants techniques³, même si elles transitent par exemple par un serveur situé à l'étranger⁴. La loi exige d'ailleurs la destruction des données recueillies en cas d'interception⁵. De principe, l'interception des communications impliquant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national relève de la loi relative au renseignement, notamment en cas de « communication mixte » lorsqu'une personne située sur le territoire national communique vers l'étranger en utilisant un numéro d'abonnement ou un identifiant rattachable à la France⁶. En revanche, deux exceptions sont prévues au troisième alinéa de l'article L. 854-1 du code de la sécurité intérieure pour l'interception des communications rattachables à la France de personnes situées à l'étranger. Les mesures de surveillance internationale peuvent s'appliquer :

¹ A titre d'exemple, il peut être librement déployé des capacités satellitaires visant à intercepter les communications hertziennes sur l'ensemble du globe. En France, les capacités satellitaires d'interception sont en plein développement avec la réalisation du Programme CERES (capacité de renseignement électromagnétique spatiale) débuté en 2015. S'appuyant sur une constellation de trois satellites, le dispositif devrait pouvoir intercepter, caractériser et localiser sur l'ensemble du globe des communications électroniques ainsi que de cartographier et d'analyser les émetteurs de signaux électromagnétiques d'intérêt (cf. page web de la DGA dédiée au Programme CERES sur le site du Ministère des Armées : <https://www.defense.gouv.fr/dga/equipement/information-communication-espace/le-programme-ceres-capacite-de-renseignement-electromagnetique-spatiale>).

² Sur ce point, voir Titre II de la Seconde Partie.

³ Par exemple, l'indicatif téléphonique international +33 pour la France ou l'adresse IP correspondant au territoire national.

⁴ En ce sens, voir Observations complémentaires du gouvernement devant le Conseil constitutionnel lors de l'examen de la loi sur le renseignement.

⁵ Alinéa 5 de l'article L. 854-1 du code de la sécurité intérieure.

⁶ A ce sujet, voir P. Adam et P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 72.

- aux personnes faisant l'objet d'une interception de sécurité lorsqu'elles ont quitté le territoire. Il s'agit d'un « droit de suite » permettant d'assurer la continuité des interceptions¹ ;
- aux personnes détectées à l'étranger comme présentant une menace pour les intérêts fondamentaux de la Nation.

L'approche retenue par la loi du 30 novembre 2015 repose sur le critère géographique, c'est-à-dire que la ou les personnes surveillées, françaises ou étrangères, sont situées hors du territoire national². Cette approche a pour effet de ne pas prendre en compte les relations qu'entretiennent les personnes surveillées avec la France, à l'exception des personnes présentant une menace pour les intérêts fondamentaux de la Nation. Elle s'oppose à l'approche américaine dont le régime du *Foreign Intelligence Surveillance Act* (FISA), notamment amendé en 2008 sur la surveillance des communications des personnes situées à l'étranger, opère une distinction entre les citoyens et résidents américains (« USPER ») et les non-américains (« non-USPER »)³. A la différence des premiers, les seconds ne sont pas protégés par le Quatrième amendement de la Constitution des Etats-Unis qui exige de sérieuses justifications et l'établissement d'un mandat motivé pour procéder à des interceptions. Cette distinction a pour conséquence de permettre aux autorités américaines d'intercepter librement les données des « non-USPER » qui transitent par les Etats-Unis ou qui y sont hébergées. En réalité, la différence entre les approches française et américaine concerne les garanties applicables ou non aux personnes surveillées. Sur ce point, la loi française semble plus protectrice en introduisant un régime d'autorisation, que les communications interceptées concernent des personnes étrangères ou françaises.

En ce qui concerne les mesures de surveillance, la loi du 30 novembre 2015 organise un système de collecte et d'exploitation des données qui s'inspire des considérations de la CEDH sur le modèle britannique dégagées dans son arrêt

¹ Sur ce point, voir P. Bas, *Rapport sur la proposition de loi, adoptée par l'Assemblée nationale après engagement de la procédure accélérée, relative aux mesures de surveillance des communications électroniques internationales*, op. cit., p. 22.

² En ce sens, voir J. -J. Urvoas, *Rapport sur le projet de loi relatif au renseignement*, op. cit., p. 219 à 225.

³ Sur ce point, voir Etude du Parlement européen sur les programmes de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE, septembre 2013, p. 24 à 30.

Liberty et autres du 1^{er} juillet 2008¹. L'article 3 §2 de la loi sur l'interception des communications de 1985 (*Interception of Communications Act 1985*) autorisait les autorités britanniques investies d'un mandat à intercepter les communications à destination ou provenance de l'étranger et à exploiter les données recueillies à l'aide d'un système numérique de recherche par mots-clés sans toutefois préciser les catégories de communications et de données ciblées par les mesures de surveillance. Si ce manque de clarté a été sanctionné par la Cour, il reste que cette dernière n'a pas remis en question l'adoption d'une législation spécifique en matière d'interception de communications de personnes situées à l'étranger tout en indiquant les exigences législatives à suivre à partir du cas d'espèce britannique. S'inspirant de ce dernier, la loi française a donc prévu un dispositif qui se décompose en deux étapes avec trois niveaux d'autorisations accordées par le Premier ministre afin d'éviter les atteintes disproportionnées au respect au droit à la vie privée².

La première étape, les interceptions. Le Premier ministre autorise les interceptions sur les réseaux de communications électroniques qu'il a préalablement désigné dans une décision motivée³. Il convient de préciser que le terme « réseaux » renvoie à « *toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de commutation et de routage* »⁴. Ces réseaux peuvent donc être hertziens ou physiques (réseaux satellitaires, terrestres ou encore des réseaux électriques utilisés pour l'acheminement des communications). L'autorisation est accordée à la DGSE qui intercepte l'ensemble des « flux d'informations » transitant par le réseau désigné par le Premier ministre⁵, c'est-à-dire les correspondances et les données de connexion⁶. Selon la DPR, « *les interventions techniques sont réalisées*

¹ CEDH, 1^{er} juillet 2008, *affaire Liberty et autres c. Royaume-Uni* (requête n° 58243/00).

² En ce sens, voir J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 67 à 71.

³ Article L. 854-2-I du code de la sécurité intérieure.

⁴ Article L. 32-2° du code des postes et des communications électroniques.

⁵ Sur ce point, voir P. Adam et P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 71.

⁶ Alinéa 2 de l'article L. 854-1 du code de la sécurité intérieure.

juridiquement par le Groupement interministériel de contrôle »¹, ce qui semble signifier qu'en pratique le GIC sollicite les opérateurs concernés soumis à la loi française et prend en charge les communications interceptées rattachables à la France². Notons que les opérations matérielles nécessaires à la mise en œuvre des interceptions sur les réseaux ciblés sont effectuées par les opérateurs de télécommunications concernés dans les mêmes conditions que pour les interceptions de sécurité³.

La deuxième étape, les exploitations. Les services de renseignement du premier cercle peuvent être autorisés par le Premier ministre, sur demande motivée de leur ministre de tutelle, à exploiter les données recueillies et traitées par la DGSE pour l'une ou plusieurs des finalités de l'article L. 811-3 du code de la sécurité intérieure selon deux types d'autorisation :

- l'autorisation d'exploitation non individualisée des données de connexion⁴, notamment par la mise en œuvre de « traitements automatisés ». Ces traitements concernent par exemple l'exploitation statistique des données de connexion recueillies⁵. Il ressort des débats parlementaires que les traitements automatisés renvoient directement à la technique algorithmique de l'article L. 851-3 du code de la sécurité intérieure permettant de filtrer les données de connexion non nominatives pour détecter des « signaux faibles »⁶ ;
- l'autorisation d'exploitation des correspondances et des données de connexion ou seulement de ces dernières⁷. Elle peut concerner des zones géographiques ou des organisations, des groupes de personnes ou des

¹ A ce sujet, voir J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 68.

² Sur ce point, voir P. Adam et P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 71 et 72.

³ Article L. 854-7 du code de la sécurité intérieure.

⁴ Article L. 854-2-II du code de la sécurité intérieure.

⁵ Cf. P. Adam et P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 71.

⁶ Cf. P. Bas, *Rapport sur la proposition de loi, adoptée par l'Assemblée nationale après engagement de la procédure accélérée, relative aux mesures de surveillance des communications électroniques internationales*, op. cit., p. 25.

⁷ Article L. 854-2-III du code de la sécurité intérieure.

personnes. Par ailleurs, la loi n'empêche pas le gouvernement de délimiter l'exploitation des données recueillies à certains numéros ou identifiants ou encore de soumettre certaines communications à des conditions d'accès particulières comme il avait été proposé lors des débats parlementaires¹.

Selon la DPR, les traitements opérés sur les communications internationales interceptées sont assurés par la DGSE qui « *met à disposition des autres services de renseignement concernés les flux d'informations qui ont été recueillies* »². Toutefois, les correspondances interceptées de communications rattachables à la France sont exploitées au GIC dans les mêmes conditions que pour les interceptions de sécurité selon l'article L. 854-8 du code de la sécurité intérieure³.

Contrairement à la philosophie de la loi relative au renseignement qui fonde la recherche et la collecte de renseignements sur le ciblage des personnes, la loi relative aux mesures de surveillance internationale semble se rapprocher de la conception américaine « *où la NSA intercepte et stocke massivement les flux de communication puis sollicite des autorisations pour exploiter les informations conservées* »⁴. Le choix opéré par le législateur de 2015 constituerait alors un changement philosophique dans l'action de la DGSE par rapport à ce qui avait été exprimé par la DPR dans son rapport pour l'année 2014⁵. Néanmoins, la loi du 30 novembre 2015 reste attachée, à notre sens, à la proportionnalité de la surveillance en délimitant les réseaux pouvant faire l'objet d'une surveillance et en distinguant les communications internationales et celles rattachées à la France ainsi qu'en organisant des dispositifs d'exploitation différents des renseignements fondés sur les deux catégories de données de contenu et de connexion.

Si le dispositif nous apparaît également répondre aux critiques formulées par la CEDH dans sa décision de 2008 sanctionnant le régime britannique de

¹ Cf. P. Bas, *Rapport sur la proposition de loi, adoptée par l'Assemblée nationale après engagement de la procédure accélérée, relative aux mesures de surveillance des communications électroniques internationales*, op. cit., p. 26.

² Cf. P. Adam et P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 71.

³ Ibid., p. 72.

⁴ En ce sens, voir J. -J. Urvoas et J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, op. cit., p. 133.

⁵ Ibid.

surveillance internationale, sa compatibilité au regard tant de la Conv. EDH que du droit de l'Union européenne a été soulevée à deux reprises devant le Conseil d'Etat. La question de l'application du droit de l'Union européenne a été posée une première fois dans le cadre du contentieux des techniques de renseignement par l'eurodéputée Sophie in't Veld¹. Néanmoins, cette dernière a été déboutée de l'ensemble de ses demandes en juin 2018 sans que la haute juridiction n'ait eu à se prononcer sur la conventionnalité des mesures de surveillance internationale². Un mois plus tard, le Conseil d'Etat s'est finalement prononcé à la fois sur l'application du droit de l'Union européenne et sur la compatibilité des mesures concernées avec les articles 8 et 13 de la Conv. EDH à l'occasion, cette fois-ci, du contentieux des décrets relatifs au renseignement³. Concernant les deux articles de la convention, le Conseil d'Etat n'a pas relevé de contrariété avec les dispositions relatives aux mesures de surveillance internationale. Pour ce qui est du droit de l'Union européenne, la haute juridiction administrative a considéré que les mesures prévues par la loi du 30 novembre 2015 n'entrent pas dans son champ d'application car elles sont directement mises en œuvre par l'Etat sans régir les activités des opérateurs en leur imposant des obligations spécifiques. Cette solution a été réaffirmée en avril 2021⁴.

Outre les critiques portées sur la conventionnalité des dispositions de la loi du 30 novembre 2015, il a été souligné la nécessité de modifier le dispositif législatif afin de répondre à certaines incohérences pratiques qui ont été relevées dans l'articulation de la surveillance internationale avec le renseignement intérieur après trois années d'expérience. L'interdiction de principe « *d'exploiter les données légalement recueillies au titre de la surveillance des communications internationales pour apprécier la menace que présente un résident français en France du fait de ses liens hors du territoire national* » a été jugée « *difficilement compréhensible* » au regard notamment du caractère transnational des menaces

¹ Cf. A. Guiton, *Surveillance internationale : l'eurodéputée Sophie in 't Veld déboutée par le Conseil d'Etat*, Libération, 27 juin 2018.

² CE, 20 juin 2018, *Mme B...D...A... 't Veld* (requêtes n° 404012 et 404013).

³ CE, 26 juillet 2018, *FRENCH DATA NETWORK et autres* (requête n° 394922).

⁴ CE, 21 avril 2021, *FRENCH DATA NETWORK et autres* (requête n° 393099, point 95).

du terrorisme et des cyberattaques¹. Il a donc été proposé, par voie d'amendement, d'introduire la possibilité pour les services de renseignement « *d'exploiter les communications de personnes communiquant depuis la France mais interceptées dans le cadre d'une communication internationale* »² dans la loi de programmation militaire (LPM) pour les années 2019 à 2025. En accord avec le Conseil d'Etat³ et la CNCTR⁴, le dispositif retenu à l'article 37 de la loi de programmation militaire du 13 juillet 2018⁵ a créé trois nouvelles mesures.

La première mesure constitue en réalité un prolongement de l'étendue de l'autorisation d'exploitation des communications prévues à l'article L. 854-2-III du code de la sécurité intérieure. Cette dernière vaut désormais autorisation de « vérifications ponctuelles » sur les données de connexion interceptées afin de détecter une menace sur les intérêts fondamentaux de la Nation dans les relations entre des numéros d'abonnement ou des identifiants techniques rattachables à la France et des zones géographiques, organisations ou personnes surveillées au titre des mesures de surveillance des communications internationales⁶. Les vérifications ponctuelles envisagées présentent trois caractéristiques : il s'agit d'opérations très rapides de quelques minutes qui sont non répétées et qui permettent d'établir un graphe relationnel ou la présence d'une personne à l'étranger⁷. Si les vérifications portent en principe uniquement sur les données de connexion, elles peuvent également porter sur des correspondances rattachables à la France pour :

- détecter, de manière urgente, une menace terroriste ;

¹ Sénat, séance du 22 mai 2018 (compte rendu intégral des débats).

² Sur ce point, voir Y. Braun-Pivet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018*, Tome 1, DPR, 11 avril 2019, p. 42.

³ CE, sect. admin., avis, 4 mai 2018 (n° 394761).

⁴ Délibération de la CNCTR n° 1/20185 du 9 mai 2018.

⁵ Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

⁶ Article L. 854-2-IV du code de la sécurité intérieure.

⁷ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 49 et 50.

- détecter, à des fins d'analyse technique, des éléments de cyberattaques susceptibles de porter atteinte à l'indépendance nationale, l'intégrité du territoire et à la défense nationale.

Ces « levées de doute » n'ont pas été considérées comme des mesures de surveillance individuelle par le Conseil d'Etat dans son avis du 4 mai 2018 et la CNCTR dans sa délibération du 9 mai 2018. En effet, ces mesures peuvent servir, tout au plus, à préparer la mise en œuvre ou non d'une surveillance individuelle¹. Dans le cas où une surveillance se révélerait nécessaire, il est d'ailleurs prévu que l'exploitation des données interceptées doit faire l'objet d'une autorisation soit dans le cadre de la surveillance nationale, selon le régime des données de connexion ou celui des interceptions de correspondances, soit dans le cadre de la seconde nouvelle mesure prévue à l'article L. 854-2-V du code de la sécurité intérieure.

Cette deuxième mesure constitue une nouvelle dérogation au principe posé par l'article L. 854-1 du code de la sécurité intérieure sur l'interdiction d'exploiter des communications rattachables à la France dans le cadre des mesures de surveillance internationales. Dans les conditions de l'article L. 854-2-III, les services de renseignement peuvent ainsi être autorisés à exploiter les communications ou les seules données de connexion interceptées de personnes situées sur le territoire national utilisant des numéros d'abonnement ou des identifiants rattachables à la France pour communiquer avec l'étranger. Cependant, l'autorisation ne peut être accordée que pour les finalités 1°, 2°, 4°, 6° et 7° mentionnées à l'article L. 811-3 du code de la sécurité intérieure². Comme souhaité par la CNCTR dans sa délibération du 9 mai 2018, un contingentement des autorisations a été mis en place. Néanmoins, il a été limité aux autorisations d'exploitation des correspondances contrairement aux recommandations de la CNCTR qui englobait les données de connexion³. Cette solution est compréhensible puisque le contingentement a été envisagé par la CNCTR par souci de cohérence

¹ Délibération de la CNCTR n° 1/20185 du 9 mai 2018.

² Les finalités 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 ; la prévention du terrorisme ; la prévention de la criminalité et de la délinquance organisées ; et, la prévention de la prolifération des armes de destruction massive.

³ Cf. CNCTR, *3^{ème} rapport annuel (2018)*, p. 33.

avec les principes régissant les interceptions de sécurité de l'article L. 852-1 du code de la sécurité intérieure¹.

La troisième et dernière mesure élargie les autorisations de surveillance nationale d'accès aux données de connexion, en temps différé² ou en temps réel³, et d'interceptions de sécurité à la mise en œuvre des mesures de surveillance internationale⁴. Autrement dit, les mesures de surveillance nationale concernées peuvent porter également sur « *le recueil et l'exploitation de données équivalentes issues de communications électroniques internationales* »⁵. Précisons que cette nouvelle faculté doit être mise en œuvre dans le respect des garanties qui entourent les autorisations de surveillance nationale concernées. Ajoutons que le Conseil d'Etat et la CNCTR avait insisté pour que cette nouvelle mesure ne s'applique qu'aux autorisations nationales accordées postérieurement à la modification de la loi du 30 novembre 2015, ce qui pourrait traduire un certain changement d'échelle dans la quantité des données traitées par les services et dans le nombre de personnes susceptibles d'être concernées par les mesures de surveillance.

L'affirmation du régime de surveillance des communications internationales en droit français et ses évolutions soulèvent plusieurs remarques. Comme ses homologues, la France a opéré en 2015 une distinction légale entre la surveillance nationale et la surveillance internationale selon un principe de territorialité en matière de communications électroniques⁶. En outre, les deux régimes de surveillance se distinguent dans leur portée. Alors que la surveillance nationale de la loi du 24 juillet 2015 consacre l'individualisation des techniques de renseignement en ciblant des personnes et leur entourage⁷, les mesures de la loi du 30 novembre 2015 peuvent s'apparenter à de la « surveillance stratégique » en

¹ Délibération de la CNCTR n° 1/20185 du 9 mai 2018.

² Article L. 851-1 du code de la sécurité intérieure.

³ Article L. 851-2 du code de la sécurité intérieure.

⁴ Quatrième alinéa de l'article L. 854-1 du code de la sécurité intérieure.

⁵ Délibération de la CNCTR n° 1/20185 du 9 mai 2018.

⁶ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 46.

⁷ Sur ce point, voir F. Vadillo, *Quand l'Etat de droit rencontre l'Etat secret : cadre et garanties du recours aux techniques de recueil de renseignement*, Le droit du renseignement, op. cit., p. 92.

ce qu'elles visent, au-delà des personnes, des organisations ou des zones géographiques qui « *traduisent donc directement les choix de l'exécutif en termes de stratégie de renseignement extérieur au vu de la réalité des menaces* »¹. Cette surveillance stratégique internationale n'est pas propre à la France et se retrouvait dans la législation britannique sanctionnée par la CEDH dans les arrêts *Liberty et autres* et *Big Brother Watch et autres*. Elle a également été promue en Allemagne dans une loi encadrant, de manière similaire à la loi britannique, la surveillance des télécommunications des étrangers hors du territoire allemand par le Service fédéral de renseignement (Bundesnachrichtendienst - BND). La loi allemande a toutefois été censurée par la Cour constitutionnelle fédérale le 19 mai 2020 pour son manque de précisions et son insuffisance de garanties au regard de la Loi fondamentale de la République fédérale d'Allemagne, notamment son article 10 protégeant le secret des correspondances². Il est intéressant de relever certaines similitudes entre les réserves émises par la Cour et la loi du 30 novembre 2015 comme par exemple la nécessité d'inscrire dans la loi la séparation entre les communications nationales et internationales ou encore entre la surveillance stratégique des communications et la surveillance des personnes³. La législation française nous apparaît donc satisfaisante au regard de la situation à l'étranger.

En revanche, les modifications apportées par la loi de programmation militaire de 2018 tendent à atténuer le principe de territorialité promu par le législateur de 2015 entraînant une augmentation de la surveillance internationale, notamment du fait des autorisations possibles d'exploitation des communications nationales prévues à l'article L. 854-2-V⁴. L'utilisation des mesures de surveillance internationale devrait d'ailleurs continuer de croître en raison de son importance dans la surveillance du cyberspace devenu un « *nouveau terrain d'action des services de renseignement* »⁵.

¹ En ce sens, voir les observations complémentaires du gouvernement devant le Conseil constitutionnel lors de l'examen de la loi sur le renseignement.

² Cour constitutionnelle fédérale allemande, 19 mai 2020, *affaire 1 BvR 2835/17*.

³ Articles L. 854-1 et L. 854-2-II et III du code de la sécurité intérieure.

⁴ Sur ce point, voir CNCTR, *4^{ème} rapport annuel (2019)*, p. 60 et 61.

⁵ A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 266 et suivantes.

Enfin, notons que le renforcement du dispositif légal de la surveillance des communications internationales concerne davantage l'exploitation des données que les techniques d'interception, ce qui nous amène à nous intéresser plus spécifiquement à l'analyse de la montée en puissance des moyens numériques d'exploitation des renseignements.

CHAPITRE II

L'EXPLOITATION NUMERIQUE DES RENSEIGNEMENTS

Les données utiles aux services de renseignement, quel que soit leur source (humaine ou technique), sont analysés numériquement dans des traitements de données (**Section I**) qui devraient s'enrichir de certaines innovations numériques incontournables telles que l'intelligence artificielle (**Section II**). Dans ces domaines historiquement régis par le droit du numérique, le droit du renseignement tend à prendre une place prépondérante pour faire évoluer les capacités d'exploitation numérique des renseignements.

SECTION I : Les traitements de données

Bénéficiant d'un cadre juridique protecteur de l'administration et du secret de la défense nationale, les fichiers de renseignement constituent les principaux traitements de données des services pour analyser les données qu'ils ont collecté (§1). Les services devraient également pouvoir se fonder sur des notions de partage de données appréhendées tant par le droit de la protection des données que par le droit du renseignement : les accès aux fichiers et le rapprochement d'informations qui en découle (§2), les interconnexions (§3) et le partage d'informations (§4).

§1. Les fichiers de renseignement

En matière de surveillance, la notion de « fichiers de police et de renseignement » est relativement ancienne. Si dès l'Ancien Régime, les autorités de police ont pu constituer des fiches sur les citoyens, la notion apparaît véritablement à la fin du XIXème siècle avec le début de la police scientifique¹. L'essor de l'informatique dans les années 1980 a accéléré et facilité l'utilisation des fichiers pour les services de police et de renseignement dans la conservation et le

¹ A ce sujet, voir J. -M. Cotteret et E. Denécé, *Le renseignement au service de la démocratie*, Fauves Editions, 2018, p. 123 et 124.

traitement des informations qu'ils collectent¹. Aujourd'hui, les fichiers représentent un outil quotidien et stratégique pour les services de renseignement parmi les moyens numériques dont ils disposent, notamment pour « *exploiter au mieux le fruit de leurs investigations* »² et « *n'utiliser les techniques de renseignement qu'à titre subsidiaire* »³.

Catégorie particulière des fichiers des forces de sécurité, les fichiers de renseignement ont pour finalité l'anticipation et la prévention des menaces et comprennent, à ce titre, des informations sur des personnes susceptibles de porter atteinte aux intérêts de l'Etat⁴. A la différence des fichiers judiciaires, ils ne concernent pas nécessairement des personnes ayant commis des infractions ou qui sont recherchées par la justice. La constitution de fichiers sur des individus considérés comme potentiellement dangereux pour la défense des intérêts nationaux n'est alors pas sans crainte pour les libertés publiques, d'autant plus avec les possibilités actuelles de « *l'exploitation massive des données numériques* » qui s'accompagne d'un risque de surveillance numérique massive des citoyens⁵.

Afin de concilier les besoins en traitement des données des services de renseignement et les libertés publiques, un cadre juridique général mais dérogatoire du droit commun de la protection des données a été prévu par la loi informatique et libertés du 6 janvier 1978 instituant la Commission nationale de l'informatique et des libertés (CNIL)⁶. Ce cadre juridique a été complété en 2015 par la loi relative au renseignement rattachant ainsi l'encadrement des fichiers de renseignement au droit du renseignement. Depuis 1978, de nombreux fichiers de renseignement ont pu alors être juridiquement consacrés permettant à chaque service de disposer légalement de leurs propres traitements de données sur des individus.

¹ A ce sujet, voir A. Bauer et C. Soullez, « *Des fichiers, pour quelles finalités ?* », Alain Bauer éd., *Les fichiers de police et de gendarmerie*. Presses Universitaires de France, 2011, pp. 7-29.

² Sur ce point, voir J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 26.

³ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 119.

⁴ Sur ce point, voir A. Bauer et C. Soullez, « *Des fichiers, pour quelles finalités ?* », op. cit., pp. 7-29.

⁵ En ce sens, voir J. Mafart, « *Fichier* », Hugues Moutouh éd., *Dictionnaire du renseignement*. op. cit., pp. 379-383.

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

A - Le cadre juridique général, de la loi « Informatique et libertés » à la loi relative au renseignement

Avant de nous intéresser à l'encadrement des fichiers de renseignement par la loi relative au renseignement de 2015, il convient d'exposer le cadre juridique initial qui a été mis en place par la loi informatique et libertés de 1978 et ses évolutions.

1. La loi informatique et libertés et ses évolutions

Adoptée à la suite du scandale du projet SAFARI (Système automatisé des fichiers administratifs et du répertoire des individus)¹, la première version de la loi informatique et libertés a consacré la notion de « traitements intéressant la sûreté de l'Etat, la défense et la sécurité publique » (plus couramment appelés « fichiers de souveraineté »²), qui intègre les fichiers de renseignement. En vertu de l'article 15 de la loi du 6 janvier 1978, la création de ces traitements est décidée par la loi ou par un acte réglementaire pris après avis de la CNIL. Néanmoins, à la différence des autres traitements opérés pour le compte de l'Etat, ceux intéressant la sûreté de l'Etat, la défense et la sécurité publique bénéficient d'un régime dérogatoire afin d'assurer notamment la protection du secret de la défense nationale attachée à l'activité des services de renseignement. L'article 19 de la loi a donc prévu que les demandes d'avis à la CNIL relatives à ces traitements puissent ne pas comporter certaines des mentions normalement exigées par la loi. Plus encore, l'article 20 a renvoyé la possibilité au gouvernement de prévoir par décret en Conseil d'Etat l'absence de publication des actes réglementaires portant création de ces traitements. S'agissant du « droit d'accès » consacré par la loi informatique et libertés qui permet aux personnes fichées d'obtenir des informations sur le traitement de leurs données directement auprès des responsables concernés, le législateur a aménagé un « droit d'accès indirect » pour

¹ Afin de centraliser ses renseignements, le ministère de l'intérieur du gouvernement du Premier ministre Pierre Messmer a eu pour ambition de mettre en place le projet SAFARI qui avait pour objet d'interconnecter l'ensemble des fichiers administratifs à partir du numéro de sécurité sociale des français (cf. J. Mafart, « Fichier », Hugues Moutouh éd., *Dictionnaire du renseignement*. Perrin, 2018, pp. 379-383). Le projet a été révélé par Le Monde en mars 1974 et a été dénoncé comme portant une grave atteinte aux libertés publiques, ce qui a entraîné son abandon (cf. P. Boucher, « Safari » ou la chasse aux français, Le Monde, 21 mars 1974, [Le monde \(cnil.fr\)](http://www.lemonde.fr)).

² Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 215.

les traitements intéressant la sûreté de l'Etat, la défense et la sécurité publique¹. La demande d'accès est alors adressée à la CNIL qui désigne l'un de ses membres habilités au secret appartenant au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour procéder aux investigations et aux modifications si nécessaires. A l'issue des investigations, le requérant se voit seulement notifier qu'il a été procédé aux vérifications.

Le dispositif dérogatoire a été précisé par un décret du 28 décembre 1979 portant notamment sur les demandes d'avis et la publicité des actes de la CNIL relatifs aux fichiers de souveraineté². S'agissant des demandes d'avis, l'article 1 du décret est venu préciser les sept mentions devant obligatoirement être mentionnées :

- « -l'autorité qui présente la demande ;*
- la finalité et, s'il y a lieu, la dénomination du traitement ;*
- le service ou les services chargés de mettre celui-ci en œuvre ;*
- le service auprès duquel s'exerce le droit d'accès défini au chapitre V de la loi susvisée du 6 janvier 1978 ainsi que les mesures prises pour faciliter l'exercice de ce droit ;*
- les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées ;*
- les destinataires ou catégories de destinataires habilités à recevoir communication de ces informations ;*
- les rapprochements, interconnexions ou toute autre forme de mise en relation de ces informations ».*

Pour ce qui concerne les actes de la CNIL, il a été décidé de ne pas les rendre publics lorsqu'ils concernent un traitement créé en application de la dérogation prévue à l'article 20 de la loi du 6 janvier 1978³. Pour l'application de ce dernier article, un décret en Conseil d'Etat du 7 mars 1986 est venu ensuite présenter la

¹ Article 39 de la loi du 6 janvier 1978.

² Décret n°79-1160 du 28 décembre 1979 fixant les conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

³ Article 2 du Décret n°79-1160 du 28 décembre 1979.

première liste des fichiers de renseignement tenus secrets¹ : il s'agissait des fichiers de la DST, de la DGSE et de la DPSD créés par décrets et le fichier d'informations nominatives mis en œuvre par la DPSD créé par un arrêté. En 1994, quatre autres traitements secrets créés par décrets et arrêtés sont venus compléter la liste du décret de 1986 : un nouveau fichier de la DGSE et le fichier du personnel de la DGSE² ; le fichier de la DRM et le fichier des personnes étrangères de la DRM³. Soulignons qu'une distinction ressort des décrets de 1986 et 1994 entre les fichiers de renseignement créés par un décret et ceux créés par un arrêté. Cette distinction renvoie à l'application de l'article 31 de la loi informatique et libertés de 1978 qui autorise, à titre dérogatoire et par décret en Conseil d'Etat après avis conforme de la CNIL, « *la conservation des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales des personnes* » pour des motifs d'intérêt public. Les fichiers qui ont été créés par arrêtés ne bénéficient donc pas de cette dérogation portant non plus sur la publicité des actes réglementaires mais sur le contenu même des fichiers. Notons que la distinction retenue reprend les recommandations de la CNIL ayant rendu un avis défavorable dans une délibération en date du 26 mai 1981 sur un projet de décret visant à accorder la dérogation de l'article 31 à de très nombreux fichiers des ministères de la défense et de l'intérieur et du Premier ministre⁴. La Commission avait estimé que les fichiers de surveillance pouvaient ne pas présenter le même intérêt public nécessitant donc d'apprécier l'application de l'article 31 « *pour chaque groupe de fichiers analogues en tenant compte de la nature de la population concernée et des dangers qu'elle peut ou non présenter pour*

¹ Décret n°86-326 du 7 mars 1986 portant application à certains actes réglementaires relatifs à des traitements automatisés d'informations nominatives intéressant la sécurité publique des dispositions de l'art. 20 (al. 2) de la loi 7817 du 06-01-1978.

² Décret n° 94-619 du 18 juillet 1994 complétant le décret n° 86-326 du 7 mars 1986 portant application à certains actes réglementaires relatifs à des traitements automatisés d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique des dispositions du deuxième alinéa de l'article 20 de la loi n° 78-17 du 6 janvier 1978.

³ Décret n° 94-620 du 18 juillet 1994 complétant le décret n° 86-326 du 7 mars 1986 portant application à certains actes réglementaires relatifs à des traitements automatisés d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique des dispositions du deuxième alinéa de l'article 20 de la loi n° 78-17 du 6 janvier 1978.

⁴ Délibération 81-66 du 26 mai 1981.

la sûreté de l'Etat, la Défense et la Sécurité publique »¹. Il est vrai qu'un fichier portant sur le personnel d'un service de renseignement ne présente pas le même intérêt public qu'un fichier portant sur des individus soupçonnés d'espionnage ou de terrorisme. Comme il a pu être souligné par la doctrine en 1992, le dispositif législatif et réglementaire applicable aux fichiers de renseignement a constitué un véritable progrès même si son objectif a été de préserver la confidentialité de ces traitements sensibles². Pour autant, des questions ont été soulevées sur l'application de ce dispositif dérogatoire (déclaration aménagée, absence de publicité, droit d'accès indirect et traitement pouvant porter sur des données très sensibles) et sur la conventionnalité du régime général des fichiers de souveraineté et de renseignement en vigueur avant la réforme de 2004 de la loi de 1978.

S'agissant d'abord du droit d'accès aux fichiers de souveraineté, le Conseil d'Etat a eu l'occasion de préciser que ce droit s'exerce uniquement sur le fondement du droit d'accès indirect prévu par la loi informatique et libertés³, excluant par conséquent l'application de la loi « CADA » portant sur l'accès aux documents administratif⁴. De son côté, la CNIL avait adopté une interprétation large de l'article 39 de la loi de 1978 selon laquelle le droit d'accès fait référence aux informations contenues dans un fichier, ce qui ouvrait la voie à un droit d'accès mixte (direct et indirect) lorsqu'un fichier comportait des informations relevant à la fois de la dérogation de l'article 39 et du droit commun⁵. Cependant, dans son arrêt *Lochak* du 27 avril 1988, le Conseil d'Etat est venu consacrer une approche restrictive du droit d'accès indirect en contradiction avec l'interprétation de la CNIL⁶. La haute juridiction administrative a, en effet, jugé que les dispositions de l'article 39 s'appliquaient à l'ensemble du fichier visé par la demande d'accès

¹ Délibération 81-66 du 26 mai 1981.

² En ce sens, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, Recueil Dalloz 1992, p. 73.

³ Conseil d'Etat, Assemblée, 19 mai 1983, *M. Bertin* (requête n° 40680).

⁴ Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal modifiée par la loi n°79-587 du 11 juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public.

⁵ Délibération 80-10 du 01 avril 1980.

⁶ A ce sujet, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

même si certaines informations contenues dans le fichier ne nécessitaient pas de protection particulière relative au secret¹. Si la position du Conseil d'Etat ne pose pas de difficulté au regard de l'article 39 qui s'intéresse bien aux fichiers souveraineté et non aux informations qu'ils contiennent², elle demeurerait moins protectrice des libertés que l'interprétation retenue par la CNIL et renforçait l'opacité des activités des services de police et de renseignement³. Néanmoins, il est intéressant de noter que la CNIL a conservé sa position sur la théorie du droit d'accès mixte dans ses délibérations du 27 avril 1988 et du 9 juin 1992 portant sur le fichier des personnes recherchées (FPR)⁴, démontrant ainsi la forte implication de la Commission pour œuvrer dans le sens d'un meilleur encadrement dans l'usage des fichiers. D'ailleurs, l'interprétation retenue par la Commission a trouvé à s'appliquer avec quelques aménagements dans le décret du 14 octobre 1991 encadrant les fichiers gérés par les services des renseignements généraux (RG)⁵. Conformément à la délibération 91-054 du 9 juillet 1991 de la CNIL portant sur l'application de l'article 31 de la loi de 1978 aux fichiers des RG, l'article 7 du décret organisait un droit d'accès mixte en fonction des informations concernées. Le décret allait d'ailleurs plus loin en autorisant la CNIL, avec l'accord du ministre de l'Intérieur, à indiquer au requérant non connu des RG qu'aucune information le concernant ne figure dans les fichiers. En revanche, il soumettait la constatation par la CNIL des informations pouvant être communiquées à l'accord du ministre de l'Intérieur qui disposait également d'un droit d'opposition à la communication des informations au requérant lorsque cette communication peut nuire à la sûreté de l'Etat, à la défense ou à la sécurité publique. L'effectivité du droit d'accès mixte dépendait donc de l'attitude de la CNIL et du ministre, relativisant ainsi la portée de ce droit dans la protection des libertés⁶. Statuant sur une demande d'accès aux

¹ Conseil d'Etat, 27 avril 1988, *Mme Lochak* (requête n° 75383).

² Sur ce point, voir D. Martin, *Les fichiers de police*, Presse universitaire de France, Que sais-je ? n° 3461, 9 octobre 2015.

³ En ce sens, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

⁴ Délibération 88-120 du 08 novembre 1988 et délibération 92-056 du 09 juin 1992.

⁵ Décret n° 91-1051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁶ En ce sens, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

fichiers des RG en 2003, le Conseil d'Etat a eu l'occasion de faire évoluer sa position sur le droit d'accès mixte aux fichiers de souveraineté en confirmant le dispositif mis en place par le décret de 1991¹. Dans cette affaire, le juge administratif avait également précisé que le droit d'opposition du ministre à la communication des informations ne peut se fonder exclusivement sur un motif d'ordre général tel qu'en l'espèce l'appartenance à un mouvement sectaire.

Par ailleurs, il convient de rappeler que la théorie du droit d'accès mixte a trouvé seulement à s'appliquer aux fichiers des RG et ne concernait pas les autres fichiers de renseignement toujours soumis à la jurisprudence *Lochak*. En outre, rappelons qu'à la différence des autres fichiers de renseignement, le décret de 1991 encadrant les fichiers des RG a été publié ainsi que l'avis de la CNIL². Il a pu alors être observé un certain glissement d'un encadrement d'ordre général vers « *des règles sectorielles* » dans l'encadrement juridique des fichiers de renseignement³. Pour notre part, ce glissement s'est opéré en faveur de la protection des droits et libertés des individus puisque le régime général dérogatoire mis en place par la loi informatique et libertés et la jurisprudence du Conseil d'Etat demeuraient plus favorables à l'Etat et à la protection du secret.

Ensuite, sur la question de la conventionnalité du régime dérogatoire applicable aux fichiers de souveraineté, ce dernier a été jugé compatible avec les stipulations de l'article 8 de la Conv. EDH et de l'article 9 de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe du 28 janvier 1981 par le Conseil d'Etat dans une décision du 28 juillet 1995⁴. La position du Conseil d'Etat nous apparaît cohérente puisque les stipulations invoquées prévoient qu'il peut être prévu des dérogations par la loi lorsqu'elles sont nécessaires dans une société démocratique à la protection de la sécurité de l'Etat. Cette solution a été réaffirmée en 2001 par la Cour administrative d'appel de Paris statuant sur un litige relatif à la communication des informations d'une personne inscrite dans les fichiers des

¹ Conseil d'Etat, 30 juillet 2003, *M. Raoust* (requête n° 242812).

² Délibération 91-083 du 24 septembre 1991.

³ En ce sens, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

⁴ Conseil d'Etat, 28 juillet 1995, *CGT* (requête n° 132453).

RG en raison de son appartenance à l'église de scientologie¹, mouvement considéré comme sectaire par un rapport parlementaire de 1995². En ce qui concerne le droit de l'Union européenne (UE), le législateur français a rappelé que les fichiers de souveraineté et de renseignement étaient exclus du champ d'application de la directive européenne 95/46 du 24 octobre 1995 sur la protection des données personnelles³ lors des débats sur la loi de transposition n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel modifiant la loi informatique et libertés de 1978⁴. La loi de 2004 a également été l'occasion de clarifier et de simplifier certaines dispositions du dispositif dérogatoire des fichiers de renseignement prévu par la loi du 6 janvier 1978.

Les premières innovations apportées par la loi de 2004 ont touché aux actes réglementaires autorisant la mise en œuvre de fichiers de souveraineté. Reprenant la pratique antérieure, l'article 26 nouveau de la loi informatique et libertés a organisé la distinction entre les fichiers autorisés par arrêté et ceux autorisés par décret en Conseil d'Etat lorsqu'ils portent sur des données sensibles (article 26-I et II). Néanmoins, le législateur a abandonné la procédure de l'avis conforme qui était prévu à l'alinéa 3 de l'article 31 de la loi informatique et libertés ainsi que la possibilité « *de passer outre l'avis défavorable de la CNIL par un décret pris sur avis conforme du Conseil d'Etat* »⁵. En contrepartie, il a été ajouté aux dispositions de l'article 26 nouveau réaffirmant la dérogation relative à la publicité des actes réglementaires autorisant les fichiers de souveraineté la publication du sens de

¹ Cour administrative d'appel de Paris, 6 décembre 2001, *Mme Robert* (n° 99PA01993).

² Cf. A. Gest, *Rapport fait au nom de la commission d'enquête sur les sectes*, Assemblée nationale, 22 décembre 1995.

³ Voir notamment le considérant 13 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

⁴ Cf. A. Türk, *Rapport sur le projet de loi, adopté par l'Assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Sénat, 19 mars 2003, p. 25.

⁵ Cf. G. Gouzes, *Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Assemblée nationale, 9 janvier 2002, p. 55.

l'avis émis par la CNIL sur le décret d'autorisation (article 26-III)¹. Conformément aux préconisations du rapport de Guy Braibant², le législateur a souhaité éviter les divergences entre la CNIL et le Conseil d'Etat dans la procédure d'autorisation des fichiers de souveraineté tout en allant « *dans le sens d'une plus grande transparence de l'Etat dans l'exercice de ses missions régaliennes* »³. On peut relever que la CNIL avait estimé que la publication du sens de son avis « *paraît de nature à assurer le maintien d'un haut niveau de garanties et, en tout état de cause, à préserver la portée qui doit s'attacher aux interventions d'une autorité administrative indépendante à l'égard de traitements particulièrement sensibles* »⁴.

D'autres innovations ont concerné le droit d'accès indirect et le contrôle de la CNIL. La loi de 2004 a consacré l'application de la théorie du droit d'accès mixte aux fichiers de souveraineté dans les conditions similaires à celles énoncées dans le décret de 1991 relatif aux fichiers des RG. En réalité, il s'agit d'une innovation apportée par la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure qui a été reprise par le législateur de 2004⁵. Par ailleurs, il a été introduit la possibilité pour le gouvernement d'ajouter au décret en Conseil d'Etat autorisant une dispense de publication pour les fichiers de souveraineté une exemption au contrôle *a posteriori* de la CNIL (contrôle sur place et sur pièce) afin d'assurer la protection du secret⁶. Autrement dit, la CNIL contrôle les fichiers de souveraineté

¹ Le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi informatique et libertés modifiée est venu préciser les mentions pouvant figurer sur l'avis de la CNIL : « favorable », « favorable avec réserve » ou « défavorable » (article 83).

² Cf. G. Braibant, *Données personnelles et société de l'information*, Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46, 3 mars 1998.

³ Cf. G. Gouzes, *Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, op. cit., p. 55.

⁴ Sur ce point, voir A. Türk, *Rapport sur le projet de loi, adopté par l'Assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, op. cit., p. 105.

⁵ Ibid., p. 130.

⁶ Cf. A. Türk, *Rapport sur le projet de loi, adopté avec modification par l'Assemblée nationale en deuxième lecture, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Sénat, 23 juin 2004.

et de renseignement « par carottage » dans le cadre du contrôle *a priori* et de l'exercice du droit d'accès¹.

Sur l'ensemble des modifications apportées par la loi de 2004 sur les fichiers de souveraineté, seules les dispositions nouvelles relatives à l'avis simple de la CNIL ont été contestées devant le Conseil constitutionnel par des parlementaires, ces derniers dénonçant « *un des reculs les plus manifestes* » de la loi informatique et libertés et une « *situation constitutionnellement préjudiciable* »². Le Conseil a toutefois validé le nouveau dispositif en jugeant notamment que les dispositions litigieuses ne privaient pas de garanties légales le droit au respect de la vie privée et n'étaient « *contraires à aucun principe ni à aucune règle de valeur constitutionnelle* »³. Relevons que les requérants avaient invoqué la théorie de « l'effet cliquet » dégagée par la jurisprudence du Conseil constitutionnel selon laquelle « *le législateur ne saurait modifier ou abroger des dispositions législatives touchant une liberté comme la liberté de communication qu'en vue d'en rendre l'exercice plus effectif* »⁴. Cette argumentation a été rejetée par le Conseil qui a considéré que le législateur s'était seulement borné à substituer une procédure par une autre sans priver de toute garantie légale le respect du droit à la vie privée⁵. Allant au bout de son raisonnement, le juge constitutionnel a rappelé que le législateur avait introduit la publication de l'avis de la CNIL concomitamment à la publication de l'acte réglementaire de création des traitements de souveraineté et réaffirmé la nécessité d'un décret en Conseil d'Etat pour ces traitements lorsqu'ils portent sur des données sensibles.

Bien que le cadre juridique dérogatoire des fichiers de souveraineté et de renseignement ait été clarifié par la loi du 6 août 2004, il reste que législateur

¹ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 216.

² Décision n° 2004-499 DC du 29 juillet 2004 (considérant 25).

³ Décision n° 2004-499 DC du 29 juillet 2004 (considérant 26).

⁴ Sur ce point, voir J. Andriantsimbazovina, *La conception des libertés par le Conseil constitutionnel et par la Cour européenne des droits de l'homme*, Les nouveaux cahiers du Conseil constitutionnel n° 32, juillet 2011, <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-conception-des-libertes-par-le-conseil-constitutionnel-et-par-la-cour-europeenne-des-droits-de-l>.

⁵ Cf. Commentaire de la décision n° 2004-499 DC du 29 juillet 2004, Les Cahiers du Conseil constitutionnel, Cahier n° 17, https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/commentaires/cahier17/ccc_499dc.pdf.

n'avait pas jugé nécessaire d'introduire dans la loi la dérogation prévue à l'ancien article 19 de la loi informatique et libertés relative aux mentions devant figurer dans les demandes d'avis à la CNIL. Cette dérogation n'a pas été reprise à l'article 30 nouveau de la loi modifiée car elle était toujours applicable jusqu'au mois d'août 2007 en vertu des dispositions transitoires prévues par la loi de 2004¹. Considérant néanmoins que ces « fichiers spécialisés » devaient « bénéficier d'une protection renforcée » face aux terroristes, le législateur a réaffirmé la dérogation de l'ancien article 19 dans la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme². L'article 13 de cette loi est alors venue modifier l'article 30 nouveau de la loi informatique et libertés permettant de limiter les informations figurant dans les demandes d'avis à la CNIL portant sur les fichiers de souveraineté précisés par un décret en Conseil d'Etat pris après avis de la CNIL. Il ne s'agit donc pas d'une nouvelle dérogation renforçant l'opacité des fichiers de renseignement mais d'une simple consolidation législative du droit antérieur toujours en vigueur.

Le décret n° 2007-914 du 15 mai 2007 a ainsi listé les fichiers bénéficiant de la dérogation de l'article 30 nouveau de la loi informatique et libertés³. La liste reprenait celle établie par le décret n° 86-326 du 7 mars 1986 abrogé, c'est-à-dire les fichiers de la DST, de la DGSE, de la DPSD et de la DRM. En outre, le décret du 15 mai 2007 appliquait pour ces fichiers les dérogations des articles 26 et 44 de la loi informatique et libertés relatives respectivement à la dispense de publication des actes réglementaires d'autorisation et du contrôle *a posteriori* de la CNIL. En revanche, le décret de 2007 ne précisait pas les informations figurant dans les demandes d'avis à la CNIL, le gouvernement de l'époque ayant préféré insérer cette précision à l'article 16 du décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi informatique et libertés modifié par le décret n° 2007-451 du mars 2007. Prenant acte de ce choix, la CNIL avait fait part de son souhait de voir figurer dans le décret d'application de l'article 30 la référence au décret du 20 octobre 2005 et, dans ce dernier, les éléments devant être au minimum transmis à la Commission suivants :

¹ Sur ce point, voir Intervention de M. P. Goujon lors de la séance du 15 décembre 2005 du Sénat.

² Ibid.

³ Décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

« -l'identité et l'adresse du responsable du traitement ;

-la ou les finalités du traitement, s'il y a lieu, la dénomination du traitement, ainsi que la description générale de ses fonctions ;

-le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;

-les catégories de personnes concernées par le traitement ;

-la durée de conservation des informations traitées ;

-le ou les services chargés de mettre en œuvre le traitement ;

-les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

-les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

-le service auprès duquel s'exerce le droit d'accès visé à l'article 41 de la loi du 6 janvier 1978 susvisée, ainsi que les mesures prises pour faciliter l'exercice de ce droit »¹.

Le gouvernement a repris ces éléments dans le décret du 20 octobre 2005 modifié à l'exception de ceux portant sur les catégories de personnes concernées par les fichiers et sur la durée de conservation des données. Le décret du 15 mai 2007 a été régulièrement modifié pour mettre à jour et compléter la liste des fichiers bénéficiant du régime dérogatoire des fichiers de souveraineté. Ces modifications soulèvent deux remarques : d'une part, la majorité des nouveaux fichiers sont gérés par des services de renseignement du premier cercle ou du second cercle ; d'autre part, les modifications du décret de 2007 ont découpé en « trois catégories » les fichiers de souveraineté, c'est-à-dire les fichiers bénéficiant de l'ensemble des dérogations, ceux qui ne disposent pas de la dispense de publication du texte en portant création et ceux qui ne bénéficient pas de l'exemption de contrôle *a posteriori* de la CNIL². La plupart des fichiers de renseignement entrent dans la première catégorie.

¹ Délibération 2007-001 du 11 janvier 2007 portant avis sur le projet de décret pris pour l'application du dernier alinéa du I de l'article 30 de la loi du 6 janvier 1978 modifiée.

² A ce sujet, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 216 et 217.

Depuis 2004, l'application du cadre législatif et réglementaire des fichiers de renseignement a eu l'occasion d'être contesté et critiqué sans être toutefois véritablement remis en cause. En effet, le Conseil d'Etat a rejeté en 2011 une QPC sur les dispositions dérogatoires de la loi informatique et libertés modifiée relatives aux fichiers de souveraineté en jugeant que cette dernière n'était pas nouvelle et non sérieuse¹. A l'appui de son recours en annulation de plusieurs décrets d'autorisation ou de modification de fichiers de renseignement, le requérant avait notamment mis en cause l'absence de contrôle, notamment juridictionnel, de ces fichiers. Dans sa décision de rejet, le Conseil d'Etat a pu préciser avec clarté que la loi du 6 janvier 1978 modifiée « *n'a ni pour objet ni pour effet de soustraire ces fichiers au contrôle du juge et encadre leur création de nombreuses garanties* » (considérant 4). Par ailleurs, certains auteurs ont émis des avis critiques sur le régime dérogatoire des fichiers de souveraineté en soulignant particulièrement le manque de précisions sur la champ d'application de la dispense de publication des actes d'autorisation de ces fichiers² et l'augmentation du nombre des fichiers de renseignement bénéficiant « généreusement » du dispositif dérogatoire de la loi informatique et libertés³, ce qui a pu susciter une inquiétude sur le risque de faciliter des dérives telles que le détournement des données ou leur consultation illégale⁴. Il est vrai que depuis 2004 les fichiers de renseignement n'ont pas cessé d'augmenter, la liste du décret du 15 mai 2007 comporte plus d'une quinzaine de fichier en 2021⁵. Toutefois, on précisera que des fichiers ne relevant pas du renseignement comme le fichier LEGATO de la Légion étrangère ont été intégrés à liste du décret de 2007. En ce qui concerne l'opacité de ces fichiers, elle se comprend aisément par la sensibilité des données traitées au regard des intérêts de l'Etat. On notera également que l'exécutif n'a pas

¹ Conseil d'Etat, 12 mai 2011, *M. Gonzales-Mestres* (requête n° 318652).

² En ce sens, voir J. -M. Cotteret, *Les fichiers de police et de renseignement en France*, Rapport de recherche 21, CF2R, octobre 2017, p 13 et suivantes.

³ En ce sens, voir V. Gautron et D. Monniaux, *De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme*, Archives de politique criminelle, vol 38, n° 1, 2016, pp. 123-135 ; cf. V. Gautron, *Une mémoire policière hypertrophiée : la fin du droit à l'oubli ?*, Les Cahiers de la Justice, vol 4, n° 4, 2016, pp. 607-617.

⁴ Sur ce point, voir V. Gautron, *Usages et mésusages des fichiers de police : la sécurité contre la sûreté ?*, AJ Pénal 2010 p. 266.

⁵ Décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 33 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par le décret n° 2021-697 du 31 mai 2021.

systématiquement cherché l'opacité des fichiers de renseignement, en témoigne l'encadrement des fichiers des RG même si ces derniers font figure d'exception parmi les fichiers de souveraineté.

Avant d'aborder les apports de 2015 de la législation relative au renseignement, il nous apparaît opportun de s'attarder dès à présent sur les modifications de la loi informatique et libertés issues de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et de l'ordonnance n° 2018-1125 du 12 décembre 2018. En effet, ces textes sont sans incidence sur les apports de la loi relative au renseignement mais introduisent de nouvelles précisions sur le régime des fichiers de souveraineté.

Adaptant le droit français au nouveau cadre juridique européen de la protection des données consacré par le « paquet européen » de 2016 composé du Règlement général sur la protection des données (RGPD)¹ et de la Directive « Police-Justice »², la loi du 20 juin 2018 n'a pas remis en cause le régime dérogatoire applicable aux fichiers de renseignement, ces derniers étant toujours exclu du champ d'application du droit de l'Union européenne. Lors des débats parlementaires sur le projet de loi, le gouvernement avait rappelé l'incompétence de l'Union dans ce domaine³ et fait part de son intention de ne pas modifier le dispositif en vigueur jugé « *robuste, récent et efficace qui comporte des garanties réelles* »⁴. On notera que le Conseil d'Etat n'a pas remis en question la position du gouvernement dans son avis sur le projet de loi⁵ et qu'il a d'ailleurs tenu à réaffirmer l'exclusion de l'application du droit européen dans une décision rendue

¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE).

² Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

³ Cf. Etude d'impact du projet de loi relatif à la protection des données personnelles du 12 décembre 2017.

⁴ En ce sens, voir P. Forteza, *Rapport sur le projet de loi relatif à la protection des données personnelles*, Assemblée nationale, 25 janvier 2018, p. 44.

⁵ Conseil d'Etat, avis, 7 décembre 2017, *Projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (n° 393836).

en 2020¹. Toutefois, si la CNIL n'a pas relevé de difficulté dans l'inapplicabilité du RGPD, elle a, en revanche, souligné que les fichiers de sécurité publique entrent dans le champ d'application de la Directive « Police-Justice »². La distinction entre les fichiers intéressant la sûreté de l'Etat et la défense et ceux intéressant seulement la sécurité publique a été reprise par l'ordonnance du 12 décembre 2018 réécrivant la loi relative à la protection des données personnelles³. Finalement, cette distinction n'a pas impacté le droit applicable aux fichiers des services de renseignement du premier cercle puisque la directive européenne elle-même considère que les activités relatives à la sécurité nationale ne relèvent pas du droit de l'Union européenne⁴. En revanche, il convient de préciser que les fichiers de renseignement incluent des fichiers de sécurité publique gérés par le ministère de l'intérieur pour les besoins des services du renseignement intérieur et territorial⁵. Ces fichiers sont, quant à eux, soumis aux dispositions de la loi informatique et libertés transposant la directive européenne. Enfin, on relèvera qu'en plus d'exclure les fichiers de souveraineté du champ d'application du droit de l'Union européenne, aujourd'hui droit commun de la protection des données, l'ordonnance de 2018 a adopté une conception différente du principe européen de minimisation des données⁶. Alors que ce principe exige que les données soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du fichier, la loi française atténue la limitation des données en disposant que les fichiers de souveraineté doivent porter sur des « *données non excessives* »⁷. Cette atténuation n'est pas sans interroger sur le respect de la protection des données personnelles en matière de renseignement au regard des inquiétudes relatives à la surveillance de masse.

¹ Conseil d'Etat, 27 mars 2020, *Association Cercle de réflexion et de proposition d'actions sur la psychiatrie* (requête n° 431350).

² Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978 (demande d'avis n°17023753).

³ Cf. Titre III et IV de la nouvelle loi informatique et libertés.

⁴ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 (considérant 14).

⁵ A ce sujet, voir D. Paris et P. Morel-À-L'Huissier, *Rapport d'information sur les fichiers mis à disposition des forces de sécurité*, Assemblée nationale, 17 octobre 2018, p. 20.

⁶ Sur ce point, voir M. Bourgeois et M. Moine, *Réécriture de la loi informatique et libertés : encore des nouveautés*, Cahiers de droit de l'entreprise, janvier 2019, dossier 4.

⁷ 3° de l'article 4 nouveau de la loi informatique et libertés issu de l'ordonnance du 12 décembre 2018.

Fichiers stratégiques pour la souveraineté de la France, il nous semble cohérent que les fichiers des services de renseignement soient encadrés par un régime juridique dérogatoire en droit interne. Dès lors, on pourra regretter, comme pour Jean-Jacques Urvoas au regard de la sensibilité du sujet pour les libertés, que ces fichiers n'aient pas été autant abordés que les techniques de renseignement dans la loi relative au renseignement¹. Pour autant, la question des fichiers n'est pas totalement absente de la loi de 2015, cette dernière ayant confié leur contrôle juridictionnel à la formation spécialisée du Conseil d'Etat chargée du contentieux du renseignement.

2. Les apports de la loi relative au renseignement de 2015

Transférant le contentieux du droit d'accès indirect (pour l'accès, la rectification ou l'effacement de données) aux fichiers intéressant la sûreté de l'Etat à la nouvelle formation spécialisée du Conseil d'Etat², la loi de 2015 introduit les fichiers de renseignement dans le droit du renseignement. Sans entrer dans les détails de cette nouvelle formation habilitée au secret de la défense nationale, il convient de souligner que cette innovation de la loi relative au renseignement n'est pas des moindre car elle rend effectif le contrôle juridictionnel des fichiers de renseignement qui demeurait dans une impasse jurisprudentielle depuis l'arrêt *Moon*³. En effet, bien que le juge administratif fût déjà compétent dans ce domaine, l'administration pouvait lui opposer le secret de la défense nationale⁴. Le transfert du contentieux du droit d'accès indirect au juge du renseignement implique que ce dernier fait également office de juge de la protection des données au sens de la loi informatique et libertés. La loi relative au renseignement nous apparaît alors comme un prolongement de la loi de 1978. D'ailleurs, la loi de 2015 n'a pas manqué de souligner que le respect de cette protection constitue l'un des principes régissant l'activités et le contrôle des services de renseignement⁵. On soulignera

¹ Cf. Entretien avec Jean-Jacques Urvoas, *Était-il tolérable que la France soit le seul Etat européen où les services de renseignement agissaient en dehors de tout cadre juridique ?*, La semaine juridique Administrations et Collectivités territoriales n° 40, 5 octobre 2015.

² Article L. 841-2 du code de la sécurité intérieure.

³ CE, ass., 6 novembre 2002, *Moon Sun Myung* (requête n° 194295).

⁴ Sur ce point, voir O. Le Bot, *Le contentieux du renseignement devant la formation spécialisée du Conseil d'Etat*, RDFA 2017, p. 721 ; L. Marthinet, *Contentieux de l'accès indirect aux fichiers : sortie de l'impasse ?*, AJDA 2016, p. 1733.

⁵ Article L. 801-1 du code de la sécurité intérieure.

ainsi un rapprochement bienvenu entre le droit du renseignement et le droit de la protection des données, reste à savoir si ce rapprochement ne risque pas d'entraîner un déséquilibre entre ces deux droits qui serait préjudiciable pour la conciliation entre les droits et libertés et les missions des services.

Le décret n° 2015-1808 du 28 décembre 2015 d'application de l'article L. 841-2 du code de la sécurité intérieure est venu entériner le basculement des fichiers de renseignement dans le champ du droit du renseignement. Ce décret créé l'article R. 841-2 du code de la sécurité qui liste les fichiers soumis au contrôle du juge du renseignement, ce qui comprend ainsi les fichiers des services de renseignement qui sont désormais mentionnés, notons-le, dans le livre VIII : « Du renseignement » de la partie réglementaire du code de la sécurité intérieure. Si l'article R. 841-2 apparaît similaire au décret du 15 mai 2007 d'application de la loi informatique et libertés, il convient cependant de relever deux grandes différences entre ces textes.

D'abord, les deux textes n'ont pas le même objet. Le décret de 2007 porte sur les dérogations à la loi informatique et libertés alors que l'article R. 841-2 délimite les fichiers soumis au contrôle juridictionnel de la formation spécialisée du Conseil d'Etat. Ce dernier s'intéresse d'ailleurs davantage aux données intéressant la sûreté de l'Etat plus qu'aux fichiers eux-mêmes, ce qui explique l'intégration des fichiers de renseignement policier du ministère de l'intérieur. Ces fichiers relèvent normalement du renseignement de sécurité publique mais peuvent comporter des données intéressant la sûreté de l'Etat¹.

Ensuite, certains fichiers du renseignement mentionnés dans la liste du décret de 2007 n'ont pas été retenus dans celle de l'article R. 841-2. Il s'agit particulièrement du « fichier de la DGSE » et du « fichier du personnel de la DGSE » qui ont été créés par arrêtés. Cette exclusion a pour conséquence que ces deux fichiers bénéficient de l'ensemble des dérogations accordées par la loi informatique et libertés hormis la possibilité de traiter des données sensibles tout en écartant leur contrôle juridictionnel devant le juge du renseignement. Cette solution de maintenir la compétence du juge administratif de droit commun pour statuer en matière de droit d'accès indirect sur ces fichiers peut sembler curieuse

¹ Il s'agit des fichiers de prévention des atteintes à la sécurité publique du ministère de l'intérieur PASP, GIPASP et EASP.

sur le plan d'un recours effectif et discriminatoire. On peut comprendre que ces fichiers ne concernent normalement pas des données sensibles et le souci de sécuriser la confidentialité du personnel de la DGSE et du fonctionnement du service, mais cette solution peut être critiquable pour le respect des droits des agents. En effet, il peut tout à fait être envisagé que ce type de fichier puisse leur porter préjudice (atteinte à la vie privée disproportionnée, interférence dans la carrière de l'agent par exemple) sans aucune possibilité d'un réel recours. En outre, on remarquera que l'article R. 841-2 concerne en réalité les fichiers des personnes surveillées plus que les fichiers des services de renseignement. L'intention est louable en matière de protection des droits et libertés mais elle néglige les droits des agents de la DGSE. La différence de traitement entre les personnes surveillées et le personnel de la DGSE dans le droit à la protection de leurs données nous semble discriminatoire et injuste. Par ailleurs, cette situation démontrerait un certain déséquilibre préjudiciable pour les droits et libertés dans le rapprochement évoqué plus haut entre le droit du renseignement et le droit de la protection des données ainsi que la limite du juge du renseignement comme juge de la protection des données. A notre sens, il est regrettable que la combinaison de l'article L. 801-1 du code de la sécurité intérieure et de l'article L. 841-2 du même code n'ait pas été plus innovante en confiant le contrôle juridictionnel de l'ensemble des fichiers des services au juge du renseignement, d'autant plus qu'il suffit d'insérer les fichiers manquant à la liste de l'article R. 841-2.

Les apports de la loi relative au renseignement et de son application précédemment évoquée nous permettent, par conséquent, de diviser en trois catégories les fichiers de renseignement :

- les fichiers de la DGSE non soumis au contrôle du juge du renseignement ;
- les fichiers de renseignement soumis uniquement au contrôle du juge du renseignement
- les fichiers de renseignement dits « partagés » qui sont soumis à la fois au juge du renseignement pour les données intéressant la sûreté de l'Etat et

au juge administratif de droit commun pour les données intéressant la sécurité publique¹.

Comme relevé par le rapport d'information de juin 2020 sur l'évaluation de la loi relative au renseignement², la dernière catégorie a soulevé des difficultés en raison du découpage nécessaire à réaliser sur ces fichiers afin de déterminer les données intéressant la sûreté de l'Etat. Ces données peuvent difficilement se distinguer d'autres données, d'autant plus que l'intérêt d'une donnée pour la sécurité publique ou la sûreté de l'Etat peut évoluer dans le temps³. L'appréhension des fichiers par le droit du renseignement a pu complexifier tant leur mise en œuvre par les services que leur contrôle, notamment pour le justiciable dans la détermination du juge compétent ou des normes invocables. D'ailleurs, la méconnaissance de la directive européenne « Police-Justice » normalement invocable par le justiciable en matière de fichiers de sécurité publique a été rendue également plus complexe depuis que le Conseil d'Etat a jugé, en toute logique, que les données intéressant la sûreté de l'Etat de ces fichiers échappent au champ d'application du droit de l'Union européenne⁴. En outre, le rapport d'information a aussi relevé que *« certaines des données de ces fichiers peuvent ne pas être communiquées en raison de leur sensibilité sans pour autant relever de la sûreté de l'État. Il semble aussi que certains services refusent, en pratique, l'accès à toute donnée de manière à ne donner aucune indication, même indirecte, sur la nature de ces données »*⁵.

Face à ces difficultés, le rapport d'information avait alors préconisé de réviser les textes réglementaires applicables aux différents fichiers afin de clarifier leur régime juridique. Dans le prolongement de ces préconisations, on pourra saluer les efforts de clarification entrepris dans les décrets de 2020 modifiant les fichiers de renseignement de sécurité publique PASP, GIPASP et EASP inscrits à

¹ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 119 et suivantes.

² Ibid.

³ Cf. infra. B - *Les règles spécifiques aux fichiers de renseignement*. Notamment sur les difficultés soulevées sur le fichier STARTRAC de Tracfin.

⁴ Conseil d'Etat, 12 juillet 2021, M. A... B... (requête n° 426962).

⁵ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 124.

l'article R. 841-2 qui ont proposé une définition des données intéressant la sûreté de l'Etat, c'est-à-dire « *celles qui révèlent des activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste portant atteinte à ces mêmes intérêts* »¹. En revanche, cette nécessité de clarifier le régime de chacun des fichiers traduit une certaine limite à l'établissement d'un cadre juridique général des fichiers de renseignement, ce qui nous conduit à proposer une étude cas par cas.

B - Les règles spécifiques aux fichiers de renseignement

A partir des deux listes de fichiers établies pour l'application de la loi informatique et libertés et de la loi relative au renseignement, il est possible désormais d'étudier les règles spécifiques applicables à chacun des fichiers relevant du renseignement. Pour ce faire, nous procéderont à un classement des fichiers selon l'activité de renseignement concernée et, par là même, par ministère de tutelle selon l'organisation française de la communauté du renseignement : 1/ les fichiers du renseignement intérieur (ministère de l'intérieur) ; 2/ les fichiers du renseignement extérieur et militaire (ministère de la défense) ; 3/ les fichiers du renseignement économique et financier (ministère de l'économie) ; 4/ le fichier CAR du renseignement pénitentiaire (ministère de la justice).

1. Les fichiers du renseignement intérieur

On peut encore distinguer, ici, trois catégories de fichiers : les fichiers du service de renseignement intérieur du premier cercle ; ceux relevant spécifiquement de la lutte anti-terroriste ; et, les fichiers du renseignement territorial et d'enquêtes administratives, notamment utilisés par les services du second cercle.

Les fichiers du service de renseignement intérieure du premier cercle

La DGSi gère un unique fichier de renseignement intitulé CRISTINA (centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux). Géré par la DCRI avant la réforme de 2014², ce fichier est le

¹ En ce sens, voir CNIL, *Publication des décrets relatifs aux fichiers PASP, GIPASP et EASP : la CNIL précise sa mission d'accompagnement*, 11 décembre 2020 (<https://www.cnil.fr/fr/publication-des-decrets-relatifs-aux-fichiers-pasp-gipasp-et-easp-la-cnil-precise-sa-mission>).

² Décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure.

fruit d'une fusion des fichiers de la DST et des RG¹. Antérieur à la loi informatique et libertés, ces deux fichiers ont été déclarés à la CNIL et fait l'objet d'une légalisation à partir des années 1980². S'agissant du fichier de la DST, peu d'informations sont disponibles hormis qu'il a bénéficié de l'ensemble des dérogations prévues par la loi informatique et liberté en matière de fichier de souveraineté selon le décret du 7 mars 1986, ce qui signifie que seules des données intéressant la sûreté de l'Etat étaient traitées dans ce fichier³. En revanche, il en a été autrement pour le fichier des RG qui concernait aussi bien la sûreté de l'Etat que la sécurité publique, la CNIL considérant que l'encadrement de ce fichier devait être plus transparent.

L'élaboration d'un texte réglementaire spécifique applicable au fichier des RG a été longue et progressive en raison « *de négociations difficiles entre le ministère de l'Intérieur, le Conseil d'Etat et la CNIL* »⁴. D'autant plus que si un compromis a été trouvé au début de l'année 1990⁵, la légalisation du fichier des RG a été suivie d'un scandale médiatique dénonçant notamment la possibilité de « *ficher librement l'origine ethnique, les opinions politiques, religieuses, philosophiques, syndicales des Français* », ce qui a poussé le gouvernement de l'époque à rapidement retirer le texte réglementaire incriminé⁶. Finalement, le décret n°91-1051 du 14 octobre 1991 a remplacé le texte retiré en ayant pour objet de préciser les dérogations de la loi informatique et libertés pouvant s'appliquer au fichier des RG. A ce titre, notons que le nouveau texte s'est montré plus cohérent avec l'esprit de la loi informatique et libertés en s'appropriant les progrès souhaités par la CNIL, ce qui souligne « l'action continue » de cette

¹ A ce sujet, voir D. Batho et J. A. Bénisti, *Rapport d'information sur les fichiers de police*, Assemblée nationale, 24 mars 2009, p. 64.

² Sur ce point, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

³ Cf. supra. *Le cadre juridique général, de la loi informatique et libertés à la loi renseignement*.

⁴ Cf. D. Batho et J. A. Bénisti, *Rapport d'information sur les fichiers de police*, op. cit., p. 60 et suivantes.

⁵ Décret n° 90-184 du 27 février 1990 portant application aux fichiers automatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁶ Cf. J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

dernière dans l'encadrement des fichiers comme l'a relevé le Professeur Jean Frayssinet¹.

Le décret du 14 octobre 1991 est venu ainsi définir les données sensibles pouvant être traitées par les RG ainsi que les garanties exigées dans la mise en œuvre du fichier et son contrôle. En ce qui concerne les dispositions sur le droit d'accès à ce fichier, elles ont déjà été abordées précédemment dans le cadre juridique général des fichiers de renseignement².

Le texte réaffirme l'interdiction de principe du traitement des données sensibles posée par la loi de 1978. Par dérogation à ce principe, le décret autorise le traitement des données sensibles relatives :

- aux « *signes physiques particuliers, objectifs et inaltérables, comme éléments de signalement* » de personnes physiques majeures soupçonnées de porter atteinte à la sûreté de l'Etat ou à la sécurité publique ainsi que de l'entourage de ces personnes ;
- aux « *activités politiques, philosophiques, religieuses ou syndicales* » de personnes physiques majeures ayant accès à des informations protégées en relation avec la sûreté de l'Etat ou la sécurité publique ou « *qui ont sollicité, exercé ou exercent un mandat politique, syndical ou économique ou qui jouent un rôle politique, économique, social ou religieux significatif, sous condition que ces informations soient nécessaires pour donner au Gouvernement ou à ses représentants les moyens d'apprécier la situation politique, économique ou sociale et de prévoir son évolution* » (fichier dit « des personnalités »)³. Cette dernière finalité concerne également le traitement de données sur l'activité de personnes morales.

Sur ces éléments, on retiendra certaines remarques du Professeur Jean Frayssinet qui permettent une meilleure compréhension de ces dispositions⁴. Il a ainsi relevé que les termes du décret définissant les données sensibles autorisées

¹ Cf. J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

² Cf. supra. *Le cadre juridique général, de la loi informatique et libertés à la loi renseignement*.

³ 30 de l'article 3 du décret n° 91-1051 et 91-1052 du 14 octobre 1991.

⁴ Cf. J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

à être traitées renvoyaient pour « les signes physiques » à la race et à l'ethnie et pour les « activités » aux opinions et convictions. Il a également relevé deux remarques sur les personnes concernées. D'une part, il a noté que les personnes morales étaient visées par le décret alors que l'application de la loi informatique et libertés a pour objet la protection des données des personnes physiques. A ce sujet, cette précision nous apparaît bienvenue dans un souci de plus de transparence et de protection des données en droit du renseignement comme en droit du numérique, notamment dans un contexte juridique où les données personnes morales ne bénéficient pas d'une protection spécifique. D'autre part, il n'a pas manqué de rappeler les inquiétudes de la CNIL sur la possibilité de traiter des données relatives à l'entourage des personnes surveillées (parents, amis, ou contacts professionnels par exemple) dont les activités sont susceptibles de porter atteinte à la sûreté de l'Etat tout en précisant que le ministère de l'intérieur avait indiqué que ce traitement ne concernerait que les personnes ayant un lien direct avec l'activité de la personne surveillée¹. Pour autant, on objectera que le texte retenu n'a pas été modifié dans ce sens, ce qui peut faire douter de la réalité des indications du ministère de l'intérieur. Enfin, le Professeur Jean Frayssinet a eu l'occasion d'apporter quelques commentaires sur la légalité du fichage réalisé par les RG au regard du décret de 1991 dans le cadre de l'arrêt *Mme Robert* de la Cour administrative d'appel de Paris du 6 décembre 2001². Dans cette affaire, la requérante avait soutenu que sa seule appartenance à l'Eglise de scientologie « *ne saurait justifier l'enregistrement d'informations la concernant dans les fichiers des renseignements généraux* ». Pour le Professeur Frayssinet, un fichage fondé uniquement sur l'appartenance à une « *Eglise quelconque* » semblerait excessif et contraire aux dispositions du décret de 1991. Pour notre part, une telle situation constituerait effectivement un fichage illégal. Il convient de préciser que l'illégalité du fichage invoquée par la requérante était inopérant en l'espèce puisque le contentieux portait sur l'accès à ses données³, ce qui n'a pas permis de déterminer

¹ Délibération portant avis conforme sur le projet de décret présenté par le ministère de l'Intérieur portant application de l'article 31 alinéa 3 de la loi n° 78-17 du 6 janvier 1978 aux fichiers gérés par les services des renseignements généraux.

² Cf. Jean Frayssinet, *L'accès aux données nominatives des fichiers des renseignements généraux*, Communication Commercier électronique n° 10, Octobre 2002, chron. 23.

³ A ce sujet, voir F. Bossuoy, *L'accès aux fichiers des renseignements généraux*, AJDA 2002 p. 446.

si le fichage de Mme Robert avait été réellement motivé que par son appartenance à l'Eglise de scientologie. Néanmoins, relevons que les activités de l'Eglise de scientologie, considérée comme une secte au moment des faits¹, étaient surveillées par les RG qui n'auraient sans doute pas eu trop de difficultés à justifier le fichage de Mme Robert au regard des finalités du décret de 1991 et des personnes pouvant être surveillées. L'affaire ne concernait donc pas une « Eglise quelconque » mais bien une institution dont l'activité des membres était susceptible de porter atteinte au moins à la sécurité publique.

Lors de la création de la DCRI en 2008, une partie du fichier des RG et celui de la DST ont fusionné pour former CRISTINA. En pratique, il s'agissait de réaliser un « travail de titan » qui nécessitait d'examiner au cas par cas les données devant être transférées à la nouvelle DCRI, certaines données pouvant intéresser à la fois le service central du renseignement intérieur et les services du renseignement territorial de sécurité publique (SDIG)². Sur le plan juridique, le décret n° 2008-631 du 27 juin 2008 est venu affirmer publiquement l'existence légale du fichier CRISTINA et autoriser le transfert des données du fichier des RG³. Il ressort du décret que le nouveau fichier ainsi créé s'est vu appliquer l'ensemble des dérogations prévue par la loi informatique et libertés pour les fichiers de souveraineté⁴. Cette solution, qui reprend celle retenue pour le fichier de la DST, nous semble cohérente puisque le fichier intéresse, en principe, seulement la sûreté de l'Etat, ce qui implique que seules les données intéressant la sûreté de l'Etat du fichier des RG devraient avoir été transférées dans CRISTINA. Comme pour le fichier de la DST, peu d'informations sont disponibles sur ce nouveau fichier. Cependant, on relèvera que le décret de 2008 portant création du fichier a fait l'objet d'un avis favorable avec réserves de la CNIL tout comme le décret de 2017 modifiant le décret précédent⁵. En outre, la légalité de CRISTINA a été

¹ Sur ce point, voir C. Maugüé, *Communication des fichiers des renseignements généraux*, AJDA 2003 p. 2101.

² Sur la pratique, voir D. Batho et J. A. Bénisti, *Rapport d'information sur les fichiers de police*, op. cit., p. 177 et suivantes.

³ Décret n° 2008-631 du 27 juin 2008 portant modification du décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux et du décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978.

⁴ Cf. supra. *Le cadre juridique général, de la loi informatique et libertés à la loi renseignement*.

⁵ Délibération n° 2008-177 du 16 juin 2008 portant avis sur le projet de décret portant création au profit de la direction centrale du renseignement intérieur d'un traitement automatisé de données

contestée en 2010 devant le Conseil d'Etat¹ qui a rendu une décision qui participe à plus de transparence sur le cadre juridique de ce fichier². Ayant eu accès au texte créateur du fichier litigieux, le Conseil d'Etat a pu juger que le fichier autorise le traitement de « données pertinentes »³ au regard de la lutte contre l'espionnage et le terrorisme qui constituent des finalités de CRISTINA, ce qui justifie l'application des dérogations accordées par la loi de 1978. Il a également confirmé la conventionnalité du décret non publié au regard de la Conv. EDH en raison de ses finalités en considérant que le fichier constitue une mesure nécessaire à la sécurité nationale dans une société démocratique. L'arrêt du Conseil d'Etat révèle deux finalités du fichier CRISTINA qui n'étaient pas évoquées dans le décret de 1991 relatif au RG. On peut raisonnablement supposer que la finalité relative à l'espionnage renvoi au cadre juridique de l'ancien fichier de la DST. Pour ce qui concerne la finalité du terrorisme, elle avait déjà été consacrée juridiquement en 1991 pour un second fichier des RG dédié spécialement à cette finalité qui a été également absorbé par CRISTINA en 2008.

Les fichiers spécifiques au renseignement anti-terroriste

Deux fichiers particuliers de renseignement concernent le terrorisme : le FIT (fichier informatisé du terrorisme) et le FSPRT (fichier des signalements pour la prévention de la radicalisation à caractère terroriste).

Issu de l'application « violence-attentat-terrorisme », le FIT constituait le second fichier des RG dont la base légale a été consacrée et publiée en octobre 1991⁴. Avant d'être règlementé, ce fichier a donc connu les mêmes déconvenues que le fichier des RG⁵. Strictement autorisé pour la finalité de la lutte contre le

à caractère personnel dénommé « CRISTINA » ; Délibération n° 2017-156 du 18 mai 2017 portant avis sur un projet de décret modifiant le décret du 27 juin 2008 portant création au profit de la direction centrale du renseignement intérieure d'un traitement automatisé de données à caractère personnel dénommé CRISTINA.

¹ CE, 16 avril 2010, *Association AIDES et autres*, décision n° 320196.

² En ce sens, voir L. Delabie, *CRISTINA sous l'œil du Conseil d'Etat : les fichiers classés secret défense sont sous contrôle*, AJDA 2010 p. 1878.

³ La notion de « données pertinentes » désigne les données « qui sont en adéquation avec la finalité du traitement et qui sont proportionnées à cette finalité » (Cf. L. Delabie, *CRISTINA sous l'œil du Conseil d'Etat : les fichiers classés secret défense sont sous contrôle*, op. cit.).

⁴ Décret n° 91-1052 du 14 octobre 1991 relatif au fichier informatisé du terrorisme mis en œuvre par les services des renseignements généraux du ministère de l'intérieur.

⁵ En ce sens, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

terrorisme, le FIT servait à traiter deux catégories de données sur des personnes physiques surveillées et leur entourage :

- les données relatives à l'état civil, l'adresse et la profession ainsi qu'aux références du ou des dossiers pouvant concerner la personne (« *lien fonctionnel avec la documentation sur support papier ou des microformes* »¹) ;
- les données permettant l'identification de la personne surveillée (le signalement, le comportement, les numéros de téléphone, le motif du signalement, l'identité des personnes de l'entourage, les déplacements et antécédents judiciaires sauf si décision de non-lieu, de relaxe ou d'acquittement).

Les règles relatives aux personnes et données concernées par le FIT ont été confrontées aux mêmes interrogations que pour le fichier des RG. Ainsi, on relèvera les mêmes remarques qui ont été faites concernant le fichage de l'entourage surveillés et sur les précisions du ministère de l'intérieur devant la CNIL. De même, le décret relatif au FIT entendait autoriser, notamment à travers le terme « signalement », le traitement de données sensibles ethniques ou relatives aux activités politiques, philosophiques, religieuses ou syndicales². Par ailleurs, on soulignera que le Conseil d'Etat a eu l'occasion en 1995 de confirmer la légalité du décret relatif au FIT au regard de la loi informatique et libertés ainsi que sa conventionnalité au regard tant de la Conv. EDH que de la Convention 108 sur la protection des données³. La finalité spécifique de lutte contre le terrorisme a emporté, comme ce fut le cas en 2010 au sujet de CRISTINA dans l'arrêt *Association AIDES et autres*, la conviction du juge administratif sur la nécessité du FIT. Ce dernier a été finalement absorbé par le fichier CRISTINA en 2008. Enfin, ajoutons que le décret du FIT organisait un cadre coopératif entre services de renseignement en matière de lutte anti-terroriste en autorisant notamment un

¹ En ce sens, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

² A ce sujet, voir J. Frayssinet, *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, op. cit..

³ CE, 28 juillet 1995, *Confédération générale du travail* (décision n° 132452).

accès temporaire au fichier aux fonctionnaires habilités de la DST ou de la DGSE¹. Il est intéressant de noter que l'on retrouve cette logique coopérative dans le FSPRT administré par l'UCLAT au sein de la DGSI et qui constitue « *une base de données collaborative partagée avec les services de plusieurs ministères engagés dans lutte contre le terrorisme et la radicalisation violente* »².

Créé en mars 2015 par un décret non publié après avis favorable de la CNIL³, le FSPRT est un fichier de renseignement inscrit à l'article R. 841-2 du code de la sécurité intérieure qui bénéficie de l'ensemble des dérogations de loi de 1978 relatives aux traitements de souveraineté⁴. Ce fichier centralise les « *informations objectives relatives aux personnes engagées dans un processus de radicalisation, susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opération de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste* »⁵. Les informations ainsi traitées à la suite de signalements étaient initialement destinées aux services de renseignement intérieur (DGSI, SCRT et DRPP). Finalement, il a été décidé d'élargir l'accès au fichier à la DGSE, la DRSD et à l'administration pénitentiaire par un décret non publié du 30 octobre 2015 modifiant celui portant création du FSPRT⁶. Notons que ce décret a fait l'objet d'un avis favorable avec réserve de la CNIL⁷. Il est probable que les réserves émises par la CNIL concernaient les modalités d'accès au FSPRT par les nouveaux services. On notera que ces derniers disposent d'un accès indirect au fichier via le Service

¹ Sur ce point, voir M. Garrigos-Kerjan, *La tendance sécuritaire de la lutte contre le terrorisme*, Archives de politique criminelle, 2006/1 (n° 28), p. 187 à 213.

² Cf. Rubrique dédiée au FSPRT du site internet de la DGSI (<https://www.dgsi.interieur.gouv.fr/la-dgsi-en-clair/decouvrir-la-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents-2>).

³ Délibération n° 2014-499 du 11 décembre 2014 portant avis sur un projet de décret relatif à la création d'un traitement automatisé de données à caractère personnel dénommé « FSPRT ».

⁴ Décret n° 2015-252 du 4 mars 2015 modifiant le décret n° 2007-914 du 15 mai 2007 modifié pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁵ Cf. Rubrique dédiée au FSPRT du site internet de la DGSI (<https://www.dgsi.interieur.gouv.fr/la-dgsi-en-clair/decouvrir-la-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents-2>).

⁶ Sur ce point, voir G. Fenech, *Rapport d'enquête relative aux moyens mis en œuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015*, Assemblée nationale, 5 juillet 2016, p. 183.

⁷ Délibération n° 2015-342 du 6 octobre 2015 portant avis sur un projet de décret modifiant le décret portant création d'un traitement automatisé de données à caractère personnel dénommé « FSPRT ».

national des enquêtes administratives de sécurité (SNEAS)¹, ce qui devrait constituer une réponse aux inquiétudes de la CNIL. A ce sujet, la DPR a rendu un avis défavorable à la demande de la DGSE et de la DRSD d'accéder directement au FSPRT². Cette prudence nous semble judicieuse puisqu'une telle évolution conduirait la DGSE et la DRSD à accéder aux données de personnes surveillées ne relevant pas nécessairement de leur champ de compétence. En revanche, la DPR est favorable à une extension envisagée des accès au profit de Tracfin et de la DNRED dans le but de les faire contribuer « à l'évaluation des situations et des profils signalés au FSPRT »³. Pour notre part, une telle extension nous apparaît cohérente au regard de la place qu'occupent ces deux services dans la communauté française du renseignement et dans la lutte anti-terroriste à la condition que les modalités d'accès envisagées ne permettent pas un accès direct et permanent au FSPRT. En effet, le FSPRT est une base de données sensibles pouvant ficher de nombreuses personnes avec des profils variés.

Selon la doctrine d'emploi du FSPRT, les personnes signalées font l'objet d'un processus d'évaluation sur la base d'indicateurs objectifs de radicalisation comme par exemple les velléités ou départ effectif vers un théâtre de guerre, l'apologie et l'adhésion à des discours et théories subversives et violentes, une ritualisation extrême, soudaine et militante, le recours à des stratégies de dissimulation et de prosélytisme ou encore un comportement en rupture avec la société et la famille⁴. On peut raisonnablement penser que ces informations sont inscrites dans le FSPRT lorsque le signalement est validé par les services et qu'elles sont accompagnées d'informations de « signalement » sur la personne concernée en ce sens qu'elles permettent son identification. Comme dans le cas du FIT des RG, il est donc probable que les données autorisées à être traitées par le décret créant le FSPRT soient des données sensibles telles que celles portant sur l'ethnie, la race ou encore les opinions et convictions des personnes. En ce qui concerne les

¹ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 150.

² Ibid.

³ Cf. Y. Braun-Pivet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018*, op. cit., p. 57 et suivantes.

⁴ A ce sujet, voir G. Fenech, *Rapport d'enquête relative aux moyens mis en œuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015*, op. cit., p. 180 et suivantes.

personnes pouvant être fichées, il s'agirait des personnes radicalisées ou faisant l'objet d'une radicalisation, ce qui constitue une seule et large catégorie de personnes et qui peut concerner des personnes non nécessairement impliquées dans une organisation ou une activité à caractère terroriste. Cependant, remarquons que le FSPRT ne semble pas viser l'entourage de la personne signalée à la différence du FIT des RG. Ajoutons que l'organisation des accès aux données pour les services de renseignement semble établir différentes catégories de personnes au sein du FSPRT :

- en fonction du niveau de radicalisation¹ : la DGSi analyse les données des personnes ayant le plus haut niveau de radicalisation (haut du spectre), le reste des données du FSPRT sont analysées par le SCRT et la DRPP ;
- en fonction de l'activité : les données des personnes radicalisées en prison font l'objet d'une analyse par le renseignement pénitentiaire et les données des militaires radicalisés le sont par la DRSD. Enfin, les données des personnes inscrites au FSPRT qui quittent le territoire national sont notamment analysées par la DGSE². Sur ce dernier point, on soulignera que le FSPRT se limite aux personnes radicalisées présentes en France.

Plus un fichier de signalement qu'un fichier de « travail de renseignement », le FSPRT entre en concurrence, dans son utilisation, avec les fichiers propres aux services de renseignement qui traitent de données de personnes radicalisées comme par exemple le fichier CRISTINA. Selon la Commission d'enquête relative aux moyens mis en œuvre par l'Etat pour lutter contre le terrorisme depuis janvier 2015, il en résulte des risques de doublons, de confusions ou encore d'erreurs ou de manquement³. Cette commission avait alors préconisé de faire évoluer le FSPRT en une base de données exhaustive et exclusive à la lutte anti-terroriste dans la même idée que le fichier américain TIDE (The Terrorist Identities Datamart Environment). Ce dernier permet à l'ensemble de la communauté du renseignement américain d'accéder aux données des personnes suspectées de

¹ A ce sujet, voir A. Deprau, *FPR et FSPRT : quel fichier pertinent pour le suivi des radicalisés ?*, CF2R, Tribune libre n° 86, janvier 2020.

² Sur ce point, voir G. Fenech, *Rapport d'enquête relative aux moyens mis en œuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015*, op. cit., p. 183.

³ En ce sens, voir G. Fenech, *Rapport d'enquête relative aux moyens mis en œuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015*, op. cit., p. 183.

terrorisme aux niveaux national et international ainsi que de leur entourage¹. Il constitue alors un véritable fichier de « travail de renseignement » qui constitue une référence pour les services américains. Si une telle évolution peut être envisagée en France sur le plan juridique (à la condition toutefois du respect de nombreuses garanties sur les données traitées, les personnes visées ou encore les accès autorisés), il reste qu'elle devrait remettre en question la finalité terroriste des fichiers propres aux services pour véritablement neutraliser les risques de doublons.

Par ailleurs, il n'est pas certain que faire évoluer le FSPRT dans le même sens que le TIDE emporte la conviction des défenseurs des libertés. La CNCDH s'était montrée très critique à l'égard du FSPRT en 2017 allant jusqu'à demander sa suppression en estimant que « *les pouvoirs publics mettent en place un filet de détection trop étendu au regard de ce qui est requis par l'objectif de lutte contre le terrorisme, puis proposent des dispositifs de prise en charge qui sont non seulement coûteux, souvent inadaptés et à l'origine d'atteintes disproportionnées aux libertés, mais qui risquent encore d'être contre-productifs* »². Il est vrai que le FSPRT semble moins s'intéresser aux activités des personnes susceptibles ou non de porter atteinte à la sûreté de l'Etat qu'à leur opinion politique ou conviction religieuse, ce qui nous apparaît quelque peu critiquable au regard des libertés. Dans ces conditions, il ne serait donc pas souhaitable de faire du FSPRT un fichier de « travail de renseignement » pour l'ensemble des services de lutte anti-terroriste. Il conviendrait de clarifier davantage que le ciblage des personnes susceptibles d'être inscrites au FSPRT s'effectue au regard du risque de leur activité individuelle ou collective pour la sûreté de l'Etat et la sécurité publique même si la formation spécialisée du Conseil d'Etat n'a relevé aucune illégalité à propos du FSPRT dans une décision récente de juillet 2021³.

¹ Voir G. Fenech, *Rapport d'enquête relative aux moyens mis en œuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015*, op. cit., p. 184.

² CNCDH, *Avis sur la prévention de la radicalisation*, 18 mai 2017.

³ CE, 12 juillet 2021, *M. A... B...* (n° 448577).

Les fichiers du renseignement territorial et des enquêtes administratives

Dans cette catégorie de fichiers, il est possible de distinguer deux types de fichiers selon leur finalité : les fichiers de renseignement de prévention des atteintes à la sécurité publique ou à la sûreté de l'Etat au niveau territorial et ceux utilisés à des fins d'enquêtes administratives. Cette distinction puise ses origines dans le décret de 1991 encadrant le fichier des RG¹.

Lors de la réforme du renseignement intérieur de 2008, il a été envisagé de confier à la direction centrale de la sécurité publique de la Police nationale la gestion d'un nouveau fichier reprenant les informations collectées dans le fichier des RG relevant de la compétence du renseignement territorial : le fichier EDVIGE (Exploitation documentaire et valorisation de l'information générale)². Cependant, les changements apportés par les dispositions prévues par le décret portant création d'EDVIGE autorisant notamment le traitement de données relatives à des mineurs ou relatives à la santé et à la sexualité des personnes ont entraîné une importante polémique aboutissant au retrait du fichier par le gouvernement³. On rappellera toutefois que si le décret de 1991 ne prévoyait l'enregistrement de ces données, ces dernières étaient tout de même traitées dans le fichier des RG, de manière illégale pour les mineurs et légalement pour les données de santé ou sur la vie sexuelle puisqu'elles ont été considérées comme des données sensibles au sens de la loi informatique et libertés qu'à partir de la loi du 6 août 2004⁴. A la suite de cette affaire, un nouveau projet de fichier a été initié, le fichier EDVISP (Exploitation documentaire et valorisation de l'information relative à la sécurité publique). Si le projet s'est montré plus rassurant, il a été toutefois préconisé que les finalités relatives aux atteintes à la sécurité publique et aux enquêtes administratives fassent l'objet d'un fichier spécifique ainsi que l'abandon du « fichier des personnalités » qui n'apparaissaient plus indispensable⁵. Ces préconisations ont été suivies d'effets, le projet EDVIRSP a été avorté pour laisser

¹ Cf. supra. *Les fichiers du service de renseignement intérieure du premier cercle*.

² Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE ».

³ Cf. M. Jean, *EDVIGE*, Dictionnaire du renseignement, op. cit., p. 327 et suivantes.

⁴ En ce sens, voir D. Batho et J. A. Bénisti, *Rapport d'information sur les fichiers de police*, op. cit., p. 57 et suivantes.

⁵ Ibid.

place à trois nouveaux fichiers. Il a été décidé de mettre en place deux fichiers relatifs à la prévention des atteintes à la sécurité publique avec le fichier de la Police nationale PASP (Prévention des atteintes à la sécurité publique) créé en 2009¹ et celui de la Gendarmerie nationale GIPASP (Gestion de l'information et prévention des atteintes à la sécurité publique) créé en 2011². S'agissant des enquêtes administratives, cette finalité a été prévue spécifiquement par le fichier EASP (Enquêtes administratives liées à la sécurité publique) créé en 2009³.

Les décrets de 2009 et 2011 reprennent pour l'essentiel les dispositions envisagées en 1991 en tirant les conséquences du malentendu de 2008, notamment en n'interdisant le traitement portant sur des données de santé ou la vie sexuelle. En outre, le « fichier des personnalité » a été supprimé, ce qui correspond au recentrage des missions du renseignement territorial sur les dérives urbaines ou dans le sport par exemple⁴. En revanche, le fichage des mineurs a été confirmé et la liste des données susceptibles d'être traitées a été rallongée comme prévu dans le cadre du projet EDVIGE. Les données concernées sont notamment les informations relatives aux adresses physiques, aux numéros de téléphones et adresses électroniques, aux titres d'identité, à l'immatriculation des véhicules, aux informations patrimoniales, aux activités publiques, comportement et déplacements ou encore aux agissements susceptibles de recevoir une qualification pénale. A côté de ces éléments qui ont toujours fait l'objet de critiques, la notion nouvelle d'« origine géographique » introduite dans les données sensibles autorisées à être traitées dans les fichiers PASP et GIPASP a particulièrement attiré l'attention des commentateurs⁵. En effet, cette nouvelle notion n'a pas été définie dans le décret, ce qui interrogeait sur les données sensibles entrant dans son champ d'application. Validant la légalité du décret

¹ Décret n° 2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique.

² Décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique.

³ Décret n° 2009-1250 du 16 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique.

⁴ En ce sens, voir J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 154.

⁵ Sur ce point, voir notamment G. Koubi, *Les données à caractère personnel, outil des services de renseignement*, La Semaine Juridique Administrations et Collectivités territoriales n° 46, 9 novembre 2009 ; V. Gautron, *Usages et mésusages des fichiers de police : la sécurité contre la sûreté ?*, op. cit..

relatif au fichier GIPASP, le Conseil d'Etat a eu l'occasion en 2013 de préciser cette notion dans l'arrêt *Association SOS Racisme, Touche pas à mon pote*¹. La haute juridiction administrative a ainsi considéré qu'entrent dans cette notion des données qui « *doivent être en rapport direct avec le motif de l'enregistrement de la personne en cause dans le traitement* » et qui « *ne peuvent être que de nature factuelle et objective et ne sauraient, en conséquence, avoir pour effet [...] de déterminer une origine raciale ou ethnique, ni, par suite, de procéder à la collecte d'informations relatives à ces origines* » (considérant 6). Par la suite, un décret du 7 mai 2013 est venu modifier les décrets PASP et GIPASP en supprimant la notion d'origine géographique des dispositions relatives aux données sensibles pour la réintroduire dans la liste des simples données personnelles pouvant être traitées². Ne relevant donc pas des données sensibles, il a été précisé que cette notion se limite à l'indication du lieu de naissance, des lieux résidence et des zones d'activité. Sur ces indications, il a pu être soutenu que le lieu de naissance pouvait s'interpréter, de manière extensive et contraire à la décision du Conseil d'Etat à notre sens, comme une donnée sensible³.

En décembre 2020, les fichiers PASP, GIPASP et EASP, codifiés aux articles R. 236-1 et suivants du code de la sécurité intérieure, ont fait l'objet d'une extension par trois nouveaux décrets⁴ dont l'objectif est d'améliorer l'efficacité de la lutte contre le terrorisme et contre les violences qui ont notamment accompagnées le mouvement des « gilets jaunes »⁵. Ces décrets ont d'abord élargi

¹ Conseil d'Etat, 11 mars 2013, *Asscoiation SOS Racisme, Touche pas à mon pote* (requête n° 348613).

² Décret n° 2013-390 du 7 mai 2013 modifiant le décret n° 2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique et le décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et à la prévention des atteintes à la sécurité publique.

³ En ce sens, voir G. Koubi, *Décret PASP, GI-PASP. Précisions sur la donnée « origine géographique »*, site internet Droit cri-TIC, 11 mai 2013.

⁴ Le décret n° 2020-1511 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique » ; le décret n° 2020-1512 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Gestion de l'information et prévention des atteintes à la sécurité publique » ; et, le décret n° 2020-1510 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique ».

⁵ En ce sens, voir F. Dumas et F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, DPR, 1^{er} juillet 2021, p. 43 et suivantes.

les finalités des fichiers qui concernent plus largement le terrorisme et les atteintes à la sûreté de l'Etat, à l'intégrité du territoire ou des institutions de la République. Sur ce point, un risque d'amalgames entre les enjeux de sécurité publique et de sûreté de l'Etat a été souligné, d'autant plus qu'il existe d'autres traitements intéressants plus spécifiquement la sûreté de l'Etat et la lutte contre le terrorisme¹. Cette extension des finalités nous semble effectivement présenter des risques d'éparpillement, de doublons ou d'erreurs dans le traitement des données intéressant la sûreté de l'Etat, même si les décrets proposent une définition de ce type de données tout en précisant qu'elles doivent être identifiables dans le traitement. Au-delà des fichiers, l'extension de leurs finalités interroge sur la répartition des compétences entre le renseignement territorial et de sécurité publique et la DGSI en matière de sûreté de l'Etat et de lutte contre le terrorisme mais aussi sur la divergence ou la convergence de leurs doctrines dans ces domaines. Par ailleurs, l'extension des personnes et données susceptibles d'être enregistrées qui accompagnent les nouvelles finalités des fichiers PASP et GIPASP qui étaient seulement prévus pour les atteintes à la sécurité publique nous apparaissent symptomatique d'une tendance sécuritaire des pouvoirs publics.

S'agissant des personnes, les décrets de 2020 réintroduisent la possibilité de traiter des données de personnes morales mais aussi sur des groupements afin « *de mieux surveiller les activités associatives, en particulier dans le cadre de la lutte contre la radicalisation et le terrorisme* »². En ce qui concerne les données, la liste des informations pouvant être enregistrées s'est considérablement élargie en intégrant plusieurs rubriques, notamment sur : les éléments d'identification ; les coordonnées ; la situation sociale, économique et familiale ; les activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'Etat ; les facteurs de dangerosité ou encore les facteurs de fragilité de la personne. On retiendra particulièrement la possibilité de traiter des données d'identification utilisées sur internet (pseudonymes, sites et réseaux concernés et identifiants techniques) à l'exclusion des mots de passe ou relatives aux activités sur les réseaux sociaux pouvant porter atteinte à la sécurité publique ou à la sûreté de

¹ En ce sens, voir G. Koubi, *Cadences sécuritaires : des fichiers de renseignements extensibles*, La Semaine Juridique Administrations et Collectivités territoriales n° 3, 18 janvier 2021, act. 33.

² Cf. F. Dumas et F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 44.

l'Etat. Dans le cadre des données sensibles autorisées à être traitées à titre dérogatoire, les décrets de 2020 ont introduit les « données de santé révélant une dangerosité particulière » et ont supprimé la limitation liée aux « activités » pour les données relatives aux opinions politiques, philosophiques, religieuses ou syndicales.

Comme pour certains commentateurs¹, on regrettera que les décrets de 2020 n'ait pas pris en compte certaines recommandations de la CNIL et que son avis n'ait pas été sollicité lors de la rédaction définitive des textes. A la suite de la publication des décrets, la CNIL a notamment considéré que la référence « aux activités sur les réseaux sociaux » n'était pas suffisamment précisée et a tenu à rappeler qu'elle n'avait pas eu l'occasion de se prononcer sur la suppression de la limite liée aux « activités » dans le cadre des données sensibles sur les opinions². Pour les réseaux sociaux, on relèvera néanmoins que le gouvernement avait précisé « *que les informations collectées porteront principalement sur les commentaires postés sur les réseaux sociaux et les photos ou illustrations mises en ligne, ces éléments étant considérés comme pertinents dans le cadre de la prévention des atteintes à la sécurité publique ou la sûreté de l'Etat* »³. Pour autant, ces précisions n'ont pas été insérées dans la rédaction finale des décrets. Dans ces considérations, il est vrai que l'on peut s'interroger sur la légitimité des fichiers du renseignement territorial ainsi que sur l'application effective du droit de la protection des données aux fichiers de renseignement⁴. D'ailleurs, l'élargissement des données autorisées à être traitées dans les fichiers du renseignement territorial nous apparaît à contre-courant du principe de minimisation des données consacré en droit européen de la protection des données. Il pourrait alors être soulevé la question même d'une autonomie du droit des fichiers de renseignement par rapport au droit de la protection des données.

¹ Ibid., p. 46 ; G. Koubi, *Cadences sécuritaires : des fichiers de renseignements extensibles*, op. cit. ; E. Douad, *Décrets en matière de renseignement territorial*, Dalloz IP/IT 2021, p. 234.

² Cf. CNIL, *Publication des décrets relatifs aux fichiers PASP, GIPASP et EASP : la CNIL précise sa mission d'accompagnement*, 11 décembre 2020 (<https://www.cnil.fr/fr/publication-des-decrets-relatifs-aux-fichiers-pasp-gipasp-et-easp-la-cnil-precise-sa-mission>).

³ Délibération n° 2020-064 du 25 juin 2020 portant avis sur un projet de décret modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique » (demande d'avis n° 19013316).

⁴ Sur ce point, voir E. Douad, *Décrets en matière de renseignement territorial*, op. cit..

Si les décrets de 2020 ont été largement contestés, voire considérés comme un retour en force du projet EDVIGE¹, il reste que le Conseil d'Etat, saisi en référé liberté par plusieurs syndicats, n'a pas relevé d'atteinte grave manifestement illégale portée aux libertés fondamentales d'opinion, de conscience, de religion et syndicale dans leurs dispositions². La motivation de l'exécutif de la lutte contre une menace terroriste évaluée comme de plus en plus endogène semble avoir emporté la conviction du juge mais aussi celle de la DPR³. L'absence d'atteinte grave manifestement illégale portée aux libertés ne nous semble pas à remettre en question mais il conviendrait de veiller à ce que les données autorisées à être traitées soient bien identifiables pour éviter les risques d'abus. Or, il ressort des considérations précédentes que la référence « aux activités sur les réseaux sociaux » pourrait par exemple faire l'objet de précisions par le juge administratif ou l'exécutif.

Au côté de ces fichiers, le renseignement territorial parisien (Direction du renseignement de la Préfecture de police de Paris – DRPP) dispose également de son propre fichier de renseignement, GESTEREXT (Gestion du terrorisme et des extrémismes à potentialité violente). Initialement créé en 1996 sous l'intitulé GESTER, ce fichier se rapproche davantage de CRISTINA que des fichiers du renseignement territorial puisqu'il a pour finalité la sûreté de l'Etat et traite « *des données sur des personnes et des faits relatifs au terrorisme ainsi qu'à des mouvements subversifs violents et phénomènes de société précurseurs de menaces pour la sécurité nationale* »⁴. Peu d'informations sont disponibles sur le fichier GESTEREXT et sur les règles spécifiques l'encadrant. Protégé par le secret de la défense nationale, ce fichier entre dans la catégorie des fichiers de souveraineté et bénéficie de l'ensemble des dérogations prévues par la loi informatique et libertés. On notera qu'en 2017, le décret portant création du fichier GESTREXT a fait l'objet

¹ En ce sens, voir G. Koubi, *Cadences sécuritaires : des fichiers de renseignements extensibles*, op. cit..

² CE, 4 janvier 2021, *Association VIA La Voie du Peuple et autres et CGT et autres* (requêtes n° 447868 ; 447970 ; 447972 ; 447974).

³ Cf. F. Dumas et F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 46.

⁴ A ce sujet, voir D. Batho et J. A. Bénisti, *Rapport d'information sur les fichiers de police*, op. cit., p. 363 et suivantes.

d'un avis favorable avec réserves de la CNIL¹. En outre, il convient de mentionner que la DRPP et le SCRT disposent de traitements partagés de gestion électronique des documents autorisés depuis 2016 qui ont pour finalité d'améliorer et de faciliter l'analyse des phénomènes observés par les deux services². Précisons qu'il ne s'agit pas de fichiers de renseignement selon la CNIL, les données enregistrées n'ayant pas vocation à être utilisées dans le cadre de la surveillance mais pour la documentation des services³. Ces fichiers constituent tout de même des fichiers de services de renseignement, ce qui nous amène à rappeler que leur contrôle doit veiller à ce que les données personnelles enregistrées ne soient pas traitées pour une autre finalité que la documentation.

Enfin, notons que la DPR a envisagé la création d'un nouveau fichier commun dédié aux services du renseignement territorial dans une perspective de renforcement de leurs moyens, ce qui aurait notamment pour objectif de permettre aux différents services de police et de gendarmerie de profiter de leurs productions de manière égale⁴. Cette solution semble cohérente mais nécessite, à notre sens, de revoir les fichiers PASP, GIPASP et GESTEREXT afin de ne pas renforcer davantage les risques de doublons, d'éparpillements et d'erreurs dans les données, notamment s'il s'agit de données intéressant la sûreté de l'Etat.

¹ Délibération n° 2017-157 du 18 mai 2017 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « GESTEREXT ».

² Décret n° 2016-1045 du 29 juillet 2016 relatif à la mise en œuvre de traitements de conservation, de gestion et d'exploitation électroniques des documents des services du ministère de l'intérieur chargés des missions de renseignement territorial.

³ Délibération no 2015-158 du 28 mai 2015 portant avis sur un projet de décret relatif à la mise en œuvre de traitements de gestion électronique des documents des services de renseignement (demande d'avis n° 14027164).

⁴ Cf. F. Dumas et F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 92.

2. Les fichiers du renseignement extérieur et militaire

On distinguera les fichiers de la DGSE, ceux de la DRM et celui de la DRSD.

Les fichiers de la DGSE

Selon les deux listes des fichiers de souveraineté établies pour l'application de la loi informatique et libertés et de la loi relative au renseignement, trois fichiers mis en œuvre par la DGSE sont encadrés par des textes réglementaires non publiés. Il s'agit des fichiers d'informations nominatives de la DGSE créé par décret et du « fichier de la DGSE » et du « fichier du personnel de la DGSE » créés par arrêté. Deux catégories de fichiers semblent se distinguer : les fichiers des personnes *a priori* étrangères surveillées et les fichiers relatifs au fonctionnement et au personnel du service. Sur ce point, on rappellera que les fichiers de la seconde catégorie n'ont pas été insérés à l'article R. 841-2 du code de la sécurité intérieure et échappent donc à la compétence du juge du renseignement, ce qui pourrait traduire une atténuation de la protection des données des agents de la DGSE par rapport au personnes surveillées¹. Néanmoins, rappelons également que les fichiers créés par arrêté ne devraient pas porter sur des données sensibles au sens de la loi informatique et libertés, le traitement de ces données devant faire l'objet d'un décret. Pour ce qui concerne les fichiers de la DGSE soumis au contrôle de la formation spécialisée du Conseil d'Etat, on relèvera que le juge administratif n'a relevé aucune illégalité à leur encontre dans le cadre d'une affaire contentieuse en 2017².

Les fichiers de la DRM

Tout d'abord, la DRM dispose d'un fichier d'ordre général d'informations nominatives qui a été baptisé DOREMI par un décret de 2018 qui a fait l'objet d'un avis favorable avec réserves de la CNIL³. Peu d'informations sont disponibles sur ce fichier. En revanche, on retiendra qu'en 2017 la formation spécialisée du Conseil d'Etat n'a pas remis ce fichier mais a toutefois constaté que des données

¹ Cf. surpa. *Le cadre juridique général, de la loi informatique et libertés à la loi renseignement*.

² Conseil d'Etat, 8 novembre 2017, *Mme B...* (requête n° 396549).

³ Délibération n° 2018-355 du 13 décembre 2018 portant avis sur un projet de décret autorisant la mise en œuvre par la direction du renseignement militaire d'un traitement automatisé de données à caractère personnel dénommé « DOREMI ».

de la journaliste requérante figuraient illégalement dans le fichier¹. En conséquence, le juge administratif a ordonné à la DRM l'effacement des données concernées. Sans pouvoir disposer d'éléments plus précis sur cette affaire, notre analyse se limitera à confirmer les propos du Professeur Xavier Latour sur le contentieux du fichier de la DRSD² : le Conseil d'Etat affirme son nouveau rôle de juge du renseignement « contre les dérives du fichage » et les fichiers de renseignement ne sont pas à l'abri d'un dysfonctionnement comme par exemple une mauvaise saisie, des informations non actualisées ou encore un effacement tardif.

Ensuite, la DRM est le service disposant actuellement du seul fichier de renseignement de données biométriques, le fichier BIOPEX créé par un décret du 2 août 2017 non publié³. Ce fichier est destiné à traiter les données biométriques prélevées dans le cadre de l'application de l'article L. 2381-1 du code de la défense qui autorise les militaires français déployés en opération extérieure à procéder à des prélèvements biologiques d'identification sur les personnes suivantes :

- les personnes décédées lors d'actions de combat ou capturées par les forces armées ;
- les personnes dont il existe des raisons précises et sérieuses de penser qu'elles présentent une menace pour la sécurité des forces ou des populations civiles (uniquement des prélèvements salivaires et après avoir été informées des motifs et finalités du prélèvement) ;
- les personnels civils recrutés localement et les personnes accédant à une zone protégée ou placée sous le contrôle de l'autorité militaire française.

Il convient donc de relever que le fichier BIOPEX n'a pas vocation à enregistrer des données sur des personnes civiles situées sur le territoire national et qu'il concerne uniquement les opérations militaires extérieures. Toutefois, soulignons que le fichier a fait l'objet d'un avis favorable avec réserves de la CNIL⁴.

¹ Conseil d'Etat, 8 novembre 2017, *Mme B...* (requête n° 396549).

² Cf. X. Latour, *La première injonction d'effacement de données dans un fichier intéressant la sûreté de l'État : une victoire à la Pyrrhus ?*, La Semaine Juridique Edition Générale n° 23, 5 Juin 2017, 652.

³ A ce sujet, voir C. Cambon, *Rapport sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*, Sénat, 16 mai 2018, p.192.

⁴ Délibération n° 2017-216 du 13 juillet 2017 portant avis sur un projet de décret autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé BiopeX.

Le fichier de la DRSD

Créé par décret en 2014, le fichier SIREX (Système d'information de la recherche et de l'exploitation du renseignement de contre-ingérence) est le fichier de souveraineté de la DRSD qui fait suite aux fichiers de l'ancienne DPSD. Ce fichier est disponible « *dans toutes les emprises de la DRSD, y compris à l'étranger et en opérations extérieures* » à travers le système IntraRSD qui en constitue le « support »¹. Les données stockées dans ce fichier sont classifiées « confidentiel-défense » pour la plupart. Comme pour les autres fichiers de renseignement, SIREX a reçu un avis favorable avec une réserve de la CNIL². Le contenu de ce fichier est notamment utilisé à des fins d'enquêtes administratives en matière d'accès à certaines activités professionnelles dans des secteurs sensibles. C'est dans ce contexte qu'en 2017, pour la première fois, la formation spécialisée du Conseil d'Etat a été amenée à sanctionner un fichage illégal dans un fichier de renseignement³. Le signalement du requérant dans le fichier de la DRSD avait eu pour conséquence d'écarter son recrutement à un emploi dans l'aéronautique alors que des données le concernant figuraient illégalement dans le fichier litigieux, le Conseil d'Etat ordonnant ainsi l'effacement des données⁴. Comme l'a souligné le Professeur Xavier Latour, l'intervention du juge administratif « représente une protection appréciable » sans toutefois satisfaire pleinement le requérant qui n'est pas en mesure de connaître toute la réalité du fichage dont il a fait l'objet en raison de la protection du secret de la défense nationale⁵.

¹ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 176.

² Délibération n° 2014-142 du 17 avril 2014 portant avis sur un projet de décret portant création du système d'information de la recherche et de l'exploitation du renseignement de contre-ingérence dénommé « SIREX ».

³ A ce sujet, voir X. Latour, *La première injonction d'effacement de données dans un fichier intéressant la sûreté de l'État : une victoire à la Pyrrhus ?*, op. cit..

⁴ Conseil d'Etat, 5 mai 2017, *M. B...* (requête n° 396669).

⁵ Cf. X. Latour, *La première injonction d'effacement de données dans un fichier intéressant la sûreté de l'État : une victoire à la Pyrrhus ?*, op. cit..

3. Les fichiers du renseignement économique et financier

Les deux services de renseignement du ministère de l'économie, Tracfin et la DNRED, disposent chacun d'un fichier : STARTRAC (Système de traitement et analyse du renseignement de Tracfin) et BCR-DNRED (Base centrale de renseignement de la DNRED).

Le fichier STARTRAC de Tracfin

Initialement créé par un arrêté du 23 décembre 2010, le cadre juridique de ce fichier a été modifié pour être prévu par décret non publié comme le suggère l'avis favorable avec réserve de la CNIL du 23 juillet 2020¹. Cette modification pourrait avoir pour objet d'autoriser le traitement de données sensibles. En ce qui concerne la légalité du cadre fixé par l'arrêté, la formation spécialisée du Conseil d'Etat a eu l'occasion de préciser qu'elle n'avait relevé aucune illégalité, notamment au regard de la liberté d'entreprendre et de la libre circulation des capitaux garantie par le Traité sur le fonctionnement de l'Union européenne². Le fichier STARTRAC a pour finalité « *de faciliter la lutte contre le blanchiment de capitaux et le financement du terrorisme en permettant le recueil, l'analyse, l'enrichissement et l'exploitation du renseignement relatif aux infractions mentionnées à l'article L. 561-23-II alinéa 3 du code monétaire et financier* »³. Ce fichier est un fichier dit « partagé », c'est-à-dire que les données traitées n'intéressent pas toutes la sûreté de l'Etat. Ainsi, il fait l'objet d'un contrôle *ri* sur place et sur pièce de la CNIL et son contrôle juridictionnel relève à la fois du juge du renseignement et du juge administratif de droit commun. A ce sujet, Tracfin a réclamé que le contentieux de l'ensemble de son fichier soit soumis à la formation spécialisée du Conseil d'Etat car il est difficile en pratique pour le service de déterminer avec certitudes les données intéressant la sûreté de l'Etat⁴. Cette solution nous semble excessive tant en matière de protection des données qu'au

¹ Délibération n° 2020-084 du 23 juillet 2020 portant avis sur un projet de décret autorisant la mise en œuvre par le service à compétence nationale TRACFIN d'un traitement automatisé de données à caractère personnel dénommé « STARTRAC » et un projet de décret modifiant l'article R. 841-2 du code de la sécurité intérieure et le décret n° 2007-914 du 15 mai 2007 pris pour application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

² Conseil d'Etat, 20 décembre 2017, *M. A...* (décision n° 396564).

³ Cf. Assemblée nationale. Question n° 104673, du 12 avril 2011.

⁴ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 124.

regard des finalités du fichier, d'autant plus que les données intéressant la sûreté de l'Etat ont été définies depuis les décrets de 2020 relatifs aux fichiers PASP, GIPASP et EASP.

Le fichier BCR-DNRED

Très peu d'informations sont disponibles sur ce fichier qui a fait l'objet d'un décret non publié en 2016 et d'un avis favorable avec réserve de la CNIL¹. Ce fichier intéressant la sûreté de l'Etat est inscrit dans la liste de l'article R. 841-2 du code de la sécurité intérieure et devrait porter sur des données sensibles comme la plupart des fichiers des services de renseignement.

4. Le fichier CAR du renseignement pénitentiaire

Ayant pour finalité le suivi des personnes placées sous main de justice et destiné à la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique, le fichier CAR a été introduit en 2015 par un décret non publié. Il a reçu un avis favorable avec réserve de la CNIL². Comme pour le fichier de la DNRED, ce fichier traiterait de données sensibles et très peu d'informations sont disponibles à son sujet. Toutefois, soulignons que ce fichier n'a pas été intégré à la liste de l'article R. 841-2 du code de la sécurité intérieure et n'entre donc pas dans la compétence du juge du renseignement. Il semblerait alors que ce fichier de sécurité publique ne porte pas sur des données intéressant la sûreté de l'Etat, ce qui serait cohérent au regard des finalités du renseignement pénitentiaire prévues à l'article L. 855-1 du code de la sécurité intérieure³. En revanche, la prévention du terrorisme figure parmi les finalités du Service national du renseignement pénitentiaire (SNRP)⁴. Or, cette dernière finalité pourrait impliquer en pratique le traitement illégal de données intéressant la sûreté de l'Etat par le SNRP. Si tel est

¹ Délibération n° 2016-010 du 21 janvier 2016 portant avis sur un projet de décret portant création au profit de la direction nationale du renseignement et des enquêtes douanières d'un traitement automatisé de données à caractère personnel dénommé « BCR-DNRED ».

² Délibération n° 2015-128 du 23 avril 2015 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel relatif au suivi des personnes placées sous main de justice et destiné à la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique dénommé « CAR ».

³ « Prévenir les évasions et d'assurer la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues » (alinéa 1 de l'article L. 855-1 du code de la sécurité intérieure).

⁴ Décret n° 2019-1503 du 30 décembre 2019 modifiant diverses dispositions relatives au renseignement pénitentiaire.

le cas, il conviendrait d'introduire la finalité relative à la sûreté de l'Etat et au terrorisme dans le décret relatif à CAR et d'intégrer ce fichier dans la liste de l'article R. 841-2 pour les seules données intéressant la sûreté de l'Etat.

On relèvera que tous les décrets étudiés portant création des fichiers de renseignement ont reçu un avis favorable avec une ou plusieurs réserves de la CNIL, ce qui tend à montrer une difficile conciliation entre le droit de la protection des données et les intérêts du renseignement qui est davantage favorable à ce dernier. Le contrôle juridictionnel en cette matière attribué par la loi relative au renseignement à la formation spécialisée du Conseil d'Etat constitue alors un outil juridique indispensable pour assurer le respect des droits et libertés dans cette difficile conciliation.

Au-delà de l'encadrement des fichiers de renseignement eux-mêmes, la régulation du partage des données constitue également une problématique croissante pour le droit du renseignement, à commencer par la question des accès aux fichiers et du rapprochement d'informations qui en découle.

§2. Les accès aux fichiers et le rapprochement d'informations

Les accès aux fichiers ne doivent pas être, ici, confondus avec le droit d'accès direct ou indirect des personnes à leurs données personnelles. Il s'agit des autorisations accordées par la loi ou les textes réglementaires aux services de renseignement d'accéder à d'autres fichiers. De manière générale, les textes conditionnent ces accès à de simples consultations des données par des agents habilités dans la limite du « besoin d'en connaître » et pour des finalités liées à leurs missions¹. En outre, les consultations font l'objet d'un dispositif de traçabilité et ne permettent pas des interconnexions avec les fichiers de renseignement². En revanche, elles peuvent aboutir à des rapprochements, c'est-à-dire « *la comparaison visuelle d'informations issues de deux fichiers ou encore l'enrichissement d'un fichier existant par saisie manuelle d'informations issues d'un*

¹ Ces conditions ont notamment été rappelées par le juge des référés du Conseil d'Etat dans sa décision relative au fichier PASP du 4 janvier 2021 (Conseil d'Etat, 4 janvier 2021, *Confédération générale du travail*, requête n° 447970, considérant 14).

² Cf. infra. §3. *Les interconnexions entre les fichiers*.

autre fichier »¹. Deux catégories d'accès peuvent être distinguées : les accès autorisés au sein de la communauté du renseignement et ceux autorisés en dehors de la communauté.

A - Au sein de la communauté du renseignement

Ce type de dispositif de partage des données est notamment mis en œuvre en matière de lutte contre le terrorisme. Ainsi, le décret de 1991 relatif au FIT des RG autorisait la consultation des données par des agents de la DST et de la DGSE « *habilités par une décision à caractère personnel, temporaire et révocable* »². Aujourd'hui, le FSPRT géré par l'UCLAT au sein de la DGSi prévoit des accès au SCRT, à la DRPP ainsi qu'à la DGSE et à la DRSD, notamment via le SNEAS. Un élargissement est également envisagé à Tracfin et à la DNRED³.

S'agissant des autres fichiers de renseignement dont les décrets non pas été publiés, on peut raisonnablement supposer que des accès sont prévus comme par exemple un accès au fichier CRISTINA par les agents de la DGSE comme dans le cadre du décret de 1991 relatif au FIT. En revanche, on relèvera que les textes encadrant les fichiers PAPS et GIPASP n'ont pas prévus d'accès aux autres services que ceux du renseignement territorial et du SNEAS pour les enquêtes administratives. Cette solution a d'ailleurs été critiquée à plusieurs reprises par des rapports parlementaires qui préconisaient d'autoriser un accès aux agents de la DGSi⁴. A notre sens, il est effectivement curieux que la DGSi ne puisse pas consulter les fichiers PAPS et GIPASP, notamment depuis que ces derniers sont autorisés à traiter des données intéressant la sûreté de l'Etat et la lutte contre le terrorisme. En outre, il serait également souhaitable que la création d'un fichier commun dédié aux services du renseignement territorial préconisé par la DPR puisse prévoir un droit de consultation pour la DGSi⁵. Plus généralement, il nous

¹ Cf. [Comment déterminer la notion d'interconnexion ? | CNIL](https://www.cnil.fr/en/node/15316) (https://www.cnil.fr/en/node/15316).

² Article 5 du décret n° 91-1052 du 14 octobre 1991 relatif au fichier informatisé du terrorisme mis en oeuvre par les services des renseignements généraux du ministère de l'intérieur.

³ Cf. supra. *Les règles spécifiques aux fichiers de renseignement*.

⁴ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 131.

⁵ Cf. F. Dumas et F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 92.

semble légitime que les agents puissent consulter les fichiers des autres services dans la limite du « besoin d'en connaître » et pour les finalités de leurs missions.

Pour aller plus loin, Jean-Jacques Urvoas a émis l'hypothèse de la création d'un fichier commun similaire au Fichier national des objectifs en matière de stupéfiants (FNOS) qui permettrait de faciliter les rapprochements entre les fichiers de renseignement¹. Le fichier FNOS a pour finalité la coordination des services concernés dans les investigations judiciaires ou douanières portant sur des individus impliqués dans le trafic de stupéfiants². Il s'agit d'une interface répertoriant les enquêtes qui permet d'alerter les services utilisateurs sur « *l'existence de fiches comportant des éléments communs* » afin que les services puissent se contacter pour procéder aux rapprochements des informations³. En matière de renseignement, un fichier thématique relatif à la lutte contre le terrorisme ou à la contre-ingérence pourrait reprendre ce dispositif pour faciliter les rapprochements d'informations entre les services et coordonner la surveillance d'un individu. En revanche, la mise en œuvre d'un fichier commun portant sur les différentes thématiques du renseignement accessible à l'ensemble des services nous semble une solution difficilement acceptable au regard de la jurisprudence du Conseil constitutionnel peu favorable à la mise en œuvre de traitements trop généraux⁴, comme le remarque Floran Vadillo⁵. Au regard des nombreuses données traitées par les différents services et des profils variés de personnes qui sont fichées, la constitution d'un tel fichier commun nous semble effectivement présenter un risque élevé pour la protection des données personnelles et les droits fondamentaux mais aussi en matière de contre-espionnage.

¹ Cf. Entretien avec Jean-Jacques Urvoas, *Était-il tolérable que la France soit le seul Etat européen où les services de renseignement agissaient en dehors de tout cadre juridique ?*, op. cit..

² Arrêté du 11 juillet 2012 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « Fichier national des objectifs en matière de stupéfiants » (FNOS).

³ Délibération n° 2012-084 du 22 mars 2012 portant avis sur un projet d'arrêté autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « Fichier national des objectifs en matière de stupéfiants » (FNOS).

⁴ Cette position du Conseil constitutionnel a été affirmée dans sa décision n° 2011-625 DC du 10 mars 2011 (considérant 71) à propos des logiciels de rapprochement judiciaire.

⁵ Cf. F. Vadillo, *Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?*, Les Cahiers de la sécurité, n° 47, février 2020, p. 43-52.

Dans la continuité des réflexions du rapport des députés Didier Paris et Pierre Morel-A-L'Huissier sur les fichiers de 2018¹, Floran Vadillo va plus loin en proposant la mise en place d'une interface « *hit/no hit* » qui aboutirait à une procédure d'autorisation de levée d'anonymat sur les données enregistrées en cas de recoupements pertinents sur le modèle du cadre juridique de la surveillance algorithmique prévu à l'article L. 851-3 du code de la sécurité intérieure². Le service demandeur aurait donc directement accès aux données enregistrées dans le fichier après autorisation de la CNCTR. Cette solution nous semble cohérente à partir du moment où les services utilisateurs peuvent directement consulter des données partagées volontairement par leurs homologues sous le contrôle de la CNCTR qui veillerait à la pertinence des accès. Néanmoins, ce contrôle pourrait impliquer un accès de la CNCTR à des données des fichiers des services de renseignement, ce qui n'est actuellement pas permis par les textes.

On relèvera que le choix de mettre en œuvre des interfaces thématiques conduirait à une nouvelle augmentation des fichiers de renseignement déjà critiquée par les défenseurs des libertés. Les critiques seraient d'autant plus grandes si ces interfaces sont interprétées comme des instruments de surveillance plus que comme une rationalisation de cette dernière, ce que semble suggérer la proposition de Floran Vadillo sur le modèle de l'article L. 851-3 du code de la sécurité intérieure.

B - En dehors de la communauté du renseignement

Les accès des services ont été progressivement étendus par la loi à des fichiers gérés par d'autres administrations, l'autorité judiciaire ou à des données traitées par des acteurs privés.

1. L'accès à des fichiers administratifs

La loi anti-terroriste du 23 janvier 2006 a autorisé les services de renseignement du ministère de l'intérieur et du ministère de la défense chargés de la lutte contre le terrorisme d'accéder à un certain nombre de fichiers administratifs du ministère de l'intérieur : le fichier national des

¹ Cf. D. Paris et P. Morel-À-L'Huissier, *Rapport d'information sur les fichiers mis à disposition des forces de sécurité*, op. cit., p. 46 et 47.

² Cf. F. Vadillo, *Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?*, op. cit..

immatriculations ; le système national de gestion des permis de conduire ; le système de gestion des cartes nationales d'identité ; le système de gestion des passeports ; et, les fichiers relatifs aux étrangers introduits à l'article L. 222-1 du code de la sécurité intérieure¹. Par la suite, la loi de programmation militaire (LPM) du 18 décembre 2013 a étendu l'accès des fichiers de l'article L. 222-1 à l'ensemble des services de renseignement du premier cercle pour les besoins de la lutte contre le terrorisme mais aussi pour la prévention des atteintes aux intérêts fondamentaux de la Nation². Dans le cadre de ces accès, une préoccupation particulière concernait l'accès des services à des données biométriques enregistrées dans les fichiers relatifs à l'identité des personnes, notamment à des fins de reconnaissance biométrique en renseignement³. Non seulement le dispositif interdit l'interconnexion des fichiers avec ceux du renseignement mais il interdit également l'accès des services aux données des empreintes digitales⁴. Ces limitations nous semblent légitimes afin d'éviter le basculement vers une surveillance de la population par reconnaissance biométrique via les fichiers d'identités électroniques⁵.

2. L'accès à des fichiers judiciaires

La loi de programmation militaire de 2013 a affirmé au niveau législatif la possibilité déjà permise pour les services du premier cercle d'accéder au traitement des antécédents judiciaires (TAJ) dans le cadre des enquêtes administratives⁶. Cette limitation avait été remise en cause par les députés Jean-Jacques Urvaos et Patrice Verchère dans leur rapport de 2013 sur le cadre

¹ Article 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

² Article 15 de la 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.

³ En ce sens, voir M. Quémener, *Présentation du décret du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (TES)*, Dalloz IP/IT 2017, p. 58.

⁴ Cf. Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

⁵ Cf. infra. Section II, §2. *La technologie biométrique*.

⁶ Article 18 de la 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.

juridique du renseignement, soulignant l'utilité que peut avoir ces fichiers judiciaires pour connaître le passé judiciaire des personnes surveillées¹.

La loi relative au renseignement de 2015 a finalement autorisé les services du premier et second cercles déterminés par décret à accéder au TAJ au-delà des enquêtes administratives pour les finalités suivantes : l'indépendance nationale, l'intégrité du territoire et la défense nationale ; la prévention du terrorisme ; et, la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique². Notons qu'en 2020, le « rapport Larrivé » sur l'évaluation de la loi relative au renseignement de 2015 s'est montré satisfait de ce dispositif et n'a pas souhaiter remettre en cause la limite relative à l'exclusion des accès aux données du TAJ portant sur les victimes, ce qui avait été préconisé en 2018 par le rapport d'information des députés Didier Paris et Pierre Morel-A-L'Huissier³. Pour notre part, aucune raison valable justifie un élargissement aux données des victimes pour les besoins du renseignement, d'autant plus que ces données concernent « *plusieurs dizaines de millions de personnes* » selon le « rapport Larrivé ». Toujours en relation avec l'autorité judiciaire, la loi relative au renseignement de 2015 a créé un nouveau fichier de lutte contre le terrorisme, le fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT)⁴. Notamment destiné à prévenir la récidive d'auteurs d'infractions terroristes, ce fichier est directement accessible pour les services de renseignement par l'intermédiaire d'un système de communications électroniques sécurisé.

La création du FIJAIT a pu soulever la question d'un décloisonnement entre les services de renseignement et l'autorité judiciaire ou d'une simple mutualisation des moyens en matière de lutte contre le terrorisme⁵. Il est certain

¹ Cf. J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 26 et suivantes.

² Article 20 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

³ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 129 et 130.

⁴ Article 19 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

⁵ Sur ce point, voir D. Thomas-Taillandier, *Le nouveau fichier national des auteurs d'infractions terroristes*, AJ Pénal 2015, p. 253.

qu'une mutualisation est à l'œuvre dans la lutte contre le terrorisme comme en témoigne le FIJAIT mais aussi le FSPRT dont les signalements proviennent de certains services de police judiciaire¹. Relevons qu'il a notamment été proposé de permettre un accès au FSPRT aux procureurs de la République². Pour autant, la loi relative au renseignement de 2015 semble davantage aller dans le sens d'un décloisonnement des fichiers si l'on ajoute les dispositions relatives au TAJ. On peut comprendre l'utilité des données judiciaires pour le renseignement, notamment pour améliorer la connaissance des services sur les procédés terroristes et criminels, à condition que les accès se limitent à des données pertinentes (ce qui n'est pas le cas des données du TAJ relatives aux victimes par exemple). A ce sujet, il nous apparaît superflu de permettre un accès à la DGSJ au fichier national des personnes incarcérées comme souhaité par les députés Didier Paris et Pierre Morel-A-L'Huissier et le « rapport Larrivé ». D'une part, ce fichier a été créé pour « *la gestion des affectations pénitentiaires des détenus ainsi que la production de statistiques sur la population pénale* »³, ce qui implique que peu d'informations devraient réellement intéresser la DGSJ et, par là même, aboutir à ouvrir un accès qui pourrait finalement ne pas être exploité par les agents. D'autre part, il serait plus pertinent d'envisager l'analyse du parcours d'un détenu dans le cadre d'une coopération entre la DGSJ et le SNRP avant d'ouvrir des accès à de nouveaux fichiers en dehors de la communauté du renseignement.

En revanche, la « judiciarisation du renseignement », c'est-à-dire l'utilisation des données des services de renseignement par les services judiciaires, s'avère plus délicate en raison des principes gouvernant la procédure pénale (présomption d'innocence, droit de la preuve et droit à un procès équitable). Cette judiciarisation apparaît cependant inévitable pour deux raisons : la première tient aux dispositions de l'article 40 du code de procédure pénale qui obligent les services de renseignement à saisir l'autorité judiciaire en cas de

¹ En ce sens, voir [Le fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste \(FSPRT\) | DGSJ \(interieur.gouv.fr\)](https://www.dgsi.interieur.gouv.fr/la-dgsi-en-clair/decouvrir-la-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents-2) (<https://www.dgsi.interieur.gouv.fr/la-dgsi-en-clair/decouvrir-la-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents-2>).

² Cf. D. Paris et P. Morel-À-L'Huissier, *Rapport d'information sur les fichiers mis à disposition des forces de sécurité*, op. cit., p. 52.

³ Arrêté du 20 février 2003 modifiant l'arrêté du 28 octobre 1996 portant création d'un fichier national automatisé des personnes incarcérées.

découverte d'une infraction, ce qui implique une certaine « primauté » de l'autorité judiciaire sur le renseignement¹ ; la seconde renvoi à « *l'importance croissante des données du renseignement pour l'office du juge* », notamment avec le recours aux techniques de renseignement dans la lutte contre le terrorisme comme le relève Bertrand Warusfel². En outre, la Cour de cassation ne s'oppose pas à la judiciarisation du renseignement qui peut être utile pour guider les investigations judiciaires mais considère généralement que les données du renseignement ne suffisent pas à fonder une condamnation, ces données ne remplissant pas les conditions probatoires et procédurales nécessaires³. Sans remettre en question la judiciarisation du renseignement, il nous semble cependant peu recommandable que le décroisement opéré dans le cadre des accès aux fichiers puisse aboutir à un droit d'accès des services répressifs aux fichiers de renseignement. On pourrait alors assister à une judiciarisation systématique du renseignement potentiellement porteuse d'un renforcement de la surveillance administrative au nom de la « primauté » de l'autorité judiciaire et d'une police de plus en plus prédictive qui pourrait remettre en cause les principes de la procédure pénale ainsi que constituer le « spectre d'une surveillance de masse liberticide ».

L'idée d'un « renseignement criminel » n'est pas non plus à remettre en question mais son intégration dans le cadre juridique du renseignement ainsi que la possibilité de créer un fichier mélangeant des données administratives et judiciaires comme proposé par Floran Vadillo conduirait nécessairement à un élargissement considérable de la surveillance administrative voire à son détournement, d'autant plus que le destinataire légitime de ce type de renseignement serait davantage l'autorité judiciaire que l'exécutif⁴. Rappelons que l'opportunité des mesures de surveillance et l'analyse des données collectées en renseignement sont guidées par les intérêts de l'Etat alors que les enquêtes

¹ La loi relative au renseignement de 2015 a notamment rappelé que les techniques de renseignement sont mises en œuvre sur le territoire national sans préjudice de l'article 40 du code de procédure pénale (article L. 811-2 du code de la sécurité intérieure).

² Cf. B. Warusfel, *Justice et renseignement dans la lutte contre la radicalisation violente*, AJ Pénal 2018, p. 119.

³ Sur ce point, voir E. Clément, *Le juge et l'espion*, AJ Pénal 2021, p. 376.

⁴ Cf. F. Vadillo, *Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?*, op. cit..

judiciaires s'inscrivent dans le cadre de la répression des infractions pénales même si ces dernières peuvent concerner les intérêts fondamentaux de la Nation. La judiciarisation du renseignement ne peut alors être qu'« incidente ». A notre sens, l'introduction d'un « renseignement criminel » dans la communauté du renseignement inviterait alors à revoir la politique publique du renseignement et le concept même de renseignement d'Etat en France qui est tourné vers la défense et la sécurité nationale plus que la sécurité des personnes et des biens. Au demeurant, le renseignement territorial peut déjà mettre en lumière des infractions de droit commun, ce qui invite davantage à judiciariser ce type de renseignement. A ce titre, la DPR préconise un accès du renseignement territorial aux fichiers judiciaires¹. Il convient de rester prudent sur le risque d'une réorientation des missions du renseignement territorial sur les investigations judiciaires. Néanmoins, cette solution nous semble permettre une judiciarisation proportionnée sans avoir à redéfinir les contours du renseignement d'Etat, à condition qu'elle reste « incidente ».

3. L'accès à des données d'acteurs privés

La loi du 23 janvier 2006 a autorisé la mise en œuvre par le ministère de l'intérieur de fichiers « PNR » (« *Passenger Name Record* » ou « données des dossiers passagers » en français) relatifs aux données des passagers de transporteurs aériens, maritimes ou ferroviaires pour les déplacements internationaux en dehors de l'Union européenne². Ce dispositif a notamment prévu un accès aux données aux agents du renseignement intérieur chargés de la lutte contre le terrorisme. En 2011, l'accès à ce dispositif a été étendu aux agents des services de renseignement du ministère de la défense également chargés de la prévention des actes de terrorisme³. Essentiellement porté sur les transporteurs aériens avec la création par arrêtés du fichier des passagers aériens (FPA)⁴ puis

¹ Cf. F. Dumas et F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 87.

² Article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

³ Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

⁴ Arrêté du 19 décembre 2006 pris pour l'application de l'article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers et portant création, à titre expérimental, d'un traitement automatisé de

du Système européen de traitement des données d'enregistrement et de réservation (SETRADER)¹, le dispositif a connu des difficultés techniques avant d'être revu fin 2013².

Ainsi, la loi de programmation militaire de 2013 est venue définir à l'article 232-7 du code de la sécurité intérieure les principes encadrant un nouveau dispositif PNR français portant sur les données transporteurs aériens. Sur cette base nouvelle, il a été créé le fichier « système API-PNR France » permettant notamment aux services de renseignement du premier cercle d'être destinataires des données des passagers conservées et transmises par les transporteurs aériens pour les vols à destination ou en provenance du territoire national à l'exception des vols à l'intérieur de la France métropolitaine³.

Renforçant le dispositif des accès aux données des transporteurs internationaux, la loi n° 2016-816 du 20 juin 2016 pour « l'économie bleue » a introduit dans le dispositif de l'article L. 232-7 du code de la sécurité intérieure les données des passagers des transporteurs maritimes à titre expérimental⁴. Par la suite, la loi SILT du 30 octobre 2017 est venue confirmer cette expérimentation avec la création de l'article L. 232-7-1⁵. Les données accessibles aux services de renseignement concernent notamment des navires battant pavillon français ou étranger sur des liaisons françaises et entre la France et l'étranger⁶. On relèvera que la loi SILT a également adapté le PNR français aux règles du PNR européen issues de la directive 2016/681 du 27 avril 2016. Toutefois, si la CJUE ne remet pas en cause l'existence des fichiers PNR, sa jurisprudence en matière de droits

données à caractère personnel relatives aux passagers enregistrées dans les systèmes de contrôle des départs des transporteurs aériens.

¹ Arrêté du 11 avril 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé SETRADER.

² En ce sens, voir J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 26 et suivantes.

³ Décret n° 2014-1095 du 26 septembre 2014 portant création d'un traitement de données à caractère personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure.

⁴ Sur ce point, voir X. Latour, *La participation des personnes privées au contrôle des migrations en France*, AJDA 2019, p. 264.

⁵ Article 14 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

⁶ A ce sujet, voir M. Quémener, *Les dispositions en lien avec le numérique de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme*, Dalloz IP/IT 2017, p. 657.

fondamentaux et de protection des données personnelles pourrait remettre en cause le PNR européen et impacter le dispositif français¹. En effet, la participation légitime des personnes privées dans la surveillance des déplacements internationaux n'est pas sans risque d'une surveillance massive potentiellement liberticide, ce qui nécessite de « *donner les gages de la fiabilité et de l'utilité des partenariats* »². Comme pour les partenariats avec les opérateurs du numérique pour les accès aux données de connexion, cette participation a pour conséquence légitime de faire intervenir le droit européen de la protection des données dans la régulation des moyens numérique du renseignement³.

En plus des fichiers administratifs, judiciaires et des données d'acteurs privés, il convient de mentionner que certains services de renseignement peuvent accéder à deux autres fichiers qui n'entrent pas spécifiquement dans les trois catégories précédentes. Il s'agit tout d'abord du Fichier des personnes recherchées (FPR) géré par le ministère de l'intérieur qui est utilisé pour des motifs judiciaires, administratifs et d'ordre public⁴. On retiendra que les services de renseignement du ministère de la défense n'ont accès aux données du FPR que pour les besoins de la lutte contre le terrorisme. En outre, ce fichier présente la particularité d'avoir été intégré à la liste de l'article R. 841-2 du code de la sécurité intérieure relatif au contentieux du juge du renseignement puisqu'il porte sur des données pouvant intéresser la sûreté de l'Etat. Pour les autres données, le contentieux du droit d'accès au FPR relève de la compétence du juge administratif de droit commun, ce qui en fait un fichier « partagé » compliqué à contester⁵. On notera que la formation spécialisée du Conseil d'Etat⁶ a eu l'occasion de confirmer la conventionnalité du FPR au regard de la Conv. EDH dans une décision de 2017⁷.

¹ En ce sens, voir X. Latour, *Les fichiers PNR et les transporteurs aériens internationaux*, Annuaire 2018 du droit de la sécurité et de la défense, Mare et Martin, 2018, p. 247 et suivantes.

² En ce sens, voir X. Latour, *La participation des personnes privées au contrôle des migrations en France*, op. cit..

³ Cf. infra. Seconde Partie.

⁴ Décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées.

⁵ En ce sens, voir J. Schmitz, *Le juge administratif et le contentieux du droit d'accès indirect aux fichiers de renseignement*, AJDA 2018, p. 406.

⁶ Conseil d'Etat, 6 novembre 2017, n° 409075.

⁷ Sur ce point, voir C. Friedrich, *Compétence du Conseil d'Etat en matière de renseignement : une délimitation restrictive*, La Semaine Juridique Administrations et Collectivités territoriales n° 46, 20 novembre 2017.

Sans être un fichier de renseignement proprement dit, le FPR semble cependant marqué par l’empreinte des services et de leurs missions de sécurité nationale dans l’évolution de son encadrement.

Ensuite, cette dernière réflexion concerne également le Système d’information Schengen (N-SIS II) ayant pour finalité de permettre aux Etats membres de consulter des signalements sur des personnes ou des biens circulant dans l’espace Schengen¹. Ce fichier est notamment accessible aux renseignements intérieur et douanier². Comme le FPR, il est inscrit à l’article R. 841-2 pour ce qui concerne les données relatives aux personnes et aux biens « *nécessaires à la prévention d’une menace grave émanant de l’intéressé ou d’autres menaces graves pour la sûreté intérieure et extérieure de l’Etat* »³. Instrument de coopération inter-étatique, la DPR n’a pas manqué de souligner en 2016 que le fichier N-SIS II souffre d’une faible implication des Etats partenaires, notamment en France où seule la DGSJ alimenterait ce fichier⁴.

Enfin, il convient de préciser que les fichiers API-PNR, FPR et le N-SIS II font l’objet d’interconnexions qui ne concernent pas directement les fichiers de renseignement mais qui nous amènent à étudier cette notion qui est de plus en plus mise en avant en matière de renseignement.

¹ Cf. [SIS II : Système d’information Schengen II | CNIL](https://www.cnil.fr/fr/sis-ii-systeme-dinformation-schengen-ii) (<https://www.cnil.fr/fr/sis-ii-systeme-dinformation-schengen-ii>).

² A ce sujet, voir la liste des autorités compétentes autorisées à consulter directement les données introduites dans le système d’information Schengen de deuxième génération, présentée conformément à l’article 31, paragraphe 8, du règlement (CE) no 1987/2006 du Parlement européen et du Conseil et à l’article 46, paragraphe 8, de la décision 2007/533/JAI du Conseil sur l’établissement, le fonctionnement et l’utilisation du système d’information Schengen de deuxième génération.

³ Article R. 231-8 du code de la sécurité intérieure.

⁴ Cf. J. -P. Raffarin, *Rapport relatif à l’activité de la délégation parlementaire au renseignement pour l’année 2015*, op. cit., p. 79 et 80.

§3. Les interconnexions entre les fichiers

L'interconnexion est une notion développée en droit de la protection des données qui « doit être regardée comme l'objet même d'un traitement qui permet d'accéder à, d'exploiter et de traiter automatiquement les données collectées pour un autre traitement et enregistrées dans le fichier qui en est issu » selon le Conseil d'Etat¹. De son côté, la CNIL retient trois critères pour déterminer une interconnexion : la mise en relation de fichiers de données personnelles ; la mise en relation d'au moins deux fichiers distincts ; la mise en relation doit être automatisée². On ajoutera que lorsque « les fichiers interconnectés sont issus de traitements ayant des finalités différentes », alors ce type d'interconnexion doit être autorisé préalablement par la CNIL³.

Auditionnée dans le cadre du rapport des députés Delphine Batho et Jacques Alain Bénisti sur les fichiers de police⁴, la CNIL a eu l'occasion de présenter les risques et opportunités des interconnexions. Elles peuvent aboutir à des détournements des finalités des fichiers ou à leur extension non prévue. Elles peuvent également entraîner des modifications techniques normalement proscrites par la loi comme par exemple l'accès illégal à des données protégées par un secret professionnel. Enfin, les interconnexions peuvent mettre en danger la sécurité des données ou remettre en question la limite de leur durée de conservation. En revanche, l'interconnexion constitue une solution technique à la mise à jour automatique des données, ce qui est gage d'une meilleure protection des droits garantis par la loi informatique et libertés. Sur ce point, l'interconnexion a pu être jugée intéressante en matière judiciaire pour pouvoir mettre à jour automatiquement et en cohérence la chaîne pénale⁵. En matière de renseignement, il s'agirait alors de mettre à jour automatiquement et en cohérence

¹ Conseil d'Etat, 19 juillet 2010, *M. F. et Mme C.* (décision n° 317182, 323441).

² Cf. [Comment déterminer la notion d'interconnexion ? | CNIL](https://www.cnil.fr/en/node/15316) (<https://www.cnil.fr/en/node/15316>).

³ Ibid.

⁴ Cf. D. Batho et J. A. Bénisti, *Rapport d'information sur les fichiers de police*, op. cit., p. 96 et 97.

⁵ Sur ce point, voir R. Vedel, *Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure*, AJ Pénal 2007, p. 64.

le cycle du renseignement dans la surveillance d'un individu qui ferait intervenir plusieurs services et donc plusieurs fichiers.

L'interconnexion des fichiers de renseignement a nécessairement pour effet d'augmenter les capacités de surveillance de l'Etat, voire opérerait un glissement vers une société de surveillance dans le cas où des interconnexions, notamment en temps réel, seraient largement étendues à des fichiers administratifs, judiciaires et privés. Pour autant, l'interconnexion des fichiers de renseignement apparaît inévitable pour plusieurs raisons. D'abord, les accès aux fichiers et le rapprochement d'informations demandent beaucoup de temps pour les services et ne permettent pas de faire émerger des « signaux faibles » dans la masse de données¹. Ensuite, l'interconnexion améliorerait la cohérence et la fiabilité des fichiers tout en permettant leur décloisonnement². En outre, les interconnexions permettraient de constituer un cadre adapté au développement de l'IA en renseignement selon Floran Vadillo³. Enfin, l'argument le plus favorable aux interconnexions des fichiers de renseignement est que la CNIL ne s'y oppose pas par principe dès lors que la protection des données est assurée⁴.

Il n'en demeure pas moins qu'aujourd'hui peu d'interconnexions sont mises en œuvre dans le domaine du renseignement. Deux exemples particuliers peuvent être mentionnés sans toutefois révéler un véritable modèle de partage automatisé des fichiers de renseignement.

Ainsi, on peut citer le fichier ACCReD (Automatisation de la consultation centralisée de renseignements et de données⁵) qui permet de trier et d'identifier les informations (ou le « criblage ») portant sur une personne enregistrée dans

¹ Sur ce point, voir J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 50.

² En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 131 et suivantes.

³ Cf. F. Vadillo, *Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?*, op. cit..

⁴ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 132.

⁵ Décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD) et décret n° 2019-1074 du 21 octobre 2019 modifiant le décret n° 2017-1224 du 3 août 2017.

plusieurs fichiers dans le cadre des enquêtes administratives¹. Clairement identifié comme une interconnexion par la CNIL², le dispositif prend la forme d'une interface « hit/no hit » qui permet notamment d'interroger les fichiers FSPRT, CRISTINA, SIREX, DGSE mais aussi PASP, GIPASP et EASP ou encore FPR et N-SIS II³. Toutefois, on précisera que la mise en relation des fichiers de renseignement est « dégradée » en ne permettant seulement qu'un signalement automatique de personnes aux services qui procèdent manuellement à une vérification dans leur fichier par la suite⁴. Notons que cette restriction ne résulte pas d'un obstacle juridique ou de la CNIL mais de la volonté de l'exécutif et des services⁵. Si les interconnexions présentent des avantages pour les services, ces derniers restent vigilants dans le partage automatique de leurs données face à un risque de perte de maîtrise de l'information et du secret nécessaire à leur activité. On relèvera enfin une divergence intéressante soulevée par Marc Cottureau entre la CNIL et le Conseil d'Etat sur la finalité de cette interconnexion. Selon l'auteur, pour la CNIL, le fichier ACCReD a une vocation restrictive de rationaliser les enquêtes administratives, alors que pour le Conseil d'Etat, ce dispositif est plus large en ayant pour finalité la sécurité publique et à la sûreté de l'Etat⁶. Dans ce cas, l'interprétation du Conseil d'Etat nous invite à regarder les interconnexions en renseignement comme des instruments surveillance et non comme de simples outils de gestion des données de surveillance.

La mise en relation du FSPRT avec le fichier HOPSYWEB, géré par les agences régionales de santé (ARS), portant sur les personnes ayant subi des soins psychiatriques sans consentement est un autre exemple d'interconnexion dans le

¹ A ce sujet, voir D. Paris et P. Morel-À-L'Huissier, *Rapport d'information sur les fichiers mis à disposition des forces de sécurité*, op. cit., p. 57.

² Délibération n° 2017-152 du 18 mai 2017 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « ACCRED » (demande d'avis n° 17006644).

³ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 213 et 214.

⁴ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 135 et 136.

⁵ Ibid.

⁶ Sur ce point, voir M. Cottureau, *Le « super fichier » des enquêtes administratives passe le contrôle de proportionnalité du Conseil d'Etat*, AJDA 2019, p. 1879.

domaine du renseignement. Créé par un décret de 2018¹, le fichier HOPSYWEB a été interconnecté au FSPRT en 2019 afin d'alerter automatiquement le préfet du département d'hospitalisation lorsqu'une personne est connue des deux fichiers². En cas de correspondance, le préfet peut alors lancer une procédure de levée de doute pour obtenir des informations complémentaires auprès de l'ARS. S'agissant du fonctionnement de l'interconnexion, la CNIL nous précise que : « *un croisement entre les données enregistrées dans les deux traitements est réalisé, a minima toutes les 24 heures. Les traitements FSPRT et HOPSYWEB sont également interrogés, dès lors qu'un nouvel individu est enregistré dans l'un de ces deux traitements* »³. En outre, précisons que le croisement s'effectue à partir du nom, du prénom et de la date de naissance de l'individu. Il convient de préciser que cette interconnexion ne permettait pas initialement aux services de renseignement d'accéder à ce croisement de données, notamment en raison de la protection du secret médical qui s'applique au fichier HOPSYWEB. Une intervention du législateur était donc nécessaire. La loi du 30 juillet 2021 relative à la prévention des actes de terrorisme et au renseignement a finalement introduit une dérogation au secret médical pour que les services de renseignement puissent être autorisés à accéder au croisement des données du FSPRT et HOPSYWEB⁴. Au regard de la position du Conseil d'Etat, l'ouverture de cette interconnexion aux services de renseignement apparaît légitime. En effet, la haute juridiction administrative a jugé en mars 2020 que l'interconnexion est soumise au régime juridique des fichiers de souveraineté car elle constitue un traitement autonome ayant pour finalité la prévention des actes terroristes de personnes radicalisées présentant des troubles psychiatriques⁵. Cependant, la solution retenue par le Conseil d'Etat n'était pas la même que la CNIL

¹ Décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement.

² Décret n° 2019-412 du 6 mai 2019 modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement.

³ Délibération n° 2018-354 du 13 décembre 2018 portant avis sur un projet de décret modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement (demande d'avis n° 18020552).

⁴ A ce sujet, voir F. Dumas et F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 36.

⁵ Conseil d'Etat, 27 mars 2020, *Cercle de réflexion et de proposition d'actions sur la psychiatrie et autres* (requête n° 431350).

qui considérerait que l'interconnexion litigieuse était un prolongement du fichier HOPSYWEB, en ce sens que la prévention du terrorisme constituait qu'une finalité secondaire¹. Par conséquent, la responsabilité de l'interconnexion aurait incombé à l'ARS en emportant l'application du RGPD. Pour notre part, la position du Conseil d'Etat nous semble plus simple et cohérente au regard de la finalité de l'interconnexion par rapport aux deux fichiers mis en relation. En effet, si la finalité d'HOPSYWEB est le suivi des personnes faisant l'objet de soins psychiatriques sans consentement afin d'homogénéiser et de sécuriser les pratiques d'hospitalisation, il reste que la prévention du terrorisme visée par l'interconnexion dépasse largement le cadre hospitalier puisque le FSPRT s'inscrit dans un dispositif de coopération nationale centralisé de signalement des individus radicalisés. D'ailleurs, l'interprétation du Conseil d'Etat nous invite à considérer l'interconnexion comme un outil de surveillance, d'autant plus qu'elle est reliée aux services de renseignement depuis la loi relative au renseignement de 2021. Il était alors également plus simple d'autonomiser juridiquement l'interconnexion afin d'éviter de faire basculer le fichier HOPSYWEB lui-même dans la catégorie des fichiers de lutte anti-terroriste et de renseignement. Simple en apparence, la solution dégagée par le Conseil d'Etat a pu cependant soulever des interrogations sur les conséquences de l'autonomisation de l'interconnexion : *« Est-elle applicable à toutes les interconnexions, aux seules interconnexions poursuivant des finalités différentes... ? Si un nouveau traitement est créé, toutes les obligations liées à ce nouveau traitement pèsent sur le responsable de traitement dont il faut au préalable déterminer l'identité. Ainsi, en cas d'interconnexion entre deux traitements ayant des responsables de traitement différents, qui doit être identifié comme le responsable de traitement ? »*². Par ailleurs, cette interconnexion validée par le Conseil d'Etat a suscité des interrogations sur la pertinence de mettre en relation un fichier de renseignement avec un fichier de suivi hospitalier et des craintes d'une évolution des interconnexions de surveillance bénéficiant du régime des

¹ Délibération n° 2018-354 du 13 décembre 2018 portant avis sur un projet de décret modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement (demande d'avis n° 18020552).

² A ce sujet, voir A. Debet, *Croisement d'Hopsyweb et du FSPRT : l'interconnexion réalisée entre les deux traitements est un traitement intéressant la sûreté de l'Etat*, Communication Commerce électronique n° 6, Juin 2020, comm. 51.

fichiers de souveraineté étendue à d'autres fichiers relatifs à la situation économique et sociale des individus au nom de la prévention du terrorisme¹. Au regard de la décision du Conseil d'Etat, il est vrai qu'une telle évolution ne semble pas être impossible juridiquement et qu'une prolifération des interconnexions des fichiers de renseignement en dehors de la communauté du renseignement marquerait politiquement un tournant vers une société de surveillance.

Cette dernière situation n'est toutefois pas encore envisagée dans l'élaboration d'un cadre juridique relatif aux interconnexions en renseignement. Les préconisations portent exclusivement sur des interconnexions entre les fichiers de renseignement. Le « rapport Larrivé » de 2020 développe ainsi plusieurs évolutions juridiques qui peuvent être confrontées aux deux exemples exposés précédemment.

Premièrement, le rapport envisage la possibilité de modifier les textes réglementaires régissant les fichiers de renseignement afin de prévoir, au cas par cas, leurs interconnexions sans qu'une autorisation de la CNIL soit nécessaire. Peu sophistiquée, cette solution semble la plus respectueuse pour la protection des données et le contrôle des services sur le partage de leurs informations.

Deuxièmement, une seconde possibilité consiste à créer des interfaces « hit/no hit » « permettant la consultation automatique et simultanée de plusieurs fichiers de renseignement aux seules fins de vérifier si l'identité de la personne concernée y est enregistrée »². Circonscrites dans un périmètre restreint répondant aux principes de finalité, de nécessité et de proportionnalité, ces interfaces visant à faire du « criblage » seraient donc prévues par un texte réglementaire spécifique. Un système d'alerte pourrait même être envisagé pour automatiser la détection des croisements de données entre les fichiers de renseignement interconnectés via l'interface. Ce cas de figure renvoie aux exemples des fichiers ACCReD et des fichiers FSPRT et HOPSYWEB. D'une part, ce type d'interfaces constituerait un instrument de surveillance autonome selon la jurisprudence du Conseil d'Etat mais qui pourrait être « dégradé », c'est-à-dire que

¹ Sur ce point, voir L. Carayon, « *Quelle folie !* », La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés, mis en ligne le 11 juin 2020.

² Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 135.

les services pourraient ne pas consentir à donner un accès automatique à leurs données en plus d'une délimitation juridique sur les données pouvant faire l'objet d'un croisement. D'autre part, la création d'interfaces pose la question de savoir quel service serait responsable du nouveau traitement ou si la création d'un nouveau service serait nécessaire. Il nous apparaît ainsi plus judicieux d'organiser préalablement la coopération entre les services pour faire correspondre la consécration juridique de ce type d'interfaces avec la réalité des relations au sein de la communauté du renseignement. Par ailleurs, le « rapport Larrivé » recommande qu'aucune « décision juridique ou affectant sensiblement les personnes ne doit être exclusivement fondée sur un tel dispositif »¹. Cette garantie nous invite à penser que ces interconnexions ne pourraient pas justifier à elles seules le déclenchement d'une technique de renseignement comme par exemple des interceptions de sécurité.

Troisièmement, le « rapport Larrivé » émet la possibilité d'encadrer des interconnexions permettant un partage automatisé d'informations allant au-delà des fonctions de criblage comme par exemple la possibilité d'échanger sur l'ensemble des données relatives à un individu surveillé. Dans ce cas, il est notamment convenu que de telles interconnexions devraient être ponctuelles. A la différence des interfaces précédentes, ce type d'interconnexions pourraient être remis en cause par la CNIL et les services eux-mêmes en raison des nombreuses données pouvant être partagées et des risques de divulgation des sources des services, sans oublier la règle du « tiers service » interdisant le partage de données classifiées reçues par un autre Etat sans son accord².

Enfin, soulignons qu'une interconnexion généralisée de tous les fichiers de renseignement est exclue même s'il est proposé de modifier, le cas échéant, la partie législative du code de la sécurité intérieure relative au renseignement pour préciser que les services peuvent recourir aux interconnexions pour les besoins de leurs missions et conforter ainsi l'assise juridique de ce dispositif, notamment

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 135.

² En ce sens, voir B. Warusfel, *Contraintes juridiques et culture du secret, comme freins à l'échange de données de sécurité en Europe*, Intervention au colloque sur l'échange de données dans l'espace de liberté, de sécurité et de justice de l'Union européenne (CESICE, Université Grenoble-Alpes, 18 novembre 2016).

dans le cas où la troisième solution serait retenue¹. Une modification législative dans le droit du renseignement a également été envisagée par Floran Vadillo. Ce dernier expose deux solutions permettant d'encadrer les interconnexions des fichiers dans le but d'« *offrir à des dispositifs d'IA un terrain d'action plus conséquent qu'aujourd'hui, au profit des missions des services de renseignement et dans le respect des droits fondamentaux* »². Une première solution consisterait à créer des interfaces thématiques relatives à la lutte anti-terroriste ou à la contre-ingérence par exemple dans la même idée que les interfaces « *hit/no hit* » avec une automatisation des accès aux données croisées selon une procédure similaire à celle de l'article L. 851-3 du code de la sécurité intérieure avec l'intervention de la CNCTR. Une seconde solution serait de qualifier l'interconnexion de technique de recueil du renseignement soumise à autorisation du Premier ministre après avis de la CNCTR pour des besoins ponctuels dans la surveillance d'un individu. Ces évolutions semblent s'inscrire dans la continuité de la troisième possibilité envisagée par le « rapport Larrivé » et devraient donc rencontrer les mêmes difficultés.

Relevons enfin que ces évolutions tendent à un bouleversement du droit des interconnexions en opérant un basculement de la loi informatique et libertés vers la loi relative au renseignement. Ce basculement trouverait son origine dans l'interprétation selon laquelle les interconnexions constitueraient une technique de surveillance des individus et non un simple outil de rationalisation du renseignement. Dans ce sens, il nous apparaît cohérent d'introduire les interconnexions dans le droit du renseignement. Cependant, ces évolutions législatives posent nécessairement la question d'une extension du rôle de la CNCTR dans le contrôle des fichiers de renseignement³.

L'encadrement du partage des données en renseignement se traduirait par une absorption des notions du droit de la protection des données par le droit du renseignement. Dans le cas des interconnexions, l'absorption pourrait avoir pour effet une requalification de la notion en technique de recueil du renseignement.

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 187.

² Cf. F. Vadillo, *Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?*, op. cit..

³ Cf. infra. §2 de la Section II du Chapitre II du Titre II de la Ier Partie.

Enfin, le droit du renseignement a développé sa propre notion de partage d'informations en dehors de celles développées par le droit de la protection des données.

§4. Le partage d'informations

En dehors du cadre de la mutualisation des fichiers, les lois relatives au renseignement prévoient des mécanismes de transmissions de renseignements entre les services et avec d'autres administrations. Dans le prolongement de ces mécanismes, il convient de s'intéresser à deux autres types de partage d'informations : la transmission d'informations par l'autorité judiciaire et le partage international de données de renseignement.

A - Les transmissions inter-services et avec d'autres administrations

La loi relative au renseignement de 2015 avait créé un nouvel article L. 863-2 dans le code de la sécurité intérieure qui consacrait la possibilité pour les services de renseignement de partager « *toutes les informations utiles à l'accomplissement de leurs missions* » ainsi qu'une habilitation pour les autorités administratives à transmettre de leur propre initiative ou sur demande des services des informations utiles à l'accomplissement des missions de ces derniers¹. Les administrations concernées sont les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural et les autres organismes chargés de la gestion d'un service public administratif ainsi que les commissions de coordination des actions de prévention des expulsions locatives. Les modalités de ces partages d'informations devaient être précisées par un décret en Conseil d'Etat qui n'a finalement jamais été pris. Pour autant, « *une procédure dite d'extension* » a été mise en place pour que des partages d'extractions et transcriptions de renseignements collectés puissent s'opérer au sein du GIC sous le contrôle de la CNCTR et dans le respect du principe de finalité². Cette procédure ne concernait que les transcriptions centralisées par

¹ A ce sujet, voir R. Gauvain et L. Kervran, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, op. cit., p. 65 et 66.

² Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 85 et 86.

le GIC relatives aux interceptions de sécurité, aux exploitations de la surveillance internationale et aux captations de paroles. Dans ces considérations, la DPR et le « rapport Larrivé » ont dénoncé la faiblesse du dispositif juridique et recommandé de le modifier¹, d'autant plus que les dispositions de l'article L. 863-2 du code de la sécurité intérieure ont été contestée et censurées.

Soutenant, sur la base d'un article publié dans le Monde en avril 2019², que l'exécutif avait décidé d'autoriser la mise en œuvre de traitements de données en application l'article L. 863-2, l'association La Quadrature du Net a introduit un recours pour excès de pouvoir contre cette décision devant le Conseil d'Etat, ce qui a abouti à une QPC sur les dispositions législatives en question³. Procédant à l'examen de l'article L. 863-2, le Conseil constitutionnel a validé le partage d'informations entre services de renseignement mais jugé que la transmission de renseignements par les autorités administratives méconnaissait le droit au respect à la vie privée⁴. En effet, les informations concernées pouvaient porter sur toutes les catégories de données personnelles, notamment les données sensibles, sans qu'aucune garantie procédurale ou de contrôle ne soit prévue. Par cette décision, le Conseil constitutionnel rappelle que le droit du renseignement ne peut pas faire l'économie de la problématique de la protection des données lorsqu'il encadre des échanges d'informations. En l'espèce, la mise en œuvre de l'articulation entre le droit de la protection des données et l'article L. 863-2 doit être déterminée par la loi même s'il est prévu que des actes réglementaires préciseront le dispositif⁵. Tirant les conséquences de la censure du Conseil constitutionnel, le législateur a revu l'ensemble du dispositif des transmissions de renseignements dans la loi relative au renseignement du 30 juillet 2021.

D'abord, il a été décidé d'introduire un mécanisme de partage d'informations inter-services à l'article L. 822-3 du code de la sécurité intérieure. De manière générale, les services de renseignement peuvent s'échanger librement

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 179 et 180.

² Cf. J. Follorou, « L'entrepôt », *bâtiment ultrasécurisé et outil essentiel du renseignement français*, Le Monde, 24 avril 2019.

³ Conseil d'Etat, 19 mai 2021, *La Quadrature du Net* (requête n° 431980).

⁴ Décision n° 2021-924 QPC du 9 juillet 2021, *La Quadrature du Net*.

⁵ Conseil d'Etat, 18 novembre 2021, *La Quadrature du Net* (requête n° 431980).

des renseignements dans la limite des compétences du service destinataire et des finalités de l'article L. 811-3 du code de la sécurité intérieure. En revanche, une autorisation du Premier ministre après avis de la CNCTR est nécessaire si les transmissions concernent : d'une part, des renseignements collectés dont la finalité du recueil est différente de celle justifiant la transmission et, d'autre part, des renseignements collectés, extraits ou transcrits provenant d'une technique de renseignement non autorisée pour le service destinataire dans le cadre de la finalité motivant la transmission. Le dispositif général des transmissions a pu soulever la question de savoir à qui revient le rôle de juger de la nécessité des transmissions et sur quels critères¹. Il ressort de l'interprétation de la CNIL que le contrôle doit être assuré *a posteriori* par la CNCTR qui doit s'assurer de la compétence du service destinataire et, conformément à la loi informatique et libertés, à ce que les données personnelles soient « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* »². On relèvera que cette interprétation rejoint celle retenue par le Conseil constitutionnel dans sa décision QPC relative à l'article L. 863-2³.

Ensuite, la loi du 30 juillet 2021 est venue modifier l'article L. 863-2 afin de préciser le cadre des transmissions d'informations opérées par les autorités administratives à la demande des services. Désormais, les autorités administratives peuvent communiquer toute information, y compris celle couverte par un secret protégé par la loi, aux services de renseignement pour l'accomplissement des missions de ces deniers et pour concourir à la défense et la promotion des intérêts fondamentaux de la Nation mentionnées à l'article L. 811-3 du code de la sécurité intérieure. Afin de répondre aux exigences du juge constitutionnel, le texte a pris soin de préciser que ces transmissions peuvent porter sur des données personnelles sensibles tout en excluant les données génétiques. Plus encore, le législateur de 2021 s'est montré cohérent en organisant

¹ En ce sens, voir F. Safi, *La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Entre pérennisation et extension de l'exception...*, La Semaine Juridique Edition Générale n° 40, 4 octobre 2021, 1012.

² 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.

³ En ce sens, voir E. Maupin, *Censure partielle de l'article L. 863-2 du code de la sécurité intérieure*, AJDA 2021, p. 1470.

la traçabilité des transmissions des données par les différents responsables de traitements et en excluant ces transmissions du droit d'information des personnes concernées¹. On soulignera que le Conseil d'Etat a confirmé la proportionnalité du dispositif au regard du droit au respect à la vie privée dans une décision de 2022 relative aux transmissions de données médicales concernant un patient hospitalisé ou l'ayant été².

Si la CNIL avait accueilli « *favorablement le resserrement des conditions posées par la loi* »³, relevons que la loi du 30 juillet 2021 a procédé à un élargissement des informations pouvant être communiquées aux services de renseignement, notamment en autorisant la transmission d'informations couvertes par un secret protégé par la loi⁴. Le nouveau dispositif de partage des renseignements a pu susciter la crainte d'une surveillance sans limite justifiée de manière insatisfaisante par la défense et la promotion des intérêts fondamentaux de la Nation, notamment lorsque ce dispositif est cumulé avec d'autres mécanismes de partage d'informations qui s'étendent par exemple à l'autorité judiciaire⁵.

B - La transmission d'informations par l'autorité judiciaire

La loi relative au renseignement de 2021 a introduit au code de procédure pénale un mécanisme de partage d'informations autorisant le procureur de la République de Paris ou le juge d'instruction compétent à transmettre, par dérogation au secret de l'enquête, aux services de renseignement des éléments relatifs à des enquêtes judiciaires en matière de cybercriminalité⁶ et de criminalité

¹ Conseil d'Etat, 21 avril 2021, *Avis sur un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement* (n° 402562).

² Conseil d'Etat, 23 novembre 2022, *Conseil national de l'ordre des médecins* (n° 464480).

³ 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.

⁴ En ce sens, voir P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement. Commentaire de la loi n° 2021-998 du 30 juillet 2021*, op. cit..

⁵ En ce sens, voir F. Safi, *La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Entre pérennisation et extension de l'exception...*, op. cit..

⁶ La transmission d'informations concerne uniquement la DGSE et la DGSI qui sont les services de renseignement compétents en matière de cyberdéfense au sens de l'article L. 2321-2 du code de la défense (Arrêté du 17 juillet 2015 déterminant les services de l'Etat mentionnés au second alinéa de l'article L. 2321-2 du code de la défense).

organisée (nouvel article 706-105-1)¹. Soulignons que ce mécanisme n'est pas nouveau puisqu'il avait déjà été mis en place par la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique en matière d'infractions terroristes². Si les particularités de la prévention du terrorisme pouvaient naturellement conduire en 2017 à rapprocher les investigations judiciaires de la surveillance en renseignement³, il avait pu être soutenu que ce rapprochement constitue une confusion des moyens de police judiciaire et de police administrative⁴. Un même constat a été partagé à propos de la loi du 30 juillet 2021 allant jusqu'à dénoncer une remise en cause de l'indépendance du juge judiciaire et la défiguration du système pénal⁵. Pour notre part, il convient d'adopter une approche plus mesurée selon laquelle la transmission d'informations de l'autorité judiciaire vers le renseignement devrait s'interpréter comme un simple rapprochement entre les deux polices. En revanche, l'inverse qui correspond à la judiciarisation du renseignement peut entraîner une confusion des polices dans le cas où, au nom de la « primauté » de l'autorité judiciaire⁶, les moyens de renseignement sont utilisés à des fins répressives dans un système où la police administrative est sollicitée par la police judiciaire. Les modifications du code de procédure pénale ne nous semblent pas adopter un tel système. Cependant, relevons que les textes précisent que la transmission d'informations peut être exercée à l'initiative de l'autorité judiciaire. Il ne faudrait pas que cette initiative aboutisse à une pratique qui consisterait pour l'autorité judiciaire à inciter les services de renseignement à judiciariser systématiquement les renseignements collectés. On assisterait alors à la confusion des polices tant redoutée. Le législateur aurait pu s'abstenir de prévoir une telle possibilité pour l'autorité judiciaire au nom d'un principe de judiciarisation « incidente » du renseignement. Quoi qu'il en soit, l'extension par la

¹ A ce sujet, voir P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement. Commentaire de la loi n° 2021-998 du 30 juillet 2021*, op. cit..

² Article 706-25-2 du code de procédure pénale.

³ Sur ce point, voir B. Warusfel, *Justice et renseignement dans la lutte contre la radicalisation violente*, op. cit..

⁴ En ce sens, voir T. Herran, *L'impact de la loi relative à la sécurité publique sur la distinction entre la police judiciaire et la police administrative*, AJ Pénal 2017, p. 472.

⁵ En ce sens, voir F. Safi, *La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Entre pérennisation et extension de l'exception...*, op. cit..

⁶ Cf. supra. *Les accès aux fichiers et le rapprochement d'informations*.

loi du 30 juillet 2021 de la coopération entre le renseignement et la police judiciaire nous invite à rester vigilant sur les risques d'une judiciarisation systématique du renseignement.

Enfin et plus problématique pour la numérisation du renseignement, le mécanisme de partage d'informations avec l'autorité judiciaire ne précise pas les données personnelles pouvant faire l'objet d'une transmission. Rappelons que la CNIL s'était inquiétée du périmètre du partage des données autorisé par la loi du 30 juillet 2021 au regard des nombreuses infractions visée par le texte et n'avait pas été entièrement convaincue par le caractère facultatif des transmissions comme garantie suffisante¹. Il nous apparaît curieux que le législateur de 2021 n'ait pas pensé à rendre cohérent le dispositif avec le droit de la protection des données personnelles comme il a pu le faire pour les articles L. 822-3 et L. 863-2 du code de la sécurité intérieure. D'autant plus que les transmissions portent sur « *des éléments de toutes nature* » qui figurent dans les procédures pénales concernées. Il aurait pu être notamment précisé que ce partage d'informations ne porte pas sur des données génétiques prélevées dans le cadre des enquêtes judiciaires par exemple. Il serait peut-être opportun de s'attarder à mettre le dispositif en accord avec la loi informatique et libertés par souci de cohérence avec la jurisprudence du Conseil constitutionnel.

En revanche, le législateur n'a pas manqué d'interdire tout échange avec des services de renseignement étrangers ou avec des organismes internationaux de renseignement sur les informations communiquées par l'autorité judiciaire. On retrouve ici l'esprit de la règle dite du « tiers service » qui limite le partage international des données de renseignement.

¹ Délibération n° 2021-045 du 15 avril 2021 portant avis sur les articles 13 bis et 13 ter du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

C - Le partage international des données de renseignement

Les données collectées par les services de renseignement n'échappent pas à la tendance croissante de la circulation des données relatives à la sécurité nationale entre Etats partenaires, dans un contexte bilatéral ou multilatéral¹. On assiste à « *la création d'un réseau interconnecté d'arrangements formels et informels de liaison de renseignement à travers le monde* »² qui devrait être facilitée et renforcée par la numérisation des services de renseignement. Cependant, la circulation internationale des données a échappé aux évolutions du droit du renseignement en France mais fait l'objet de réflexions institutionnelles et doctrinales. En effet, d'un point de vue purement juridique et non factuel ou politique, les échanges internationaux de données de renseignement ne sont pas sans soulever la question d'un risque de violation des lois relatives au renseignement ou à la protection des données et, par là même, des droits fondamentaux. Plus précisément, la CNCTR a relevé deux difficultés à envisager pour la France : d'une part, les données communiquées aux services français (« flux entrants ») peuvent entrer dans le champ d'application du droit du renseignement mais ne peuvent pas faire l'objet d'un contrôle par la CNCTR en application de l'article L. 833-2 du code de la sécurité intérieure³ et, d'autre part, la transmission de données issues des techniques de recueil de renseignement à des services étrangers (« flux sortants ») pourrait avoir pour conséquence de soustraire ces données à l'application de loi française en l'absence de textes régissant ce type de situation (outrepasser la durée légale de conservation des renseignements collectés par exemple)⁴. On relèvera que « *le risque d'un contournement des dispositions nationales de contrôle des services* » a été une

¹ A ce sujet, voir C. Chevallier-Gevers, *L'échange de données dans l'Espace de liberté, de sécurité et de justice de l'Union européenne*, Mare & Martin, 2017 et dans ce même volume, B. Warusfel, *Contraintes juridiques et culture du secret, comme freins à l'échange de données de sécurité en Europe*, p. 425 à 442.

² En ce sens, voir Svendsen A. D. M., *The globalization of intelligence since 9/11 : Frameworks and operational parameters*, Cambridge Review of International Affairs, mars 2008.

³ L'article L. 833-2 exclut la communication à la CNCTR « *des éléments communiqués par des services étrangers ou par des organismes internationaux* ».

⁴ Cf. CNCTR, 3^{ème} rapport annuel 2018, p. 50 et suivantes.

problématique également soulevée dans la doctrine britannique à propos des échanges entre la NSA et GCHQ¹.

En droit, les difficultés françaises tiennent principalement à une interprétation restrictive de la règle du « tiers service » (« *originator control* » en anglais) qui constitue la base juridique du partage international des données de renseignement. D'origine coutumière, cette règle « *interdit de transmettre à une tierce partie sans autorisation de l'émetteur un renseignement reçu d'un partenaire* »². Elle est généralement formalisée par la France dans des accords internationaux de sécurité qui stipulent par exemple que « *les informations classifiées de l'une des deux Parties ne peuvent être communiquées par l'autre à un Etat tiers ou à une organisation internationale sans l'autorisation écrite préalable de la Partie d'origine* »³. De même, elle a pu être transposée en droit interne au cas particulier des échanges entre Tracfin et ses homologues étrangers selon la formulation suivante : « *ce service ne peut transmettre à une autre autorité compétente les informations qui lui ont été ainsi communiquées par une cellule de renseignement financier homologue qu'après autorisation préalable de cette dernière* »⁴.

Selon ces différents énoncés, la règle du « tiers service » n'interdit donc pas formellement à l'Etat de prévoir un régime juridique d'encadrement et de contrôle des échanges internationaux. Pour autant, elle a été transposée dans le droit du renseignement français sous la forme d'une exclusion de la compétence de la CNCTR et de la DPR pour contrôler les échanges de données⁵. Selon les services de renseignement et le « rapport Larrivé », plusieurs arguments justifieraient cette interprétation restrictive : d'une part, les échanges relèvent « *de la souveraineté de l'Etat et de son action diplomatique* »⁶ et, d'autre part, l'établissement d'un contrôle

¹ Sur ce point, voir J. -C. Cousseran et P. Hayez, *Leçon sur le Renseignement*, op. cit., p. 160.

² Ibid., p. 162.

³ Article 5.6 de l'accord entre le Gouvernement de la République française et le Gouvernement de la République fédérale d'Allemagne sur la protection réciproque des informations classifiées, signé à Berlin le 15 mars 2005 (décret n° 2006-327 du 15 mars 2006 portant publication de l'accord).

⁴ Article L. 561-29 du code monétaire et financier.

⁵ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 171 et 172.

⁶ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 92.

présente un risque d'arrêt des partenariats mais aussi d'un « *glissement du contrôle des techniques de renseignement vers le contrôle de la production des services de renseignement* »¹. Guidée par les « *enjeux diplomatiques en cause* » et les « *impératifs opérationnels* », la DPR a rejoint la conclusion du « rapport Larrivé » selon laquelle « *il serait peu opportun* » de légiférer davantage sur le partage international des données de renseignement². Cette position de la DPR nous semble paradoxale avec sa recommandation sur la nécessité d'« *engager une réflexion sur le statut des renseignements techniques recueillis ou exploités grâce à l'assistance d'un service de renseignement étranger et sur le niveau de protection qui les entoure* ». La délégation n'a pas manqué de révéler qu'une surveillance des citoyens français ou d'individus résidant en France pouvait être opérée par un service étranger à la demande des services français, « *faute de capacités techniques suffisantes* »³. En outre, on relèvera que l'exécutif envisage « *de donner un cadre réglementaire plus formalisé à ces échanges* », notamment pour faire valider systématiquement les accords au niveau politique et fixer une « *protocolisation de la liaison* » qui par exemple ne pourrait être engagée que si le recours à un service étranger dans la collecte des renseignements est conforme aux principes démocratiques⁴.

Force est d'admettre que le partage international des données de renseignement n'est pas qu'une question de souveraineté et de diplomatie, elle est indubitablement une question de respect des droits fondamentaux dans nos démocraties libérales. Dans cet optique, on ne peut que souscrire à une évolution du droit du renseignement français au regard des exemples étrangers et de la jurisprudence de la CEDH qui nous apparaissent pertinents bien que les régimes juridiques de renseignement soient très hétérogènes. Ainsi, la CNCTR n'a pas manqué de souligner que certains Etats européens ont légiféré sur les échanges internationaux, notamment le Royaume-Uni qui n'autorise l'exploitation des « flux entrants » que sur le fondement d'une autorisation en droit interne et qui soumet

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 171 et 172.

² Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 93.

³ Ibid., p. 93 et 94.

⁴ Ibid., p. 92 et 93.

les accords d'échanges de données au contrôle d'une autorité indépendante, l'Investigatory Powers Commissioner's Office¹. Dans le cas britannique, il semblerait que l'autorité indépendante n'exerce pas un contrôle direct sur les données partagées mais sur les modalités définies dans les accords internationaux, ce qui consisterait notamment à s'assurer que les parties prenantes veillent au respect des droits fondamentaux et à la protection des données personnelles². Le modèle britannique a fait l'objet d'un contrôle par la CEDH dont la jurisprudence devrait être prise en compte par le législateur français. Dans un arrêt *Big Brother Watch c/ Royaume-Uni* de 2018 dont la solution a été confirmée définitivement en 2021, la Cour de Strasbourg a validé le dispositif britannique tout en jugeant, de manière générale, que le droit interne doit prévoir « *les circonstances dans lesquelles il est possible de demander des éléments interceptés ; la procédure à suivre pour l'examen, l'utilisation et la conservation des éléments obtenus ; les précautions à prendre pour la communication de ces éléments à d'autres parties ; et les circonstances dans lesquelles ces éléments doivent être effacés* »³. Comme le souligne la DPR, l'absence d'encadrement légal en France « *pourrait soulever des difficultés de conformité avec la convention européenne de sauvegarde des droits de l'homme* »⁴. Aujourd'hui, il n'est donc plus question de savoir si le partage international de données peut échapper à un encadrement légal, il s'agit désormais de trouver un dispositif qui répondrait aux exigences de la CEDH sans remettre fondamentalement en cause notre droit du renseignement.

En dehors de la proposition de l'exécutif concernant les accords internationaux, la doctrine propose des solutions. Selon Floran Vadillo, il pourrait être envisagé de confier à l'inspection des services de renseignement « *une mission permanente de contrôle de la règle du tiers service et, après avoir fixé des orientations, lui demander de s'assurer de la conformité de actions conduites avec*

¹ Cf. CNCTR, 3^{ème} rapport annuel 2018, p. 50 et suivantes.

² En ce sens, voir le lien internet <https://www.gov.uk/government/news/investigatory-powers-commissioner-to-oversee-uk-us-data-access-agreement>.

³ CEDH, 13 septembre 2018 et 25 mai 2021, *Big Brother Watch et autres contre Royaume-Uni* (n° 58170/13).

⁴ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 92.

celles-ci »¹. Cette proposition n'a pas emporté l'adhésion du Professeur Bertrand Warusfel en ce qu'elle diluerait davantage les compétences de contrôle du renseignement. Dans le cadre d'une solution transitoire, Bertrand Warusfel envisage, quant à lui, un dispositif qui consisterait à ce que la CNCTR soit notifiée des échanges afin de saisir, si possible, son homologue étranger pour que ce dernier puisse exercer un contrôle de la collecte et de l'exploitation des données sur la base de sa législation². Pour notre part, il pourrait être envisagé, dans la continuité des efforts de l'exécutif, de reconnaître légalement un droit de partage des données de renseignement aux services, c'est-à-dire de pouvoir stipuler des accords avec leurs homologues étrangers avec l'autorisation du pouvoir politique. Il s'agirait d'ailleurs de mettre en cohérence l'affirmation légale de la compétence exclusive de l'Etat en matière de politique publique du renseignement³ avec la possibilité des services français de recourir à des services étrangers pour opérer des missions de souveraineté comme la surveillance d'un citoyen français ou d'un individu résidant sur le territoire national. En outre, la loi exigerait que ces accords prévoient les garanties posées par la jurisprudence de la CEDH et que la CNCTR seraient saisie pour avis afin de contrôler la bonne prise en compte de ces garanties qui concernent notamment la protection des données personnelles. S'agissant de la règle du « tiers service », la loi pourrait disposer qu'elle peut être librement stipulée dans ses modalités par les parties prenantes et ainsi consacrer la possibilité de déroger à l'article L. 833-2 du code de la sécurité intérieure. Néanmoins, cette solution, qui pourrait trouver à s'appliquer uniquement sur les données partagées, inviterait nécessairement à devoir étendre les compétences de la CNCTR à la production des services de renseignement.

Quoi qu'il en soit, il est vrai qu'aucun Etat ne peut imposer unilatéralement un contrôle des données partagées sans compromettre la règle du « tiers service » et, par conséquent, les relations diplomatiques. En revanche, aucune règle ne doit avoir pour effet d'interdire, de manière générale et absolue, tout contrôle de ces échanges. Au moins, le droit interne devrait s'attacher à clarifier le cadre des

¹ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit., p. 42.

² Cf. B. Warusfel, *Quelques réformes pour le droit du renseignement ?*, Annuaire 2021 du droit de la sécurité et de la défense, Mare & Martin, 2021.

³ Article L. 811-1 du code de la sécurité intérieure.

relations diplomatiques, notamment en les inscrivant dans le respect des valeurs démocratiques et des droits fondamentaux. Au plus, les Etats devraient chercher à assortir systématiquement leurs échanges de données d'un contrôle. Au niveau européen, l'élaboration d'un cadre multilatéral de coopération en matière de contrôle du renseignement est d'ailleurs en question avec les efforts de l'IOWG (Intelligence Oversight Working Group) qui cherche à rapprocher les organes de contrôle du renseignement de la Belgique, du Danemark, des Pays-Bas, de la Norvège, de la Suisse et du Royaume-Uni¹. Relevons que ce rapprochement multilatéral en matière de renseignement n'est pas nouveau puisqu'il avait déjà été proposé d'adopter un « code du renseignement » à l'échelle européen² et que des échanges multilatéraux de renseignements ont pu trouver un cadre formalisé avec le développement de l'Intcen, la cellule de renseignement de l'Union européenne dans le domaine de la PESC³. La coopération internationale tend donc à s'affirmer publiquement malgré une réticence des services à encadrer leurs relations. Dans ce contexte, il nous apparaît alors opportun que la France se dote d'un cadre légal clair sur le partage international des données de renseignement.

Enfin, lorsque l'on additionne ces échanges internationaux avec les partages d'informations autorisés par le droit du renseignement ainsi que les interconnexions et les accès entre les fichiers de renseignement ou d'autres institutions, on ne peut que souscrire à la remarque du Professeur Xavier Latour selon laquelle « *il va se constituer un vaste réseau de données collectées, circulant entre les services spécialisés, voire au-delà* »⁴. On ajoutera que cette situation va nécessairement avoir pour conséquence d'intensifier les besoins des services en innovations numériques sur les traitements de données.

¹ Pour en savoir plus, voir notamment le rapport annuel 2019 du Comité permanent R belge et le texte « Charter of the Intelligence Oversight Working Group » du 12 décembre 2019.

² A ce sujet, voir le rapport de Pieter Omtzigt sur les opérations massives de surveillance remis l'Assemblée parlementaire du Conseil de l'Europe en janvier 2015.

³ Sur ce point, voir J. -C. Cousseran et P. Hayez, *Leçon sur le Renseignement*, op. cit., p. 169 à 171.

⁴ Cf. X. Latour, *La loi relative au renseignement : un État de surveillance ?*, op. cit..

SECTION II : Les innovations numériques sur les données

Le droit du renseignement est particulièrement amené à s'intéresser à deux innovations technologiques comme le souligne le « rapport Larrivé » de juin 2020¹ : l'utilisation de l'intelligence artificielle (§1) et la technologie biométrique (§2).

§1. L'utilisation de l'intelligence artificielle

Comme le soulève Jérôme Poirot, la question se pose déjà de savoir si les espions seront remplacés par des robots et des algorithmes dans un contexte où l'IA tend à devenir un outil indispensable du renseignement mais dont les développements, notamment avec le « *deep learning* »², suscitent des craintes pour les droits et libertés³. Sur le plan juridique, le droit positif français du renseignement appréhende progressivement la problématique de la régulation de l'IA pour les besoins des services, ce qui nous interroge sur le droit prospectif.

A - Un outil indispensable pour le renseignement qui suscite des craintes

L'IA « offre une multiplicité d'usages possibles » pour le renseignement dans « le traitement de l'image, de la parole, du texte mais aussi d'autres types de données plus hétérogènes »⁴. Le recours croissant aux capteurs numériques entraîne une « augmentation exponentielle des données » à traiter par les services de renseignement, notamment dans les domaines du renseignement spatial, cyber et militaire⁵. Ainsi pour la DRM, l'IA s'impose comme « une réponse technique

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 99 et suivantes.

² Le « *deep learning* » (ou « apprentissage profond » en français) renvoi à des modèles d'algorithmes d'apprentissage de la machine (ou « *machine learning* » en anglais) qui s'inspire du fonctionnement du cerveau humain (cf. E. Sibony, *Qu'est ce que l'intelligence artificielle ? Intelligence artificielle, un nouvel horizon : pourquoi la France a besoin d'une culture numérique ? Comprendre et débattre ses enjeux technologiques, économiques, légaux et éthiques*, Les Cahiers Lysias, juillet 2017, p.18).

³ Cf. J. Poirot, *Intelligence artificielle*, Dictionnaire du renseignement, op. cit., p. 474 à 475.

⁴ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 102 et suivantes.

⁵ A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 221.

indispensable » à la masse de données que le service se doit d'analyser¹. Il s'agit là de l'enjeu principal de l'IA en renseignement, c'est-à-dire de donner la capacité aux services de mettre en œuvre des algorithmes suffisamment entraînés pour qu'ils puissent traiter une masse de données impossibles à analyser pour un agent humain. Selon le « rapport Larrivé », l'IA aurait donc vocation à mieux discerner les données captées et ne constitue pas un nouvel outil de surveillance ou un moyen de renforcer l'intrusion des services dans la vie privée des individus². On peut toutefois relativiser cette affirmation puisque le recours à des algorithmes d'IA de détection des menaces sur les réseaux numériques, comme par exemple les « boîtes noires » autorisées et renforcées par les lois relatives au renseignement de 2015 et 2021³, ont pour objet de surveiller les données d'intérêts des individus connectés, d'alerter en cas de menace et de permettre la collecte d'informations sur la personne concernée. La possibilité de discerner les données n'est pas incompatible avec la possibilité d'opérer simultanément une surveillance.

Les intérêts pour l'IA s'accompagnent de craintes sur la pertinence de son utilisation en matière de renseignement et d'analyse prédictive. Dans son étude sur les algorithmes et l'IA de 2017, la CNIL a pu relever que les experts se montrent prudent en soulignant un risque de démultiplication de la suspicion ayant pour conséquence « *une masse de cibles impossibles à traiter* » pour les services de renseignement⁴. Par ailleurs, l'IA nécessite un très grand nombre de données pour être performant et donc de données personnelles en matière de renseignement, ce qui présente des risques pour la protection de ces données et les droits et libertés des individus. En effet, les algorithmes d'IA sont modélisés en deux temps⁵ :

- une phase d'apprentissage à partir des données collectées afin de permettre à la machine de distinguer « une situation représentant une

¹ Cf. DRM, *Intelligence artificielle et renseignement militaire*, Revue Défense Nationale, 2019/5 (N° 820), p. 107 à 116.

² Cf. G. Larrivé, Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement, op. cit., p. 103.

³ Cf. supra. Chapitre I : La recherche numérique des renseignements.

⁴ Cf. CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Décembre 2017, p. 67 et 68.

⁵ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 103 suivantes.

menace et une situation on porteuse de menace ». Cette phase implique de traiter des données relatives aux deux types de situations, c'est-à-dire des données déjà enregistrées dans les fichiers des services et d'autres données n'ayant aucun rapport avec la menace envisagée ;

- une phase opérationnelle permettant d'utiliser l'algorithme d'IA fonctionnant avec de nouvelles données indépendantes des données d'apprentissage qui sont issues des investigations opérationnelles.

Ces deux phases de modélisation peuvent entraîner des conséquences défavorables pour les données traitées (perte des données ou erreurs sur les données par exemple) et sur les personnes qui sont visées par l'utilisation de l'algorithme d'IA lorsqu'elles représentent une menace pour la machine. Dans la doctrine juridique, les conséquences de l'émergence des algorithmes d'IA dans le champ de la sécurité et de la police administrative restent difficiles à prévoir, ce qui exige de « sérieuses précautions » ou, pour certains auteurs, de ne pas autoriser l'usage de cette technologie¹.

Les intérêts de l'IA et les craintes qu'elles suscitent en matière de renseignement ont poussé les pouvoirs publics à encadrer juridiquement son déploiement et son développement par des mesures spécifiques et de manière progressive.

B - Les mesures adoptées en droit du renseignement

Introduits par la loi relative au renseignement de 2015 à titre expérimental et pérennisés par la seconde loi relative au renseignement du 30 juillet 2021², les traitements algorithmiques de détection des connexion susceptibles de révéler une menace terroriste prévus par l'article L. 851-3 du code de la sécurité intérieure constituent une première mesure de régulation de l'IA par le droit du renseignement. Si cette technique de renseignement relève du contrôle de la CNCTR et s'inscrit davantage dans une démarche de recherche de renseignements, elle est également une technique d'analyse des données comme le rappelle la CNIL³.

¹ En ce sens, voir X. Latour, *Sécurité intérieure : un droit « augmenté » ?*, AJDA 2018, p. 431.

² Cf. supra. Chapitre I : La recherche numérique des renseignements.

³ 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.

Par ailleurs, dans une logique relevant du droit de la protection des données applicable aux fichiers, la CJUE a précisé que les données ne devaient pas justifier à elles seules l'analyse automatisée de détection des activités terroristes par les algorithmes de l'article L. 851-3¹. Ces considérations impliquent qu'il aurait pu être fait le choix d'intégrer cette technique dans le cadre juridique de la loi informatique et liberté et des fichiers de souveraineté. Néanmoins, il est vrai que l'intégration de ce dispositif dans les techniques de renseignement soumises au contrôle de la CNCTR présente une plus grande cohérence juridique puisque, rappelons-le, le droit du renseignement s'assure du respect de la protection des données personnelles en vertu de l'article L. 801-1 tout en préservant le secret des moyens opérationnels des services. Pour autant, l'émergence de l'IA tend à brouiller la frontière établie en 1991 entre les moyens d'interception et les fichiers, les rôles de la CNCTR et de la CNIL mais, plus encore, la distinction entre la phase de collecte et celle d'analyse dans le cycle du renseignement.

Une seconde mesure visant à réguler l'utilisation de l'IA a été envisagée par la loi relative au renseignement du 30 juillet 2021. Elle porte plus spécifiquement sur l'apprentissage machine et un régime dérogatoire de conservation des renseignements collectés. S'inspirant des recommandations du « rapport Larrivé » sur la régulation de la modélisation des algorithmes d'IA, la loi du 30 juillet 2021 a modifié l'article L. 822-2 du code de la sécurité intérieure afin de permettre aux services du premier cercle et au GIC de « *conserver des renseignements collectés au-delà des durées normalement applicables et jusqu'à cinq ans à des fins de recherche et de développement* », c'est-à-dire pour utiliser l'IA dans le but d'améliorer ou de développer de nouvelles capacités techniques de recueil et d'exploitation de données². Les paramètres des programmes de recherche sont soumis à un régime

¹ « En outre, il importe de rappeler que toute analyse automatisée effectuée en fonction de modèles et de critères fondés sur le postulat selon lequel l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, l'état de santé ou la vie sexuelle d'une personne pourraient, par eux-mêmes et indépendamment du comportement individuel de cette personne, être pertinents au regard de la prévention du terrorisme méconnaîtrait les droits garantis aux articles 7 et 8 de la Charte, lus en combinaison avec l'article 21 de celle-ci. Ainsi, les modèles et les critères préétablis aux fins d'une analyse automatisée visant à prévenir des activités de terrorisme présentant une menace grave pour la sécurité nationale ne sauraient être fondés sur ces seules données sensibles [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 165]. » (CJUE, 6 octobre 2020, affaire C-623/17 Privacy International et dans les affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, French Data Network e.a., ainsi que C-520/18 Ordre des barreaux francophones et germanophone e.a.).

² En ce sens, voir Conseil d'Etat, *Avis sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, 21 avril 2021 (n° 402562), p. 8 et suivantes.

d'autorisation du Premier ministre et la mise en œuvre des programmes fait l'objet d'un contrôle de la CNCTR. On soulignera que la loi précise que ce dispositif n'a pas pour objet la surveillance des individus en interdisant de rechercher l'identité d'une personne par son utilisation. Comme pour les algorithmes de détection d'une menace terroriste, le dispositif envisagé constitue un traitement de données personnelles qui aurait pu être soumis aux dispositions de la loi informatique et libertés selon l'avis de la CNIL sur le projet de loi¹. Cette dernière a néanmoins validé le choix du législateur d'avoir introduit l'encadrement de ce type d'IA dans le droit du renseignement dès lors que la loi prévoit un mécanisme d'autorisation spécifique. En outre, elle a tenu à souligner que le régime de réutilisation des données, c'est-à-dire la mise en œuvre d'un nouveau traitement algorithmique, doit être précisé par décret dans le respect des principes de vigilance et de loyauté afin notamment d'éviter « la présence d'éventuels biais »². La légalisation d'une IA dans le domaine de la recherche et développement en matière de renseignement nous invite à penser que de nouveaux algorithmes d'IA autres que ceux de l'article L. 851-3 devraient être légalement autorisés à l'avenir.

Deux remarques peuvent ressortir de ces mesures : d'une part, on peut relever une certaine autonomisation du droit du renseignement en matière de protection des données dans l'encadrement de l'IA ; d'autre part, le droit du renseignement adopte une approche au cas par cas de la régulation de l'IA avec l'élaboration progressive de règles sectorielles portant, pour le moment, sur la détection de menaces terroristes et sur le développement des capacités numériques de renseignement. Ces remarques incitent à nous interroger sur les perspectives d'un cadre juridique cohérent de l'IA en renseignement.

¹ 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.

² Ibid.

C - Les perspectives juridiques de l'intelligence artificielle en renseignement

Le « rapport Villani » sur l'IA de 2018 n'avait pas manqué de souligner que *« les expérimentations et les dérogations aux règles existantes, suivant la logique de bac à sable, doivent être effectuées dans le cadre strictement défini par le droit et sous le contrôle spécifique des commissions habilitées (notamment la commission nationale de contrôle des techniques de renseignement par exemple s'agissant du renseignement) »*¹. Cette préconisation a été suivie par le législateur comme nous l'avons vu dans le cadre des deux mesures évoquées précédemment qui devraient constituer un point de départ à une théorisation du cadre juridique de l'IA en renseignement. De manière générale, ce cadre juridique devrait uniquement avoir pour socle le droit du renseignement et, plus particulièrement, son régime d'autorisation et de contrôle exercé par la CNCTR afin d'éviter l'éparpillement des règles et procédures ainsi que d'assurer au mieux la protection du secret qui accompagne les développements technologiques du renseignement qui constituent un enjeu stratégique majeur. Plus spécifiquement, il pourrait être envisagé un encadrement en deux volets distincts :

- d'une part, l'élaboration d'un véritable cadre juridique relatif à la recherche en renseignement distinguant les programmes qui impliquent ou non des individus en s'inspirant des procédures d'autorisation déjà mise en œuvre dans le cadre de la recherche médicale². Cette solution permettrait d'autoriser plus généralement le recours à l'IA qui pourrait, dans ce cadre, bénéficier de nombreuses données variées tout en renforçant la protection des données personnelles. Un principe cardinal d'interdiction d'utilisation de ce cadre à des fins de surveillance devrait cependant être rigoureusement respecté. En outre, un dispositif encadré de recherche pourrait servir à la validation de la fiabilité technique et juridique des outils d'IA de surveillance avant d'être soumis au législateur ou au pouvoir réglementaire pour un déploiement opérationnel, ce qui renvoi d'ailleurs

¹ Cf. C. Villani, *Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne*, Rapport de la mission parlementaire du 8 septembre 2017 au 8 mars 2018, p. 222.

² Pour plus de détails, voir [Recherche médicale : quel est le cadre légal ? | CNIL](https://www.cnil.fr/fr/recherche-medicale-quel-est-le-cadre-legal) (<https://www.cnil.fr/fr/recherche-medicale-quel-est-le-cadre-legal>).

au critère de fiabilité dégagé par l'arrêt *La Quadrature du Net* du 6 octobre 2020 de la CJUE à propos des algorithmes de l'article L. 851-3¹ ;

- d'autre part, la légalisation au cas par cas de techniques d'IA opérationnelles spécialisées dont les finalités devraient être strictement délimitées par des textes spécifiques à l'instar de la technique de l'article L. 851-3. Cette solution permettrait de mieux contrôler les déploiements opérationnels de l'IA dont les résultats demeurent encore trop incertains pour le respect des libertés. A notre sens, il reste préférable, ici, de progresser « par petits pas » plutôt que d'élaborer un cadre légal trop général favorable à une multiplication des outils d'IA ou au déploiement d'une IA généraliste qui pourraient s'avérer difficiles à contrôler techniquement et juridiquement.

Le cadre juridique actuel du renseignement semble limiter la nécessité pour l'IA d'« *ingérer d'importants jeux de données multicanaux et multisources* » selon Floran Vadillo². Pour l'auteur, le droit du renseignement comme le droit de la protection des données devraient évoluer vers davantage de mutualisation des produits des techniques de renseignement ou encore en renforçant les fichiers de souveraineté, notamment en permettant la constitution d'un « *fichier de souveraineté thématique (lutte contre le terrorisme ou contre-espionnage)* » ou en autorisant l'interconnexion des fichiers. Suivant un principe de « *Legal by design* », ces solutions devraient donc permettre aux services d'utiliser des outils d'IA sur les données disponibles au sein de la communauté du renseignement en s'appuyant sur l'ensemble des dispositions législatives en vigueur. Ces préconisations nous apparaissent envisageables pour donner un cadre à l'IA en renseignement et pourraient s'inscrire dans les deux volets que nous avons exposés. Dans le cadre légal de la recherche, il pourrait être autorisé plus largement des interconnexions entre des fichiers constitués pour les besoins des projets de recherche impliquant des données de renseignement anonymisées afin notamment de développer des outils d'IA de croisement de données. En revanche,

¹ En ce sens, voir W. Maxwell, *La CJUE dessine le noyau dur d'une future régulation des algorithmes*, Légitimes #388, décembre 2020, p. 671 à 675.

² Cf. F. Vadillo, *Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?*, op. cit..

une utilisation de l'IA à des fins de recueil de renseignement devrait être encadrée par le second volet, c'est-à-dire par un texte spécifique délimitant clairement la ou les spécialisations de l'IA et les finalités de l'outil dans le cadre du régime des techniques de recueil du renseignement soumises à autorisation. S'agissant d'une IA qui mutualiserait les renseignements collectés ou interconnecterait des fichiers de renseignement, on renverra à nos développements relatifs aux interconnexions qui indiquent que ces traitements pourraient être régis par la loi relative au renseignement plutôt que la loi informatique et libertés¹.

Enfin, l'IA s'est fortement développée dans le secteur privé qui dispose de très nombreux experts qualifiés dans ce domaine. Ainsi, les services de renseignement nouent légitimement des partenariats technologiques avec des entreprises privées de l'IA afin de pouvoir rapidement profiter de leurs avancées. En 2016, la DGSi a eu recours aux logiciels d'analyse des données de l'entreprise américaine Palantir². Afin d'éviter le recours à des solutions étrangères, il a été proposé de réunir des industriels technologiques français au sein d'un « *cluster Data intelligence* »³. De leur côté, les services du ministère de la défense devraient bénéficier du projet Artemis qui « *a vocation à faire émerger des applications utilisant l'intelligence artificielle pour le traitement massif des données qui permettent aux combattants de se concentrer sur les informations importantes afin de prendre des décisions rapides et efficaces* »⁴. Pour un exemple plus précis, la DRM expérimente des algorithmes d'IA de détection, de reconnaissance et d'identification d'avions, véhicules et navires avec les experts de l'entreprise Preligens, spécialisée dans l'IA d'analyse d'imagerie satellitaire⁵.

Juridiquement, le recours à l'expertise privée en matière d'IA n'est pas à remettre en question lorsque les initiatives s'inscrivent dans des projets de

¹ Cf. supra. §3. *Les interconnexions entre les fichiers.*

² Sur ce point, voir F. Vadillo, *Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?*, op. cit..

³ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 278 et 279.

⁴ Ibid., p. 279.

⁵ A ce sujet, voir [Le renseignement militaire muscle ses capacités d'analyse de l'imagerie satellitaire avec l'intelligence artificielle - Zone Militaire \(opex360.com\)](http://www.opex360.com/2021/07/08/le-renseignement-militaire-muscle-ses-capacites-danalyse-de-limagerie-satellitaire-avec-lintelligence-artificielle/) (<http://www.opex360.com/2021/07/08/le-renseignement-militaire-muscle-ses-capacites-danalyse-de-limagerie-satellitaire-avec-lintelligence-artificielle/>).

recherche pilotés et encadrés par les services de renseignement ou leur ministère de tutelle. D'ailleurs, les partenariats technologiques avec le secteur privé dans le domaine de la recherche pourraient entrer dans le champ d'application du droit relatif à la recherche en renseignement qui constituerait alors un socle juridique à une filière industrielle souveraine. En effet, cette dernière profiterait des données fournies par les services pour développer des solutions adaptées au profit de l'ensemble de la communauté du renseignement dans le respect du droit de la protection des données personnelles, du droit de la protection du secret de la défense nationale et des droits fondamentaux. On retrouverait le principe de « Legal by design » mis en avant par Floran Vadillo. En outre, la création d'un institut des données de renseignement intéressant la sûreté de l'Etat, la défense et la sécurité publique pourrait être envisagé en s'inspirant de l'Institut National des Données de Santé (INDS) et du Health Data Hub¹. Composé des services de renseignement, de la CNCTR et, pourquoi pas, des acteurs de la filière industrielle souveraine, cet institut veillerait à la bonne application des règles encadrant les projets de recherche et à leur qualité. Bien sûr, nous sommes conscients qu'une telle évolution implique de faire preuve d'une plus grande ouverture vers le secteur privé et de la recherche de la part des acteurs du renseignement même si cette ouverture serait fortement contrôlée, mais n'est-elle pas une condition nécessaire au développement d'outils souverains d'IA en renseignement ?

En revanche, il convient de rappeler que l'article L. 811-1 du code de la sécurité intérieure interdit toute délégation de la politique publique du renseignement qui relève de la compétence exclusive de l'Etat. Ces dispositions devraient s'interpréter comme ne permettant pas aux services de renseignement de déléguer leurs missions de renseignement à des opérateurs privés offrant des services d'IA de surveillance ou d'exploitation des données de sécurité nationale. En revanche, une externalisation des prestations techniques détachables des

¹ « L'INDS était un groupement d'intérêt public constitué entre l'Etat, des organismes assurant une représentation des malades et des usagers du système de santé, des producteurs de données de santé et des utilisateurs publics et privés de données de santé, y compris des organismes de recherche en santé. Il était notamment chargé de veiller à la qualité des données de santé et aux conditions générales de leur mise à disposition, garantissant leur sécurité et facilitant leur utilisation dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés... Les missions de l'INDS ont été reprises et élargies par la création du Health Data Hub (opens new window) en 2019 ». [INDS - Institut National des Données de Santé | Documentation du SNDS \(health-data-hub.fr\)](https://documentation-snds.health-data-hub.fr/glossaire/inds.html) (<https://documentation-snds.health-data-hub.fr/glossaire/inds.html>).

fonctions de souveraineté n'est pas impossible selon la jurisprudence constitutionnelle¹.

On terminera notre analyse en précisant que la première réglementation spécifique à l'IA au niveau européen, l'*AI Act* de 2024², ne trouvera pas à s'appliquer en matière de renseignement. Cette solution est confirmée par la CNCTR dans son étude dédiée à l'IA dans son rapport d'activité pour l'année 2023 qui appelle à renforcer le contrôle des systèmes d'IA en matière de sécurité et de défense, reconnaissant notamment l'encadrement limité de ces systèmes en matière de renseignement³. Toutefois, la CNCTR envisage de s'appuyer sur les règles applicables aux systèmes d'IA à haut risque de l'*AI Act* pour assurer un meilleur contrôle dans le domaine du renseignement, c'est-à-dire d'auditer les systèmes concernés et de proposer une doctrine d'emploi assurant la préservation des droits et libertés fondamentaux⁴. Cette solution nous apparaît cohérente et pourrait s'inscrire dans le contrôle continue des systèmes d'IA autorisés par la loi à des fins opérationnelles.

Parmi les défis de l'IA et de l'analyse des données, on peut citer la technologie biométrique qui intéresse également le renseignement mais dont la mise en œuvre s'avère délicate.

¹ En ce sens, voir M. Delpuech, *Le rôle de l'Etat en matière de sécurité*, *Revue des Juristes de Sciences Po* n° 19, octobre 2020.

² Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (Texte présentant de l'intérêt pour l'EEE).

³ Cf. CNCTR, 8^{ème} rapport d'activité (2023), p. 135 à 174.

⁴ Ibid.

§2. La technologie biométrique

Selon la CNIL, « la biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.) »¹. En matière de renseignement, la technologie biométrique représente un atout majeur pour identifier des cibles qui peuvent parfois recourir à de fausses identités comme en matière de contre-espionnage ou de contre-terrorisme par exemple².

Pour les services de renseignement qui envisagent d'y recourir, l'usage de la reconnaissance biométrique, et plus particulièrement la reconnaissance faciale, à des fins d'identification est « inéluctable » en matière de surveillance³. Il s'agirait notamment d'appliquer au renseignement les exemples d'usages suivants :

- « la recherche, dans une base de données comportant des photographies, de l'état civil d'une personne (victime, suspecte, etc.) non identifié [...] ;
- le suivi des déplacements d'une personne dans l'espace public, par comparaison entre son visage et les gabarits biométriques des personnes circulant ou ayant circulé dans la zone surveillée, par exemple en cas d'oubli d'un bagage ou à la suite de la commission d'un délit ;
- la reconstitution du parcours d'une personne et de ses interactions successives avec des personnes tierces, par une comparaison des mêmes éléments mais réalisée en différé, pour identifier ses contacts par exemple ;
- l'identification sur la voie publique de personnes recherchées, par confrontation en temps réel de tous les visages captés à la volée par des caméras de vidéoprotection et une base de données détenue par les forces de l'ordre »⁴.

¹ Cf. [Biométrie | CNIL](https://www.cnil.fr/fr/biometrie) (<https://www.cnil.fr/fr/biometrie>).

² A ce sujet, voir J. Poirot, *Biométrie*, Dictionnaire du renseignement, op. cit., p. 105 à 108.

³ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 118.

⁴ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 113 et 114.

Ajoutons que les dispositifs de reconnaissance faciale trouveraient à s'appliquer dans le cadre de la captation d'images par les services, de la surveillance sur internet et de la surveillance de l'espace public¹.

Cependant, la CNIL a souligné que les développements de la biométrie présentent des risques pour les libertés, notamment en entraînant « *un changement de paradigme de la surveillance* » avec « *le passage d'une surveillance ciblée de certains individus à la possibilité d'une surveillance de tous aux fins d'identifier certains* »². Cette surveillance massive pourrait s'avérer préjudiciable pour le respect du droit à la vie privée (remise en cause de l'anonymat dans l'espace public) et avoir un « effet dissuasif » sur l'exercice de certaines libertés comme la liberté d'expression et de réunion³, d'autant plus que les traitements biométriques ne sont pas encore suffisamment matures⁴.

Au niveau du cadre juridique applicable au renseignement, seule la DRM est aujourd'hui autorisée à disposer d'un dispositif biométrique dans le cadre des opérations extérieures, notamment avec le fichier BIOPEX⁵. Par ailleurs, l'article R. 222-1 du code de la sécurité intérieure prohibe toute interconnexion possible entre le système TES de gestion des données biométriques relatives aux titres électroniques sécurisés (cartes d'identité et passeports) et les traitements des services de renseignement, ce qui a notamment pour effet d'empêcher la mise en œuvre d'un dispositif de reconnaissance faciale⁶. On relèvera que cette prohibition a pour fondement la jurisprudence du Conseil constitutionnel⁷. Enfin, le « rapport Larrivé » de 2020 ne recommande aucune évolution législative, même

¹ Voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 118.

² Cf. CNIL, *Reconnaissance faciale : pour un débat à la hauteur des enjeux*, 15 novembre 2019, p. 6 et suivantes.

³ La peur engendrée par la surveillance biométrique pourrait avoir un impact sur le comportement des individus qui pourraient renoncer à exercer leurs droits (cf. Défenseur des droits, *Rapport Technologies biométriques : l'impératif respect des droits fondamentaux*, Juillet 2021, p. 14).

⁴ En ce sens, voir CNIL, *Reconnaissance faciale : pour un débat à la hauteur des enjeux*, op. cit., p. 6 et suivantes.

⁵ Cf. supra. *Les règles spécifiques aux fichiers de renseignement*.

⁶ Sur ce point, voir G. Koubi, *Le « méga-fichier » des titres électroniques sécurisés*, La Semaine Juridique Administrations et Collectivités territoriales n° 47, 28 novembre 2016.

⁷ Décision n° 2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité.

expérimentale, en faveur du renseignement au regard de la maturité de cette technologie et de ces risques pour les libertés¹.

Pour autant, le rapport précité émet l'hypothèse d'un encadrement de la reconnaissance faciale dans les lieux publics sur le territoire national par :

- l'intégration de cette capacité dans le régime des techniques de renseignement pour qu'elle puisse être autorisée uniquement que dans certains lieux publics ;
- la constitution d'« *un fichier permanent de données biométriques qui ne serait activé que lors de périodes déterminées, dans des contextes prévus ou dans des zones particulièrement exposées* »².

L'hypothèse ainsi envisagée n'est pas nouvelle. Déjà en 2011, le rapport d'information des députés Delphine Batho et Jacques Alain Bénisti sur les fichiers de police avait suggéré l'idée d'un « *fichier autonome de reconnaissance faciale* » en matière judiciaire pour exploiter des données de vidéosurveillance. Notons que le rapport allait plus loin en se montrant favorable aux propositions des auteurs du Livre blanc sur la sécurité publique de 2011 relatives à la création d'une « *base nationale des photographies* » et d'un « *système d'information global permettant le rapprochement des différentes traces criminalistiques* » ainsi que sur « *la recherche en matière de reconnaissance de tatouages, de personnes en mouvement, de signatures vocales ou encore de traces olfactives* »³. On retrouve également l'idée d'un fichier autonome de reconnaissance faciale et limité à des cas d'usages spécifiques et temporaires dans le rapport du Groupe de diagnostic stratégique (GDS) n°8 de la 30ème session nationale « Sécurité et Justice » 2018 – 2019 de l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ)⁴.

Pour notre part, l'identification par reconnaissance faciale ainsi envisagée souffre de limites techniques qui ne devraient pas permettre sa légalisation

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 119.

² Ibid.

³ Cf. D. Batho et J. A. Bénisti, *Rapport d'information sur les fichiers de police*, op. cit., p. 96 et suivantes.

⁴ Cf. Groupe de diagnostic stratégique (GDS) n°8, *Reconnaissance faciale : entre exigence de contrôle et respect de la vie privée Quels outils, quels enjeux, quelles garanties ?*, Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ), 30ème session nationale « Sécurité et Justice » 2018 – 2019.

prochaine pour la majorité des cas d'usages que nous avons évoqués précédemment. En effet, la CNIL relève qu'elle correspond à la biométrie dite « à trace », c'est-à-dire que l'association d'un dispositif de vidéosurveillance et d'un logiciel de reconnaissance faciale permet de capturer et d'utiliser à l'insu des personnes concernées des traces informatiques similaires à des traces physiques comme les empreintes digitales¹. Juridiquement, il conviendrait donc de limiter le traitement des images à celles relatives aux personnes surveillées et à leurs interactions et d'interdire la collecte des données des autres personnes pouvant être alpaguées par le dispositif. Néanmoins, la faible fiabilité actuelle des algorithmes de reconnaissance faciale peut conduire à mal reconnaître les personnes ciblées, voire aboutir à la surveillance d'un individu n'ayant aucun rapport avec l'autorisation de la mesure. Dans ces conditions, il nous semble encore difficile de concilier les capacités techniques de l'identification par reconnaissance faciale avec les garanties juridiques contre les risques d'atteinte disproportionnée aux droits et libertés des personnes.

En revanche, il se pose la question de savoir si un dispositif de reconnaissance faciale pourrait être mis en œuvre afin de seulement vérifier si l'identité d'une personne surveillée non identifiée est déjà connue des services de renseignement à l'instar du dispositif biométrique du TAJ. Ce dernier permet à la police judiciaire de comparer l'image d'un individu impliqué dans la commission d'une infraction avec les photographies enregistrées dans le TAJ². Dans ce cas, il pourrait s'agir d'opérer un rapprochement technique entre des images collectées par les services lors de leurs opérations de surveillance (utilisation de la technique de captation d'images par exemple) et des photographies issues de leurs fichiers pour repérer des alias ou l'utilisation d'une fausse identité ou encore pour reconnaître des personnes qui interagissent avec une cible. Les décrets relatifs aux fichiers des services de renseignement pourraient alors prévoir le traitement de photographies comportant des caractéristiques techniques permettant la reconnaissance faciale comme par exemple une photographie du visage de face.

¹ A ce sujet, voir la note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité, séance plénière le 25 octobre 20, p. 2.

² Délibération n° 2011-204 du 7 juillet 2011 portant avis sur un projet de décret en Conseil d'Etat relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé « traitement de procédures judiciaires » (TPJ) (demande d'avis n° 1484843).

L'utilisation du dispositif serait quant à lui autorisé par la loi dans le cadre des techniques de renseignement à titre subsidiaire, c'est-à-dire que si aucun autre moyen ne permet de vérifier si la personne est déjà connue des services. On remarquera cependant qu'il s'agit plus d'une technique d'exploitation de données que de recueil des renseignements. Dans tous les cas, l'intégration de la biométrie dans les techniques de renseignement s'accompagne d'une confusion entre recueil et exploitation des données comme pour les algorithmes d'IA en général.

Cette dernière solution fait échos à l'utilité de la biométrie « *pour repérer les personnels civils étrangers ayant servi à l'étranger, qui se font renvoyer de leur base et qui se font employer sur une autre base en changeant de nom, grâce à de faux papiers : la reconnaissance biométrique permet alors de vérifier que la personne ne porte pas son vrai nom* » comme relevé dans le « rapport Larrivé » par un interlocuteur de la mission d'information¹. Ajoutons qu'elle participerait à la fiabilité des opérations de surveillance. Soulignons enfin que cette solution correspond davantage à une « biométrie de vérification » selon les recommandations du Commissariat à la protection de la vie privée du Canada qui considère ce type de biométrie plus respectueux des droits et libertés des individus².

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 118.

² Cf. [Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée - Commissariat à la protection de la vie privée du Canada](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/) (https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/).

CONCLUSION DU TITRE

La légalisation des moyens numériques de renseignement a été initiée en droit du numérique, d'abord par la loi « informatique et libertés » de 1978 et ensuite par la loi relative au secret des correspondances électroniques de 1991. Cette légalisation s'est attachée à encadrer, d'une part, les moyens numériques de recherche des renseignements et, d'autre part, les moyens d'exploitation des renseignements selon une distinction établie par les lois de 1978 et 1991 entre les interceptions des communications et les traitements de données. Dans ce cadre juridique général fondé principalement sur les composantes numériques du droit au respect de la vie privée (protection du secret des correspondances électroniques et protection des données personnelles), les services de renseignement ont vu la légalisation de leurs moyens numériques d'investigation faiblement évoluer.

Les lois relatives au renseignement de 2015 ont opéré un profond bouleversement dans l'encadrement des moyens de recherche et d'exploitation des renseignements. Ces textes ont consacré un véritable droit du renseignement permettant de renforcer considérablement les seuls moyens numériques de recherche des renseignements en renouvelant la distinction établie par les lois de 1978 et 1991 avec notamment la consécration des techniques de recueils des renseignements. Cependant, le dispositif envisagé par le législateur de 2015 et ses évolutions entraînent en réalité une confusion entre les moyens numériques de recherche et d'exploitation. En effet, les algorithmes de détection des menaces terroristes ont été qualifiés de techniques de recueil des renseignements alors qu'il s'agit de traitements automatisés de données mis en œuvre chez les opérateurs qui auraient pu être encadré par les dispositions de loi informatique et libertés. La loi relative à la surveillance des communications internationales consacre textuellement en droit du renseignement un cadre juridique portant à la fois sur les interceptions et sur les exploitations des données. Le législateur a également fait le choix d'introduire dans le droit du renseignement des mécanismes spécifiques de partage de données entre les services et d'autres institutions alors que la circulation des données relève normalement du droit de la protection des données. En outre, un basculement de la loi « informatique et libertés » vers le droit du renseignement pourrait être à prévoir en ce qui concerne

l'encadrement des fichiers de renseignement, notamment avec la question de la requalification des interconnexions en technique de recueil des renseignements pour que les services puissent renforcer la mutualisation de leurs productions. Enfin, le droit du renseignement semble être le cadre juridique privilégié pour réguler les innovations en matière de traitements des données comme par exemple le recours à l'intelligence artificielle ou la biométrie.

L'ensemble des moyens numériques de renseignement tend peu à peu à être globalement régi par le droit du renseignement, ce qui n'est d'ailleurs pas remis en cause par la CNIL à la condition toutefois que la protection des données personnelles soit suffisamment assurée. On ajoutera que l'harmonisation de l'encadrement des moyens numériques de recherche et d'exploitation dans le droit du renseignement nous apparaît conforme aux dispositions de l'article L. 811-2 du code de la sécurité intérieure qui précise que les services de renseignement « *ont pour missions, 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* ».

De nouvelles distinctions plus adaptées à l'encadrement de la surveillance numérique viennent ainsi remplacer la distinction établie par les lois de 1978 et 1991. Il s'agit notamment de la distinction entre la surveillance nationale et internationale ou encore celle entre une surveillance « partenariale » reposant sur l'intervention des opérateurs du numérique et le partage des données et une surveillance plus directe mise en œuvre par les services à travers des dispositifs techniques spécifiques et l'exploitation de leur propre fichier.

Le droit du renseignement constitue le cadre juridique général du renforcement des besoins numériques de surveillance, ce qui n'est pas sans avoir introduit dans notre droit des outils techniques qui, par nature, permettent de collecter et traiter des données massives et qui peuvent conduire à la mise en place d'une surveillance de masse potentiellement liberticide. D'autant plus que le droit du renseignement n'a cessé d'évoluer depuis 2015 pour intégrer de nouvelles mesures de surveillance numérique ou pour renforcer les techniques déjà consacrées. Toutefois, il convient de préciser que ce renforcement des moyens

s'est concrétisé par l'adaptation des garanties prévues par le droit du renseignement aux spécificités de la surveillance numérique.

TITRE II

L'ADAPTATION DES GARANTIES AUX MOYENS NUMERIQUES DE RENSEIGNEMENT

En contrepartie d'un renforcement des moyens numériques de renseignement, les textes juridiques relatifs au renseignement et la jurisprudence des instances de contrôle ont adaptés les garanties contre les risques d'abus des services aux enjeux du droit au respect de la vie privée à l'ère numérique. Ces enjeux ont conduit le législateur à adopter un régime juridique de mise en œuvre des moyens numériques que nous qualifierons d'ambivalent en raison des différentes solutions administratives et pénales retenues (**Chapitre I**). Ils ont également entraîné un mouvement de spécialisation des contrôles (**Chapitre II**).

CHAPITRE I

L'AMBIVALENCE DU REGIME DE MISE EN ŒUVRE DES MOYENS NUMERIQUES

Depuis la loi du 10 juillet 1991 relative au secret des correspondances, le droit du renseignement distingue deux régimes juridiques applicable à la mise en œuvre des moyens numériques des services que les différentes lois relatives au renseignement postérieures à 2015 ont consolidés : un régime préventif qui soumet la surveillance numérique à une autorisation préalable (**Section I**) et un régime répressif qui permet de mettre en cause la responsabilité de l'administration ou des agents de renseignement devant un juge afin de sanctionner une surveillance numérique constitutive d'une faute (**Section II**).

SECTION I : Le régime préventif, une surveillance numérique soumise à autorisation préalable

Comme le rappelle le Professeur Bertrand Warusfel, le législateur a fait le choix de soumettre au principe de légalité uniquement les moyens de renseignement numérique attentatoires au respect du droit à la vie privée¹. Au regard du caractère très intrusif des techniques d'investigation, il a donc été décidé d'encadrer leur mise en œuvre par à une procédure d'autorisation préalable délivrée par le Premier ministre². La loi relative au renseignement du 24 juillet 2015 a d'ailleurs défini précisément les éléments du principe de légalité applicable à la procédure de mise en œuvre des techniques de renseignement. Ces éléments sont codifiés à l'article L. 801-1 du code de la sécurité intérieure, l'importance de cet article nous amène à le citer directement ici :

¹ Cf. B. Warusfel, *Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement*, Le droit du renseignement, op. cit., p. 75 et 76.

² S'inscrivant dans le cadre de la police administrative, le Premier ministre s'est vu normalement attribuer cette compétence sur le fondement de l'article 21 de la Constitution de 1958, ce qui a été validé par le Conseil constitutionnel dans sa décision n° 2015-713 DC du 23 juillet 2015 relative à la loi renseignement de 2015 (cf. M. Verpeaux, *La loi sur le renseignement, entre sécurité et libertés*, La Semaine Juridique Edition Générale n° 38, 14 septembre 2015, doct. 981).

« Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité. L'autorisation et la mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées aux chapitres Ier à III du titre V du présent livre ne peuvent être décidées que si : 1° Elles procèdent d'une autorité ayant légalement compétence pour le faire ; 2° Elles résultent d'une procédure conforme au titre II du même livre ; 3° Elles respectent les missions confiées aux services mentionnés à l'article L. 811-2 ou aux services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 ; 4° Elles sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ; 5° Les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués. La Commission nationale de contrôle des techniques de renseignement s'assure, dans les conditions prévues au présent livre, du respect de ces principes. Le Conseil d'Etat statue sur les recours formés contre les décisions relatives à l'autorisation et à la mise en œuvre de ces techniques et ceux portant sur la conservation des renseignements collectés ».

Dans le prolongement de ces éléments du principe de légalité, les dispositions du code de la sécurité intérieure spécifiques à la demande d'autorisation précisent que celle-ci doit mentionner « 1° La ou les techniques à mettre en œuvre ; 2° Le service pour lequel elle est présentée ; 3° La ou les finalités poursuivies ; 4° Le ou les motifs des mesures ; 5° La durée de validité de l'autorisation ; 6° La ou les personnes, le ou les lieux ou véhicules concernés »¹.

Il ressort de ces dispositions que le régime préventif ainsi mis en place par la loi apportent des garanties contre la surveillance numérique qui touchent aux missions des services de renseignement (§1) ou qui sont intrinsèques aux techniques numériques (§3) ou encore qui portent spécialement sur les renseignements collectés (§4).

¹ Article L. 821-2 du code de la sécurité intérieure.

§1. Les garanties relatives aux missions des services de renseignement

Tout en réaffirmant le droit au respect de la vie privée, notamment le droit au secret des correspondances et la protection des données personnelles, la loi relative au renseignement de 2015 a consacré la nécessité pour les services de renseignement de justifier la mise en œuvre des moyens numériques soumis à autorisation par un intérêt public¹. La loi a alors précisé les finalités pouvant être invoquées par les services tout en exigeant que ces derniers recourent aux techniques de renseignement que « *pour le seul exercice de leurs missions respectives* »².

A - Les finalités invocables par les services de renseignement

Avant d'analyser à l'application des finalités aux techniques de renseignement, il convient de nous intéresser au périmètre de ces finalités, notamment dans le cadre de notre étude qui porte sur la cyberdimension.

1. L'élargissement du périmètre des finalités et cyberdimension

La délimitation des finalités pour lesquelles les services de renseignement peuvent recourir à des techniques numériques intrusives est une garantie issue de l'article 3 de la loi du 10 juillet 1991 relative aux interceptions de sécurité. Cette dernière limitait les autorisations d'interceptions aux finalités du renseignement intéressant « *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* ». La loi relative au renseignement de 2015 a renouvelé et élargie cette liste de finalités en s'inspirant de la notion d'intérêts fondamentaux de la Nation définie dans l'article 410-1 du code pénal³. Désormais, l'article L. 811-3 mentionne les finalités suivantes :

- « *l'indépendance nationale, l'intégrité du territoire et la défense nationale* ;

¹ Article L. 801-1 du code de la sécurité intérieure.

² Article L. 811-3 du code de la sécurité intérieure.

³ Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 3.

- *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 ;*
- *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 L. 212-1 ; des violences collectives de nature à porter gravement atteinte à la paix publique ;*
- *la prévention de la criminalité et de la délinquance organisées ;*
- *la prévention de la prolifération des armes de destruction massive ».*

Deux remarques doivent être soulevées sur les finalités de l'article L. 811-3. D'une part, le législateur de 2015 a souhaité préciser la notion de « sécurité nationale » en consacrant textuellement la jurisprudence de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), « *ce qui explique la multiplication des items sans pour autant étendre le champ d'action des services* » selon Floran Vadillo. D'autre part, l'article L. 811-3 est venu inscrire « *la dimension défensive et offensive du renseignement* » dans la loi en disposant que les finalités sont relatives « *à la défense et à la promotion des intérêts fondamentaux de la Nation* »¹.

Dans sa décision du 23 juillet 2015, le Conseil constitutionnel a jugé que ces finalités relèvent de la police administrative et sont clairement définies et suffisamment précises puisque leur définition figure dans le code pénal et le code de procédure pénale, le code de la sécurité intérieure, le code des douanes ou le code de la défense². La position des « Sages » n'a pourtant pas convaincu un certain nombre de commentateurs de la loi relative au renseignement qui ont notamment critiqué l'absence d'un véritable contrôle de la nécessité des mesures de surveillance au regard de finalités considérées comme imprécises ou encore une allusion insuffisante à d'autres définitions dans d'autres codes pour circonscrire

¹ Cf. F. Vadillo, *Quand l'Etat de droit rencontre l'Etat secret : cadre et garanties du recours aux techniques de recueil de renseignement*, Le droit du renseignement, op. cit., p.95.

² Décision n° 2015-713 DC du 23 juillet 2015 (considérants 7 à 12).

l'usage des techniques de renseignement¹. Alors que ces finalités ont été présentées comme une garantie contre les risques d'une surveillance de masse, certains commentateurs ont pointé un abandon du caractère exceptionnel de l'usage des techniques de renseignement et la création d'une police administrative spéciale disposant de larges finalités pouvant conduire à une violation massive de la vie privée des citoyens². On relèvera que les requêtes introduites devant la Cour européenne des droits de l'Homme (CEDH) contre les dispositions de la loi relative au renseignement de 2015 portent notamment sur l'article L. 811-3 car le législateur aurait retenu une définition trop large des finalités ayant pour effet de mettre en place un régime légal non « *strictement nécessaire à la préservation des institutions démocratiques* » au sens des articles 8 et 10 de la Convention européenne des droits de l'Homme (Conv. EDH)³. Malgré ces critiques, soulignons que la précision des finalités prévue à L. 811-3 s'inscrit dans la logique des régimes dérogatoires prévus par les textes internationaux des droits l'homme⁴. Par ailleurs, notons que la liste de l'article L. 811-3 « *marque en creux les domaines qui n'entrent pas dans le champ des finalités justifiant la mise en œuvre de techniques de renseignement, en particulier le renseignement politique* », ce que la CNCTR n'a pas manqué de rappeler s'agissant de la finalité relative à la prévention des violences collectives⁵.

Depuis 2015, le périmètre défini à l'article L. 811-3 n'a pas été modifié mais les finalités du renseignement ont tout de même connu des évolutions. Parallèlement à l'introduction du renseignement pénitentiaire dans les services

¹ En ce sens, voir O. Desaulnay et R. Ollard, *Le renseignement français n'est plus hors-la-loi*, op. cit. ; R. Parizot, *Surveiller et prévenir... à quel prix ? Commentaire de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement*, JCP n° 41, 5 oct. 2015. Doctr. 1077 ; M. Rees, *La loi sur le renseignement ou le grand méchant flou*, Revue Le Lamy Droit de l'immatériel, n° 118, 1^{er} aout 2015.

² En ce sens, voir E. Bédarrides, *Des écoutes au renseignement, un exemple de la distinction entre les polices judiciaire et administrative*, AJDA 2015, p. 2026 ; C. Lazerges et H. Henrion-Stoffel, *Politique criminelle, renseignement et droits de l'homme, à propos de la loi du 24 juillet 2015 relative au renseignement*, RSC 2015, p. 761 ; J. -B. de Gubernatis et M. Martin, *La loi relative au renseignement : la victoire de la peur sur l'idéal de protection des droits et libertés ?*, Les Cahiers Portalis, vol. 3, n° 1, 2016, p. 75 à 85.

³ A ce sujet, voir CNCTR, *5^{ème} rapport annuel (2020)*, p. 25 et 26.

⁴ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 24 et 25.

⁵ L'exclusion du renseignement politique a amené la CNCTR à rappeler que la prévention des violences collectives ne peut notamment s'interpréter comme permettant la surveillance numérique d'un milieu syndical ou politique (cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 27).

autorisés à recourir aux techniques de renseignement¹, la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique a élargie les finalités du renseignement en dehors des intérêts fondamentaux de la Nation en consacrant les finalités spécifiques au milieu carcéral suivantes : la prévention des évasions et pour assurer la sécurité et le bon ordre au sein des prisons et établissements de santé destinés à recevoir des détenus selon l'article L. 855-1 du code de la sécurité intérieure². Cependant, la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice est venue écarter la notion de « bon ordre » considérée comme peu précise³.

Dans la même période, la loi de programmation militaire (LPM 2019-2025) du 13 juillet 2018 a introduit le mécanisme des « vérifications ponctuelles » dans le domaine de la surveillance internationale avec notamment comme finalité l'analyse technique d'éléments de cyberattaques susceptibles de porter atteinte à l'indépendance nationale, l'intégrité du territoire et à la défense nationale⁴. Ces dispositions font explicitement entrer la cybersécurité dans la définition des finalités de l'article L. 811-3-1°. Par ailleurs, on relèvera que la question d'ajouter une finalité spécifique à la cybersécurité n'a pas manqué d'être soulevée mais elle a finalement été écartée car *« les techniques utilisées par les attaquants ne constituaient pas en elles-mêmes une finalité mais un simple moyen et que leur utilisation s'inscrivait dans la réalisation d'une finalité prévue par la loi pour justifier l'utilisation d'une technique de renseignement »*⁵. Autrement dit, le renseignement d'intérêt cyber (RIC), comme le renseignement d'origine cyber (ROC), s'inscrit dans les finalités de l'article L. 811-3, ce qui implique que les cyberattaques concernées constituent des menaces aux intérêts fondamentaux de la Nation. Si la cybersécurité ne constitue donc pas juridiquement une finalité propre du renseignement, la cyberdéfense est en revanche une finalité opérationnelle du Plan National d'Orientation du Renseignement (PNOR) qui intègre les services de

¹ Loi n° 2016-731 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.

² Cf. CNCTR, *2^{ème} rapport annuel (2017)*, p. 30 et suivantes.

³ Cf. CNCTR, *4^{ème} rapport annuel (2019)*, p. 18 et 19.

⁴ Alinéa 3 du IV de l'article L. 854-2 du code de la sécurité intérieure.

⁵ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 261.

renseignement dans la politique publique de la cyberdéfense¹. Dans ce contexte, la DPR souhaiterait que la CNCTR puisse être en mesure d'indiquer statistiquement le nombre d'avis préalable rendus sur les techniques de renseignement dans le cadre du RIC afin de pouvoir évaluer la participation des services dans le domaine de la cyberdéfense².

La cyberdimension a également conduit le législateur à prévoir une finalité dédiée à la recherche et développement pour permettre d'entraîner les outils d'intelligence artificielle. La loi relative au renseignement du 30 juillet 2021 a introduit cette nouvelle finalité afin de justifier une dérogation à la durée légale de conservation des renseignements collectés et la mise en œuvre de programmes de recherche soumis à autorisation du Premier ministre³. Distincte des finalités de l'article L. 811-3, la finalité prévue par la loi du 30 juillet 2021 vise à clairement distinguer la recherche et le développement en renseignement et la surveillance des personnes⁴. Cette distinction dans les finalités du renseignement nous semble favorable à l'élaboration d'un cadre juridique dédié à la recherche technologique en renseignement⁵. Que ce soit par la prise en considération du RIC ou l'émergence de la recherche et développement de capacités techniques en renseignement, la cyberdimension tend à constituer un motif autonome justifiant certaines des activités des services de renseignement dans le cadre des finalités de l'article L. 811-3.

¹ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 240.

² Ibid., p. 262.

³ Article L. 822-2-III du code de la sécurité intérieure.

⁴ En ce sens, voir CNIL, 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 ; M.-P. Daubresse et A. Canayer, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, Sénat, 16 juin 2021, p. 63 et suivantes.

⁵ Cf. supra. Section II du Chapitre II du Titre I de la Ière Partie.

2. L'application des finalités dans la mise en œuvre des techniques de renseignement

D'abord, la loi a circonscrit à certaines finalités l'autorisation des techniques de renseignement les plus intrusives¹. S'agissant des techniques autorisées à être mises en œuvre sur le territoire national, les interceptions via « IMSI-catcher »² ne peuvent être utilisées que pour les finalités 1°, 4° et a du 5° de l'article L. 811-3 ainsi que les interceptions satellitaires³ que pour les finalités 1°, 2°, 4° et 6° du même article. Les sondes « temps réel » et algorithmes d'accès aux données de connexion⁴ ne sont, quant à eux, autorisés que pour la prévention du terrorisme. On relèvera qu'il a été question d'étendre à d'autres finalités la mise en œuvre des algorithmes, notamment pour le contre-espionnage et la criminalité⁵. Pour l'heure, cette solution n'a pas été retenue et nous semble inopportune au regard des performances encore limitées des algorithmes⁶. En matière de surveillance internationale, on rappellera que certaines « vérifications ponctuelles » ne sont autorisées que pour la prévention du terrorisme ou pour l'analyse des cyberattaques relevant du 1° de l'article L. 811-3⁷ et que les autorisations d'exploitation de communications rattachables au territoire national interceptées ne peuvent concerner que les finalités 1°, 2°, 4°, 6° et 7° de l'article L. 811-3⁸. Il convient de remarquer que la prévention du terrorisme constitue la seule finalité pouvant être invoquée pour l'ensemble des techniques de renseignement mais aussi la finalité la plus utilisée par les services⁹. Dans la majorité des affaires, le recours aux techniques de renseignement semble donc peu contraint par la nécessité d'invoquer des finalités précises, y compris pour les

¹ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 39.

² Article L. 852-1-II du code de la sécurité intérieure.

³ Article L. 852-3 du code de la sécurité intérieure.

⁴ Articles L. 851-2 et L. 851-3 du code de la sécurité intérieure.

⁵ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 190.

⁶ Cf. supra. §1 de la Section II du Chapitre I du Titre I de la Ière Partie.

⁷ Alinéa 2 et 3 de l'article L. 854-2-IV du code de la sécurité intérieure.

⁸ Article L. 854-2-V du code de la sécurité intérieure.

⁹ Cf. CNCTR, *5^{ème} rapport annuel (2020)*, p. 43.

techniques les plus intrusives. En revanche, relevons que les demandes d'autorisation relatives à la finalité du renseignement d'intérêt économique (« *intérêts économiques, industriels et scientifiques majeurs de la France* ») se sont heurtées à de nombreux avis défavorables de la CNCTR, cette dernière adoptant une appréciation propre au cas par cas de l'intérêt majeur des intérêts économiques¹. La Commission a finalement assoupli sa position en « *tenant compte des orientations politiques souhaitées par le Gouvernement en matière de protection des intérêts économiques de la France* »². Si la doctrine de la CNCTR avait pour objectif d'assurer le respect du droit à la vie privée contre les risques d'abus de la surveillance numérique à des fins économiques, elle avait pour effet gênant de court-circuiter l'autorité politique dans l'établissement d'une politique publique du renseignement économique.

Ensuite, la procédure d'urgence de mise en œuvre des techniques de renseignement est circonscrite à certaines finalités. En effet, l'article L. 821-5 institué par la loi relative au renseignement de 2015 permettait au Premier ministre de délivrer une autorisation exceptionnelle sans avis préalable de la CNCTR en cas d'urgence et pour les finalités 1°, 4° et a du 5° de l'article L. 811-3. Le Conseil constitutionnel avait jugé ces dispositions conformes au droit au respect à la vie privée notamment en ce qu'elles réservaient la procédure « *à des finalités qui sont relatives à la prévention d'atteintes particulièrement graves à l'ordre public* »³. Néanmoins, la loi relative au renseignement du 30 juillet 2021 est venue abroger l'article L. 821-5 du code de la sécurité intérieure pour instaurer une nouvelle procédure d'urgence conforme à l'arrêt *French Data Network* du 21 avril 2021 du Conseil d'Etat sur la nécessité de prévoir un avis conforme de la CNCTR⁴. Désormais, la décision d'autorisation du Premier ministre ne peut être exécutée en cas d'urgence que dans le cas d'un avis défavorable de la CNCTR et

¹ Sur ce point, voir P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour 2017*, DPR, op. cit., p. 54.

² A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 96 et 97.

³ A ce sujet, voir M. Verpaux, *La loi sur le renseignement, entre sécurité et libertés, à propos de la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015*, op. cit..

⁴ Cf. infra. Section II du Chapitre II du Titre II de la Ière Partie.

durant le temps d'examen de l'affaire par le Conseil d'Etat¹. L'application des finalités demeure seulement pour la procédure d'urgence concernant la captation de paroles, d'images et de données informatiques et leurs modalités pratiques d'exécution (pour les finalités 1°, 4° et a du 5° de l'article L. 811-3). En outre, la procédure d'urgence est exclue pour le recours aux algorithmes². On pourra regretter que le législateur n'ait pas suivi les recommandations de la CNIL sur l'extension de la limitation des finalités à l'ensemble des techniques de renseignement en cas d'urgence comme le prévoyait le dispositif retenu en 2015³.

Enfin, la nécessité d'invoquer les finalités de l'article L. 811-3 trouve à s'appliquer pour limiter la réutilisation des données collectées par les services de renseignement. La loi interdit toute collecte, transcription ou extraction des renseignements pour d'autres finalités que celles prévues à l'article L. 811-3⁴. Soulignons que la transcription des renseignements interceptés en dehors des finalités de l'article L. 811-3 constitue l'une des catégories d'irrégularités relevée par la CNCTR en 2020 tant en matière de surveillance nationale qu'internationale⁵. En revanche, la loi relative au renseignement du 30 juillet 2021 autorise les services à procéder à des transcriptions ou extractions sur des renseignements obtenus qui sont « *utiles à la poursuite d'une finalité différente de celle qui en a justifié le recueil* » dans la limite des finalités de l'article L. 811-3 et pour les seuls besoins des missions propres au service concerné. Par ailleurs, depuis la loi du 30 juillet 2021, les finalités fondent l'application du régime préventif d'autorisation préalable en matière de partage des renseignements entre les services⁶ dans l'hypothèse où les transmissions poursuivent une finalité différente de celle qui a justifié le recueil des renseignements concernés⁷.

¹ Article L. 821-1 du code de la sécurité intérieure.

² Sur ce point, voir P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement, commentaire de la loi n° 2021-998 du 30 juillet 2021*, op. cit..

³ Délibération n° 2021-053 du 3 mai 2021 portant avis sur les articles 11 quinquies, 11 sexies et 11 septies du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

⁴ Article L. 822-3 et L. 854-6 du code de la sécurité intérieure.

⁵ Cf. CNCTR, *5^{ème} rapport annuel (2020)*, p. 65 et suivantes.

⁶ Article L. 822-3-II-1° du code de la sécurité intérieure.

⁷ Sur ce point, voir F. Safi, *La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, entre pérennisation et extension de l'exception...*, op. cit..

En plus de devoir justifier d'un intérêt public légitime, les services sont limités dans l'utilisation des techniques de renseignement en fonction de leurs missions respectives, ce qui peut nécessiter de distinguer les compétences des services en matière de renseignement numérique.

B - Les missions des services et leurs compétences en matière de renseignement numérique

Selon les articles L. 801-1 et L. 811-3 du code de la sécurité intérieure, l'autorisation de mise en œuvre des techniques numériques de renseignement est limitée aux services habilités à y recourir dans le respect de leurs missions reconnues par les lois et règlement. La loi relative au renseignement du 24 juillet 2015 a opéré une distinction entre deux catégories de services compétents : les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure qui constituent le « premier cercle » et les services du « second cercle » désignés par un décret en Conseil d'Etat selon l'article L. 811-4 du même code¹. Si la délimitation des missions des services et leurs compétences techniques jouent un rôle contre les risques d'une surveillance numérique de masse généralisée, il s'est toutefois traduit par une montée en puissance du renseignement numérique des services spécialisés et par un élargissement des services du second cercle.

1. La montée en puissance du renseignement numérique des services du premier cercle

Selon l'article R. 811-1 du code de la sécurité intérieure, la communauté française du renseignement comprend les six services spécialisés suivants² : la DGSE, la DRSD, la DRM, la DGSI, la DNRED et Tracfin. Si la détermination des services spécialisés et de leurs missions relève du domaine réglementaire, il reste que ces services se voient confiés par la loi une mission générale, en France et à l'étranger, de recherche, de collecte, d'exploitation et de mise à disposition du Gouvernement, des renseignements géopolitiques et stratégiques et portant sur la

¹ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 36 ; G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 58 ; R. Parizot, *Surveiller et prévenir... à quel prix ?*, loi n° 2015-912 du 24 juillet 2015 relative au renseignement, op. cit..

² Sur ce point, voir P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 40 à 50.

sécurité nationale¹. A ce titre, les services du premier cercle *« ont vocation à accéder à l'ensemble des techniques de renseignements prévues par le livre VIII du code de la sécurité intérieure »*².

En droit, la loi relative au renseignement de 2015 a donc renforcé la compétence en renseignement numérique des services spécialisés, notamment pour les petites structures que sont la DRM, la DRSD, Tracfin ou la DNRED, en plus de renforcer les moyens techniques. Comme l'a relevé le Professeur Xavier Latour, le dispositif prévu pour les services spécialisés pose les questions suivantes : *« tous les services devaient-ils être traités de la même façon ? Est-il normal de conférer des moyens identiques à des services qui n'ont pas tous la même culture de l'enquête ? »*³. En effet, il convient par exemple de mentionner que *« la DGSE n'a normalement pas vocation à intervenir sur le territoire national, cette compétence relevant de la DGSI »*. Cependant, les dispositions de l'article L. 811-3 contraignent les services à justifier leur demande sur le fondement de finalités relatives à leurs missions respectives et non sur leur mission générale définie à l'article L. 811-2. Les services spécialisés disposent donc de moyens numériques identiques mais ne sont pas traités de la même façon.

En l'espèce, chaque service spécialisé doit justifier que la mise en œuvre d'une technique de renseignement s'inscrit dans le cadre de leurs missions définies par le pouvoir réglementaire. Ainsi, les demandes de la DGSI doivent concerner ses missions définies à l'article 2 du décret n° 2014-445 du 30 avril 2014 qui dispose que :

« au titre de ses missions, la direction générale de la sécurité intérieure :

a) Assure la prévention et concourt à la répression de toute forme d'ingérence étrangère ;

b) Concourt à la prévention et à la répression des actes de terrorisme ou portant atteinte à la sûreté de l'Etat, à l'intégrité du territoire ou à la permanence des institutions de la République ;

¹ Article L. 811-2 du code de la sécurité intérieure.

² Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 32.

³ Cf. X. Latour, *La loi relative au renseignement : un Etat de surveillance ?*, op. cit..

- c) Participe à la surveillance des individus et groupes d'inspiration radicale susceptibles de recourir à la violence et de porter atteinte à la sécurité nationale ;*
- d) Concourt à la prévention et à la répression des actes portant atteinte au secret de la défense nationale ou à ceux portant atteinte au potentiel économique, industriel ou scientifique du pays ;*
- e) Concourt à la prévention et à la répression des activités liées à l'acquisition ou à la fabrication d'armes de destruction massive ;*
- f) Concourt à la surveillance des activités menées par des organisations criminelles internationales et susceptibles d'affecter la sécurité nationale ;*
- g) Concourt à la prévention et à la répression de la criminalité liée aux technologies de l'information et de la communication ».*

S'agissant de la DNRED, elle peut recourir à l'ensemble des techniques de renseignement pour ses missions de lutte contre la fraude d'importance nationale et internationale ou d'une sensibilité particulière selon l'arrêté du 29 octobre 2007 portant création du service. De son côté, Tracfin est autorisé à recourir aux techniques de renseignement dans le cadre de la lutte contre la fraude fiscale, les circuits financiers clandestins, le blanchiment de capitaux et le financement du terrorisme conformément aux dispositions de l'article D. 561-33 du code monétaire et financier. Néanmoins, on remarquera que ce même article prévoit que Tracfin a pour mission de « *rechercher, collecter, exploiter et transmettre les renseignements mentionnés à l'article L. 811-2 du code de la sécurité intérieure, en sa qualité de service spécialisé de renseignement désigné par l'article R. 811-1 du même code* », ce qui nous semble superfétatoire au regard des dispositions du code de la sécurité intérieure voire contradictoire avec celles de l'article L. 811-3 du même code. Par ailleurs, on relèvera que Tracfin opère « *principalement en sources ouvertes et sur la base des déclarations de soupçons qui lui sont transmises* » et recourt « en priorité » aux techniques de renseignement impliquant les opérateurs numériques en matière de prévention du terrorisme¹.

¹ A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 73 ; P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 44 et suivantes.

Au sein des services du ministère de la défense, la DRSD doit pouvoir bénéficier des techniques de renseignement pour : « *réaliser les enquêtes administratives* » ; prévenir « *les atteintes à la défense nationale telles qu'elles sont définies par le code pénal et le code de justice militaire, notamment en mettant en œuvre des mesures de contre-ingérence pour s'opposer à toute menace pouvant prendre la forme d'activités de terrorisme, d'espionnage, de subversion, de sabotage ou de crime organisé* » ; protéger les « *personnes susceptibles d'avoir accès à des informations protégées ou à des zones, des matériels ou des installations sensibles* »¹. Quant à la DRM, elle devrait uniquement recourir aux techniques de renseignement utiles au renseignement d'intérêt militaire², c'est-à-dire essentiellement les mesures de surveillance internationale. On notera d'ailleurs que le service de renseignement militaire « *dispose d'un panel complet de capteurs (renseignement d'origine image, électromagnétique, cybernétique et humain) qui relèvent de ses moyens propres et de ceux des armées déployées sur les théâtres d'opérations* »³. Pour finir, la DGSE, qui collabore étroitement avec les services du renseignement intérieur, ne devrait également recourir qu'à des techniques de renseignement permettant « *de rechercher et d'exploiter les renseignements intéressant la sécurité de la France, ainsi que de détecter et d'entraver, hors du territoire national, les activités d'espionnage dirigées contre les intérêts français afin d'en prévenir les conséquences* »⁴. Autrement dit, la DGSE ne devrait pouvoir recourir aux techniques qu'à titre exceptionnel pour les besoins du renseignement extérieur, la DGSI étant le service assurant les mêmes missions sur le territoire national. En outre, rappelons qu'en matière de surveillance des communications internationales, seule la DGSE est compétente pour être autorisée à mettre en œuvre les interceptions⁵.

Par ailleurs, il convient de préciser que certains textes réglementaires ont exclu Tracfin de la liste des services spécialisés autorisés à recourir aux techniques

¹ Article D. 3126-6 du code de la défense.

² Articles D. 3126-10 et -11 du code de la défense.

³ A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 73 ; P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 44 et suivantes.

⁴ Article D. 3126-2 du code de la défense.

⁵ Cf. supra. §3 de la Section II du Chapitre I du Titre I de la Ière Partie.

de captation de sons, d'images et de données informatiques¹. De même, Tracfin et la DRM ne sont pas autorisés à procéder à des intrusions dans un véhicule ou lieu privé pour y introduire des dispositifs techniques de renseignement².

Dans les faits, la DGSJ, la DGSE et la DNRED sont les services qui sollicitent le plus d'autorisation et les demandes de la DRSD restent marginales en ce qui concerne les techniques les plus intrusives³.

Enfin, on rappellera que la jurisprudence du Conseil constitutionnel a clairement affirmé que le recours aux techniques de renseignement par les services du premier cercle relève uniquement de leurs missions de police administrative même si ces services disposent parfois d'une compétence judiciaire comme la DGSJ⁴. En revanche, l'élargissement des services du second cercle autorisés à recourir aux techniques de renseignement à des services judiciaires tend à brouiller la clarté de la distinction entre les polices administrative et judiciaire et n'est pas sans questionner sur les dérives d'une surveillance élargie potentiellement contraire à l'objectif poursuivi par l'article L. 811-4 et, plus généralement, à l'esprit de la loi du 24 juillet 2015.

2. L'élargissement des services du second cercle

Dans le prolongement des dispositions des articles L. 801-1 et L. 811-3, l'article L. 811-4 du code de la sécurité intérieure permet à d'autres services relevant de la tutelle des ministres de la défense, de l'intérieure, de la justice et de l'économie de recourir à certaines techniques de renseignement pour certaines finalités. Désignés par décret en Conseil d'Etat, pris après avis de la CNCTR, les services concernés composent le « second cercle » en participant ou en contribuant à la politique publique du renseignement.

L'article L. 811-4 pourrait être entendu comme une limitation à l'extension des techniques de renseignement aux services du second cercle en instaurant « *un principe de spécialité* »⁵. Cette interprétation limitative avait été affirmée par la

¹ Articles R. 853-1 et R. 853-2 du code de la sécurité intérieure.

² Article R. 853-3 du code de la sécurité intérieure.

³ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 72 et 73.

⁴ Décision n° 2015-713 DC du 23 juillet 2015 (considérants 9).

⁵ En ce sens, voir N. Catelan, *Les nouveaux textes relatifs au renseignement : un moindre mal*, op. cit..

DPR en 2015 qui s'était étonnée de la « *définition très large des services autorisés à recourir à des techniques de renseignement* » finalement retenue par l'exécutif¹.

En effet, le décret n° 2015-1639 du 11 décembre 2015 ne s'est pas contenté de désigner seulement les trois services participant directement à la politique publique du renseignement qui sont légitimement compétent pour mettre en œuvre des techniques de renseignement : le SCRT, la DRPP et le SDAO². Ces trois services ont été autorisés à mettre en œuvre la plupart des techniques de renseignement hormis les plus intrusives que sont les algorithmes et les sondes des articles L. 851-2 et L. 851-3 et pour les finalités 1°, 4°, 5° (a,b etc) ou 6° de l'article L. 811-3. Le texte a élargi le recours à certaines techniques à de nombreux services et offices judiciaires principalement pour les finalités de la prévention du terrorisme et de la lutte contre la criminalité organisée. Les techniques concernées sont essentiellement les accès aux données de connexion et la géolocalisation mais concernent parfois les interceptions de sécurité et les techniques de « IMSI-catcher » et de captation de sons, d'images et de données³. Se montrant critique envers le décret du 11 décembre 2015, la DPR avait alerté sur les risques d'un contournement de la procédure pénale dans la confusion des techniques d'enquête judiciaire et de renseignement et d'atteinte à la crédibilité des services du premier cercle ainsi que sur les risques d'erreurs dans la mise en œuvre des techniques par des services de sécurité ne disposant pas des compétences techniques requises⁴. A la lecture des dispositions de l'article L. 811-4, on concèdera que cet élargissement a été permis par le législateur qui a conféré un large pouvoir d'organisation au gouvernement⁵. Pour sa part, la CNCTR a souhaité limiter l'accès aux techniques de renseignement dans sa doctrine relative à ses avis portant sur l'application de l'article L. 811-4 en prenant en considération la part qu'occupe le renseignement dans les missions des services du second cercle et leur expertise

¹ Cf. J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 39.

² Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 36.

³ Cf. J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, Annexes 6 et 7, op. cit., p. 148 et suivantes.

⁴ Ibid., p. 39 et suivantes.

⁵ En ce sens, voir aussi M. -H. Gozzi, *Sed quis custodiet ipsos custodes ? À propos de la loi du 24 juillet 2015 relative au renseignement*, op. cit..

technique¹. Cependant, la doctrine de la CNCTR a pu se révéler parfois peu contraignante en pratique, notamment dans la montée en puissance du renseignement pénitentiaire.

Intégré dans le second cercle par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, les services de renseignement du ministère de la justice, le Bureau central du renseignement pénitentiaire (BCRP) et ses cellules interrégionales (CIRP), ont été autorisés par le décret n° 2017-36 du 16 janvier 2017, pour les finalités relatives à la prévention du terrorisme, à la criminalité organisée et pour les finalités spécifiques à la sécurité du milieu carcéral, à recourir aux mêmes techniques que pour le SCRT, la DRPP et le SDAO et notamment aux interceptions de sécurité via IMSI-catcher². Or, si la CNCTR n'a pas vu d'objection à l'intégration du renseignement pénitentiaire dans le second cercle, elle avait toutefois émis un avis défavorable sur la possibilité d'intercepter des communications par IMSI-catcher dans sa délibération n°3/2016 du 8 décembre 2016 sur le fondement de sa doctrine de 2015, ce qui n'a manifestement pas été suivi par le gouvernement³. Néanmoins, le législateur est à nouveau intervenu en 2017 pour définir plus restrictivement les techniques pouvant être utilisées par le renseignement pénitentiaire dans le cadre de ses missions relatives à la sécurité du milieu carcéral⁴. Dans ce cadre, les techniques autorisées se concentrent sur les accès aux données de connexion, la géolocalisation et les interceptions de sécurité, les interceptions par IMSI-catcher et les captations de sons, d'images et de données étant exclus⁵. En revanche, les délégations locales au renseignement pénitentiaire se sont vues reconnaître la possibilité de recourir aux techniques de renseignement mentionnées à l'article L. 855-1 sans que le décret n° 2017-749 du 3 mai 2017 relatif à leur désignation n'ait remis cette capacité en question alors que dans une délibération du 16 mars 2017 la CNCTR avait « *considéré que*

¹ Cf. CNCTR, Délibération n° 2/2015 du 12 novembre 2015.

² A ce sujet, voir P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 54 et suivantes.

³ Cf. CNCTR, *2^{ème} rapport annuel (2017)*, p. 27 et suivantes.

⁴ Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique.

⁵ Article L. 855-1 du code de la sécurité intérieure.

*l'expertise technique requise pour une mise en œuvre sûre du balisage (article L. 851-5 du code de la sécurité intérieure) et du recueil de données de connexion par IMSI catcher (article L. 851-6 du code de la sécurité intérieure) faisait obstacle à ce que cette mise en œuvre et même, dans le cas de la seconde technique, l'exploitation des données recueillies puissent être directement confiées aux délégations locales »¹. En outre, le décret n° 2019-1503 du 30 décembre 2019 portant notamment sur les compétences du nouveau Service national du renseignement pénitentiaire (SNRP) a maintenu la possibilité pour ce service de recourir aux interceptions par IMSI-catcher malgré l'avis défavorable de la CNCTR dans sa délibération n° 2/2019 du 4 juillet 2019. On relèvera tout de même que le gouvernement a suivi l'avis de la Commission sur la limitation des techniques pouvant être utilisées par le SNRP au titre de la finalité énoncée au 5° de l'article L. 811-3². On ajoutera que la loi n° 2019-222 du 23 mars 2019 a intégré les captations de paroles et d'images dans la liste des techniques de l'article L. 855-1. Cette extension a été validée par le Conseil constitutionnel dans sa décision du 21 mars 2019³, notamment en ce que les captations autorisées respectent un principe de surveillance ciblée des individus⁴. On précisera que le renseignement pénitentiaire a été autorisée, avec d'autres services considérés comme techniquement compétent par la CNCTR au regard de sa doctrine⁵, à recourir aux interceptions hertziennes de l'article L. 852-2 par le décret n° 2018-543 du 29 juin 2018⁶ et la loi du 30 décembre 2019. Si « *la société pénitentiaire est une société de surveillance* » selon l'ancien président de la CNCIS, Jean-Marie Delarue, ce dernier s'est montré très critique envers le renforcement des moyens techniques du renseignement pénitentiaire en dénonçant son inefficacité et son impact potentiellement négatif sur les relations entre les agents de l'administration pénitentiaire et les détenus⁷. Le Professeur Bertrand Warusfel a également relevé cette problématique de la conciliation entre « *les fonctions**

¹ Cf. CNCTR, 2^{ème} rapport annuel (2017), p. 33.

² Cf. CNCTR, 4^{ème} rapport annuel (2019), p. 20 et suivantes.

³ Cf. Décision n° 2019-778 DC du 21 mars 2019, *Loi de programmation 2018-2019 et de réforme de la justice*.

⁴ Cf. infra. §2 de la Section I du Chapitre I du Titre II de la Ière Partie.

⁵ Cf. CNCTR, Délibération n° 2/2018 du 17 mai 2018.

⁶ Cf. CNCTR, 3^{ème} rapport annuel (2018), p. 24 et suivantes.

⁷ Cf. J. -M. Delarue, *Le renseignement pénitentiaire*, Après-demain, 2018/1 (n° 45, NF), p. 7 à 9.

classiques des surveillants et les missions de renseignement » tout en soulignant l'émergence d'« *un renseignement intérieur hypertrophié interférant avec la pratique judiciaire* » dans la lutte contre la radicalisation violente¹.

En dehors du renseignement pénitentiaire, l'exécutif n'a cessé d'intégrer de nouveaux services ou offices judiciaires relevant du ministère de l'intérieur dans le périmètre du second cercle en accord avec les avis de la CNCTR². Si aucun incident n'est à déplorer dans l'usage des techniques par ses services, un certain « désordre » semble relancer les débats sur l'organisation de la communauté du renseignement, ce qui n'est pas sans questionner l'organisation du renseignement numérique lui-même. A titre d'exemple, on soulignera l'incohérence relevée par le Professeur Bertrand Warusfel sur la désignation de l'OFAST « *en tant que tel comme service de renseignement du second cercle* » par référence aux techniques³. En outre, l'intervention de la DGSJ comme « opérateur technique »⁴ pour les services du second cercle en matière d'IMSI-catching ou de captations de sons, d'images et de données pourrait atténuer la portée des dispositions de l'article L. 811-3. En effet, cette mutualisation technique entre le premier et le second cercle remet en cause la condition de la CNCTR relative à l'expertise technique des services pouvant être désignés en vertu de l'article L. 811-4 et risque d'entraîner des interférences de la DGSJ dans les opérations de surveillance des services du second cercle. Par ailleurs, on rappellera les risques d'un potentiel basculement des services judiciaires dans une logique de renseignement ou d'un renseignement « pré-judiciaire » en contradiction avec les exigences de la procédure pénale⁵.

Si le « rapport Larrivé » de juin 2020 n'avait pas estimé opportun ou nécessaire de revoir le périmètre de la communauté du renseignement⁶, il n'en

¹ Cf. B. Warusfel, *Justice et renseignement dans la lutte contre la radicalisation violente*, op. cit..

² Cf. CNCTR, *3^{ème} et 4^{ème} rapports annuels (2018-2019)*.

³ Cf. B. Warusfel, *Quelques réformes pour le droit du renseignement ?*, op. cit., p. 159.

⁴ Sur ce point, voir C. Cambon, *Rapport relatif à la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 73 à 75.

⁵ En ce sens, voir M. Touillier, *La loi sur le renseignement traduit-elle l'émergence d'une procédure « para-pénal » ?*, in *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, Janvier 2016, Nanterre, France, p. 159 à 176 ; J. Alix et O. Cahn, *Mutations de l'antiterrorisme et émergence d'un droit répressif de la sécurité nationale*, *Revue de Science Criminelle et de Droit Pénal Comparé*, Dalloz, 2018, p. 845.

⁶ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 63.

demeure pas moins que plusieurs propositions ont été émises. Ainsi, la DPR a recommandé de renforcer la mutualisation des techniques entre la DGSJ et les services du second cercle¹ et envisagé la création d'une nouvelle direction générale dédiée au renseignement territorial réunissant le SCRT, la SDAO et la DRPP, notamment pour améliorer le pilotage des moyens techniques². Ces propositions ne remettent pas en cause les deux cercles et les accès aux techniques de renseignement mais prolongent, selon nous, la confusion dans l'organisation du renseignement. De son côté, la CNCTR avait distingué dans sa doctrine de 2015 trois cercles : les services spécialisés, les autres services ayant des missions de renseignement à titre principal et les services et offices judiciaires qui devraient privilégier les techniques numériques d'enquête de police judiciaire. On retrouve cette distinction dans les recommandations du Professeur Bertrand Warusfel³. D'autres approches plus radicales peuvent être proposées comme la suppression pure et simple du second cercle ou encore ne retenir que les services les plus importants de ce dernier en les basculant dans le premier cercle afin de créer une communauté unique plus élargie.

Pour notre part, il conviendrait de revoir les règles d'organisation de la communauté du renseignement en révisant notamment les dispositions de l'article L. 811-4. En plus de conférer une large marge de manœuvre au gouvernement, le texte adopte une logique d'intégration des services du second cercle fondée sur l'accès aux techniques de renseignement et non sur leur participation à la politique publique du renseignement⁴, ce qui est de nature à entraîner des incohérences comme celle relative à l'OFAST. A notre sens, il serait préférable de distinguer la désignation des services pouvant intégrer le second cercle de l'accès aux techniques. En cohérence avec la doctrine de la CNCTR, le service souhaitant bénéficier des techniques de renseignement devrait être préalablement autorisé à intégrer le second cercle en fonction de ses missions

¹ Cf. C. Cambon, *Rapport relatif à la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 73 à 75.

² Cf. F. Dumas et F. -N. Buffet, *Rapport public relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 88.

³ Cf. B. Warusfel, *Quelques réformes pour le droit du renseignement ?*, op. cit., p. 160.

⁴ En ce sens, voir F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

pour la politique publique du renseignement pour ensuite être autorisé à accéder à certaines techniques selon son expertise technique et ses autres capacités légales d'enquêtes, notamment s'il s'agit d'un service judiciaire. Cette distinction dans les autorisations d'intégration au second cercle et d'accès aux techniques a une portée pratique : la première autorisation emporterait nécessairement le droit pour le service concerné de bénéficier des dispositions de l'article L. 822-3 du code de la sécurité intérieure relatives au partage des renseignements issues de la loi relative au renseignement de 2015, ce qui devrait être pris en considération dans la seconde autorisation d'accès aux techniques afin de déterminer si le jeu de la coopération inter-services n'est pas suffisant et la nécessité réelle du recours à la technique demandée.

Malgré les quelques limites des garanties relatives aux missions des services de renseignement, il nous semble important de rappeler que la précision des finalités et la délimitation des missions des services ont un rôle à jouer dans la limitation de la surveillance numérique et que les services ne sont effectivement pas restreints que par les limites technologiques. Plus encore, la philosophie du droit du renseignement français adhère à l'expression « la fin ne justifie pas tous les moyens » avec l'affirmation d'un certain nombre de garanties, dont le principe de proportionnalité, qui sont intrinsèques à la mise en œuvre des techniques numériques soumises à autorisation préalable¹.

§2. Les garanties intrinsèques aux techniques numériques de renseignement

Cinq principes consacrés par la loi relative au renseignement de 2015 sont généralement invoqués pour décrire les garanties applicables aux techniques numériques : la proportionnalité et la subsidiarité, l'individualisation, la centralisation et la territorialité². A ces principes, nous ajouterons deux règles de portée plus pratique : le contingentement des techniques et l'interdiction pour les services de renseignement de réaliser les opérations matérielles relatives à la mise en œuvre de techniques chez les opérateurs.

¹ En ce sens, voir J. -J. Urvoas, *Rapport sur le projet de loi relatif au renseignement*, op. cit., p. 41.

² A ce sujet, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 19 ; F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

A - Les principes de proportionnalité et de subsidiarité

Afin d'instituer un régime dérogatoire conforme aux exigences conventionnelles et constitutionnelles du droit au respect de la vie privée, le législateur a inscrit dans la loi les principes de proportionnalité et de subsidiarité. En effet, la jurisprudence de la CEDH exige que l'autorisation de mise en œuvre d'une mesure de surveillance se doit d'être proportionnée aux buts légitimes poursuivis, ce qui implique notamment de savoir s'il est possible d'atteindre les buts recherchés par des moyens moins intrusifs¹. On soulignera que la CEDH, elle-même, exerce un contrôle de proportionnalité sur les mesures de surveillance dont elle est saisie². De son côté, le droit de l'Union européenne affirme textuellement le respect du principe de proportionnalité à l'article 52 de la Charte des droits fondamentaux dans la limitation des droits et libertés protégés par le texte. Enfin, la jurisprudence du Conseil constitutionnel impose également le respect du principe de proportionnalité³, conduisant ainsi le juge constitutionnel à contrôler la conciliation opérée par le législateur entre le droit au respect de la vie privée et la sauvegarde de l'ordre public⁴. Dans ces considérations, les principes de proportionnalité et de subsidiarité ont été introduits dans le droit du renseignement à deux niveaux : dans l'autorisation de mise en œuvre des techniques de renseignement et dans leur contrôle. C'est ce qu'avait d'ailleurs relevé le Conseil constitutionnel dans sa décision du 23 juillet 2015 à propos du principe de proportionnalité⁵.

S'agissant de l'autorisation, l'article L. 801-1 du code de la sécurité intérieure impose expressément une obligation générale aux services de justifier la proportionnalité de la technique de renseignement concernée dans leur demande d'autorisation. Pour ce faire, les services peuvent s'appuyer sur la légistique de la loi du 24 juillet 2015 qui, en s'inspirant de l'arrêt *Uzun c. Allemagne* de la CEDH du 2 septembre 2010, a organisé une gradation entre les techniques selon leur degré d'intrusivité dans la vie privée avec une modulation des durées

¹ CEDH, 4 décembre 2015, *affaire Roman Zakharov c. Russie* (n° 47143/06).

² CEDH, 29 juin 2006, *affaire Weber et Saravia c. Allemagne* (n° 54934/00).

³ Décision n° 2003-467 DC, 13 mars 2003, *loi pour la sécurité intérieure*.

⁴ A ce sujet, voir P. Bas, *Rapport sur le projet de loi relatif au renseignement*, op. cit., p. 35.

⁵ Décision n° 2015-713 DC du 23 juillet 2015, *Loi relative au renseignement* (considérant 11).

d'autorisation maximum qui varient généralement entre quatre et deux mois¹. De manière générale, les techniques dans l'ordre sont : les accès aux données de connexion, les interceptions de sécurité et les captations de sons, d'images et de données ainsi que les pénétrations domiciliaires². Comme souligné par Floran Vadillo, « *le débat peut être ouvert* » sur l'ordonnancement des techniques tout en préconisant qu'« *il importerait de ne pas brouiller l'équilibre institué en 2015 en matière de proportionnalité des TR* »³. Nous nous accordons sur cette dernière préconisation afin d'éviter toute insécurité juridique dans l'application du principe de proportionnalité.

Pour ce qui concerne la subsidiarité, le principe n'est pas consacré de manière générale à la différence du principe de proportionnalité, ce qui amoindrit son importance. Il est matérialisé aux articles L. 853-1, L. 853-2 et L. 853-3 du code de la sécurité intérieure et donc seulement applicable aux techniques les plus intrusives de sonorisation, de captation d'images et de données et pour les pénétrations dans les lieux privés. Le principe suppose que ces techniques ne peuvent être mises en œuvre que lorsqu'il est impossible de recueillir les renseignements recherchés par un autre moyen légalement autorisé. Dans le cas particulier de l'article L. 853-3, il convient de préciser que les services sont contraints de justifier le respect du principe tant pour la mise en œuvre des techniques des articles L. 853-1 et L. 853-2 que pour l'introduction dans le lieu privé concerné⁴. On relèvera qu'une autre forme de subsidiarité a été introduite par la loi relative au renseignement du 30 juillet 2021. Selon l'article L. 852-3, il s'agit d'autoriser les services à recourir aux interceptions satellitaires que « *lorsque cette interception ne peut être mise en œuvre sur le fondement du I de l'article L. 852-1 du présent code, pour des raisons techniques ou pour des motifs de confidentialité faisant obstacle au concours des opérateurs ou des personnes*

¹ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, Annexe 7, op. cit., p. 212.

² Sur ce point, voir F. Vadillo, *Quand l'Etat de droit rencontre l'Etat secret : cadre et garanties du recours aux techniques de recueil de renseignement*, *Le droit du renseignement*, op. cit., p. 95.

³ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

⁴ A ce sujet, voir P. Bas, *Rapport sur le projet de loi relatif au renseignement*, op. cit., p. 94.

mentionnés à l'article L. 851-1 »¹. On remarquera, ici, une certaine inversion de la portée protectrice du principe de subsidiarité. Alors que le principe consacré aux articles L. 853-1 à L. 853-3 vise à protéger le droit au respect à la vie privée, le motif de subsidiarité relatif à la confidentialité de l'article L. 852-3 vise, quant à lui, à protéger les services.

Concernant le contrôle, l'article L. 801-1 charge la CNCTR, dans son contrôle *a priori* et *a posteriori*, et le Conseil d'Etat, en cas de recours, d'assurer le respect du principe de proportionnalité. Le contrôle sera plus grand lorsqu'il concerne les techniques soumises au principe de subsidiarité. De manière générale, la CNCTR prend en considération « *les règles et principes posés par la loi, ceux définis par la jurisprudence, notamment celle du Conseil d'État statuant au contentieux, et ceux fixés par les formations plénière et restreinte de la commission* » pour apprécier le respect du principe de proportionnalité². Dans le cadre de son contrôle *a priori* des demandes d'autorisation, la CNCTR vérifie si l'atteinte à la vie privée résultant de la technique demandée est proportionnée « *à la menace décrite, aux enjeux concernés et aux informations recherchées* » et, le cas échéant, si « *aucun autre moyen moins intrusif ne permettrait de recueillir les informations recherchées* »³.

Si la CNCTR doit assurer le respect du principe de proportionnalité selon les termes de l'article L. 801-1, il reste qu'elle a volontairement réduit son contrôle de proportionnalité des demandes d'identification d'abonnées ou de recensement de numéros d'abonnement au profit d'un simple contrôle de l'erreur manifeste d'appréciation, considérant ces demandes comme faiblement intrusives. La CNCTR avait même proposé de confier ce type de contrôle au GIC en raison de sa « faible valeur ajoutée »⁴. Cette proposition, qui n'a pas été retenue, et la doctrine de la CNCTR nous interroge sur leur conformité aux dispositions de l'article L. 801-1 qui pourraient s'interpréter comme une obligation d'assurer à chaque instant du contrôle le respect de la proportionnalité. A notre sens, le texte doit pouvoir laisser

¹ Cf. CNCTR, Délibération n° 3/2021 du 14 avril 2021 ; R. Gauvain et L. Kervran, *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, op. cit., p. 79.

² Article 16 du règlement intérieur de la CNCTR (Délibération n° 2/2017 du 23 mars 2017).

³ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 95.

⁴ Cf. CNCTR, 3^{ème} rapport annuel (2018), p. 48 et 49.

une certaine marge d'appréciation à l'autorité de contrôle pour concilier les réalités opérationnelles avec l'exigence de proportionnalité. En revanche, la proposition relative au GIC nous semble peu recommandable en raison du manque d'indépendance du service qui relève du Premier ministre bien qu'il dispose de compétences juridiques. Enfin, il conviendrait de souligner, au regard de cette réduction du contrôle *a priori*, qu'il ne faudrait pas faire du principe de proportionnalité un principe évanescent redouté par la Professeure Raphaële Parizot¹.

Malgré cette légère atténuation du respect du principe de proportionnalité, ce dernier reste contrôlé par la CNCTR durant et après la mise en œuvre des techniques de renseignement. D'ailleurs, on notera que les contrôles sur pièces et sur place de la CNCTR lui permettent « *de mieux comprendre les raisons motivant l'emploi de certaines techniques et, partant, de mieux apprécier la proportionnalité, voire la subsidiarité de leur mise en œuvre* »². Le respect des principes de proportionnalité et de subsidiarité est donc au cœur des échanges entre l'autorité de contrôle et les services. On soulignera également que les services sont eux-mêmes soucieux du respect de ces principes en interrogeant la CNCTR sur le caractère approprié du recours à une technique dans le cadre d'un projet de surveillance et on saluera, dans ce cas, la retenue des membres de la Commission qui « *se gardent de toute appréciation de fond tant qu'une demande d'autorisation n'est pas soumise à la CNCTR* »³

En plus d'affirmer que la « la fin ne justifie pas tous les moyens » à travers les principes de proportionnalité et de subsidiarité, le droit du renseignement français adhérerait à la philosophie de la surveillance ciblée des individus par l'application d'un principe d'individualisation des techniques de renseignement.

¹ Cf. R. Parizot, *Surveiller et prévenir... à quel prix ?*. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, op. cit..

² Cf. CNCTR, 2^{ème} rapport annuel (2017), p. 57.

³ Cf. CNCTR, 5^{ème} rapport annuel (2020), p. 57.

B - Le principe d'individualisation ou la surveillance ciblée des individus

Avec les développements des technologies numériques, on distingue communément deux types de surveillance : la surveillance ciblée qui « *présuppose l'existence de la suspicion préalable d'un individu ou d'une organisation ciblée* » et la surveillance non ciblée qui « *commence sans suspicion préalable ou cible spécifique* »¹. Cette dernière est parfois qualifiée de « surveillance stratégique » consistant à rassembler, sur le long terme, de nombreux renseignements numériques (contenus des communications et métadonnées) « *sur un phénomène ou bien sur une personne ou un groupe de personnes donné* » sans que la surveillance ne soit « *forcément déclenchée sur la base d'un soupçon à l'encontre d'une personne ou plusieurs personnes* » et de manière proactive, c'est-à-dire afin de détecter un danger encore inconnu. Plus encore, la surveillance non ciblée ou stratégique est associée à la « surveillance de masse » qui se traduit par la collecte massive et indifférenciée de données portant sur de nombreuses personnes². Il convient de préciser que la surveillance ciblée ou la surveillance de masse ne constituent pas des notions juridiques. Néanmoins, elles ont été reconnues et admises en droit européen. En revanche, le droit du renseignement français a nettement pris parti pour n'autoriser légalement que des techniques de numériques de surveillance ciblée même si certaines mesures font figure d'exception.

1. La reconnaissance de la surveillance ciblée et non ciblée en droit européen

Selon la jurisprudence de la CEDH, le caractère massif d'une surveillance numérique ne constitue pas une violation en lui-même du droit au respect de la vie privée³. La Cour laisse donc une marge d'appréciation aux Etats⁴ dans le choix

¹ A ce sujet, voir European Union Agency for Fundamental Rights, *Surveillance by intelligence services : fundamental rights safeguards and remedies in the EU* - Volume II: field perspectives and legal update, 20 octobre 2017, p. 32.

² Sur ce point, voir Conseil de l'Europe, *Surveillance de masse. Quel contrôle démocratique ?*, Conseil de l'Europe, « Hors collection », 2016,, 2016, p. 63 à 109.

³ Cf. CNCTR, *3^{ème} rapport annuel (2018)*, p. 103.

⁴ CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, req. n° 58170/13, 62322/14 et 24960/15 et *Centrum för Rättvisa c. Suède*, req. n° 35252/08.

du type de surveillance tout en contrôlant, au cas par cas, les garanties légales contre l'arbitraire et les abus¹. Dans le cadre de sa compétence, la CJUE s'est pour sa part opposée, en principe, à une conservation généralisée et indifférenciée des données personnelles mais a toutefois admis ce type de conservation lorsque l'« *État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible* » ou concernant les adresses IP lorsqu'elle est limitée dans le temps ainsi qu'une conservation ciblée et rapides des données également limitées dans le temps pour les besoins de la sécurité publique². En matière de renseignement d'Etat, le droit européen n'interdit donc pas la surveillance numérique de masse et ne privilégie pas nécessairement la surveillance ciblée à la différence du droit du renseignement français qui nous semble alors plus restrictif.

2. L'affirmation d'une surveillance ciblée en droit du renseignement français

Sans formellement consacrer de dispositions spécifiques à la surveillance ciblée, la loi du 24 juillet 2015 relative au renseignement a clairement introduit une procédure d'autorisation préalable des techniques de renseignement qui, au cas par cas selon l'article L. 821-2 du code de la sécurité intérieure, « *oblige les services de renseignement à cibler précisément leurs demandes de surveillance d'individus suspectés de représenter une menace* », le législateur ayant d'ailleurs refusé de permettre la surveillance d'une « *liste d'individus soupçonnés de préparer des attentats* » dans le cadre des accès aux données de connexion en temps réel prévus à l'article L. 851-2³. Comme le souligne Floran Vadillo, l'individualisation des techniques de renseignement limite ainsi la surveillance à une personne soupçonnée de représenter une menace et à son entourage, « *lorsque celui-ci sert d'écran* »⁴. On rappellera que la notion d'entourage cible des personnes

¹ Sur ce point, voir M. -C. de Montecler, *La CEDH admet le principe de la surveillance électronique de masse*, AJDA 2021, p. 1060.

² CJUE, 6 octobre 2020, *affaire C-623/17 Privacy International et affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, French Data Network e.a., ainsi que C-520/18 Ordre des barreaux francophones et germanophone e.a.*

³ A ce sujet, voir *Renseignement, La loi n° 2015-912 du 24 juillet 2015 relative au renseignement, 3 questions à Jean-Jacques Urvoas, député (PS) du Finistère, président de la commission des lois de l'Assemblée nationale*, Entretien, Communication Commerce électronique n° 10, Octobre 2015, entretien 9.

⁴ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

soupçonnées de fournir des informations relatives à la mesure de surveillance initiale et qu'elle exclue, en principe, une surveillance élargie à des individus totalement étrangers à la demande d'autorisation¹. Si l'affirmation d'une surveillance ciblée se déduit aisément des dispositions procédurales de la loi relative au renseignement de 2015, il reste que certaines techniques de renseignement constituent des mesures de surveillance de masse.

3. Les atténuations au principe d'individualisation

Parmi les techniques de renseignement pouvant être autorisées sur le territoire national, le recours à des algorithmes de détection des menaces terroristes et à des dispositifs d'IMSI-catching ont pu « *donner l'impression de favoriser le développement d'une surveillance de masse déclenchée par une autorité politique* »². Il est vrai que la mise en œuvre d'algorithmes sur les réseaux des opérateurs s'affranchit du principe d'individualisation au profit d'une analyse ou recherche « indifférenciée et tous azimuts » des données de connexion³. Bien qu'il ait pu être soutenu qu'il s'agit d'« *un outil de détection ciblé – et non de surveillance* »⁴ ou que la loi française n'autorise que de la « collecte de masse »⁵, il n'en demeure pas moins que l'outil technique autorisé par l'article L. 851-3 surveille les données de connexion d'individus non préalablement soupçonnés de représenter une menace afin justement de détecter une menace terroriste encore inconnue des services, ce qui correspond à la surveillance de masse ou stratégique. Pour autant, le Conseil constitutionnel a validé, sans réserve d'interprétation, le régime juridique des algorithmes en estimant que les atteintes au droit au respect de la vie privée n'étaient pas manifestement disproportionnées⁶.

¹ Sur la notion d'entourage, voir notamment CNCTR, *8^{ème} rapport d'activité (2023)*, p. 117 à 132.

² En ce sens, voir X. Latour, *La loi relative au renseignement : un État de surveillance ?*, op. cit..

³ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit. ; Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement : la CNIL publie ses avis | CNIL (<https://www.cnil.fr/fr/projet-de-loi-relatif-la-prevention-dactes-de-terrorisme-et-au-renseignement-la-cnil-publie-ses-avis>).

⁴ A ce sujet, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 189.

⁵ Sur ce point, voir W. Mastor, *La loi sur le renseignement du 24 juillet 2015, La France, Etat de surveillance ?*, AJDA 2015, p. 2018.

⁶ Décision n° 2015-713 DC du 23 juillet 2015 (considérant 58 à 60).

En outre, on soulignera que la CJUE, dans l'arrêt *La Quadrature du Net* du 6 octobre 2020, a considéré que la surveillance algorithmique constitue une ingérence « particulièrement grave » dans les droits fondamentaux sans pour autant formellement l'interdire en matière de sécurité nationale et de renseignement anti-terroriste lorsque le dispositif est suffisamment fiable et non-discriminatoire et si ces critères font l'objet d'un contrôle contraignant¹. Hormis la problématique du contrôle, le Conseil d'Etat a confirmé le respect des critères dégagés par la CJUE par les dispositions de l'article L. 851-3². A la lecture de la jurisprudence, une surveillance de masse algorithmique est donc juridiquement affirmée en France, son contrôle constituant alors un véritable défi pour la CNCTR³.

S'agissant du recours au IMSI-catcher, ce dispositif a suscité des craintes d'une surveillance ciblée techniquement impossible⁴. En effet, le dispositif offre la possibilité de capter les données de connexion et les correspondances de manière indiscriminée de l'ensemble des terminaux situés dans son périmètre d'action, ce qui « suppose un niveau d'expérience et de technicité très élevé » selon la CNCTR qui a rappelé que le législateur avait souhaité autoriser cette technique de façon exceptionnelle⁵. Afin d'éviter que les services généralisent l'utilisation de ce dispositif et de garantir le principe d'individualisation ainsi que la proportionnalité, il a été donc décidé de réduire le délai d'autorisation de mise en œuvre (deux mois en matière de données de connexion et 48 heures en matière d'interceptions), d'imposer la destruction des données recueillies dès qu'elles apparaissent sans lien avec l'autorisation et de continger le nombre maximal d'appareils et d'autorisations pouvant être simultanément en vigueur. En matière d'interception, l'autorisation de recourir au IMSI-catcher a été notamment limitée

¹ A ce sujet, voir W. Maxwell, *La CJUE dessine le noyau dur d'une future régulation des algorithmes*, op. cit..

² Conseil d'Etat, 21 avril 2021, *La Quadrature du Net*, requête n° 393099 (considérants 75 à 77).

³ Voir à ce sujet C. Lazerges et H. Henrion-Stoffel, *Politique criminelle, renseignement et droits de l'homme, A propos de la loi du 24 juillet 2015 relative au renseignement*, op. cit..

⁴ En ce sens, voir P. Achilleas et L. Binet Idest, *Un an de régulation du marché des communications électroniques*, Communication Commerce électronique n° 5, mai 2016, chron. 7.

⁵ Cf. CNCTR, 2^{ème} rapport annuel (2017), p. 28.

que pour certaines finalités¹. Ces restrictions ont pu être remises en cause par Floran Vadillo qui proposait « *d'aligner l'usage de l'IMSI-catcher sur les autres techniques au regard de son ingérence dans la vie privée de même intensité* », tout en élargissant la technique à l'ensemble des finalités de l'article L. 811-3 pour les interceptions de correspondance sous réserve du respect d'une subsidiarité par rapport à la collecte réalisable via les opérateurs². A notre sens, ces propositions ne semblent pas remettre en question les principes de proportionnalité et d'individualisation puisque la destruction des données non pertinentes et le contingentement subsistent. En revanche, elles impliqueraient un assouplissement des conditions légales et, par là même, un contrôle plus attentif de la CNCTR qui serait également chargé d'assurer le respect du principe de subsidiarité. Or, que ce soit dans le cadre des conditions en vigueur ou de celles de Floran Vadillo, le contrôle de la CNCTR nous semble être l'élément crucial pour empêcher la mise en œuvre d'opérations de surveillance de masse par IMSI-catcher contraire au principe d'individualisation. Cette dernière remarque vaut également pour les nouvelles interceptions satellitaires autorisées par la loi relative au renseignement du 30 juillet 2021³ dont l'application du principe d'individualisation serait opérée *a posteriori* au sein du GIC⁴.

Par ailleurs, le régime des mesures de surveillance des communications internationales introduit par la loi du 30 novembre 2015 adopte une logique de surveillance stratégique en permettant notamment l'interception massive des communications sur des réseaux visés et l'exploitation non individualisée des données de connexion ainsi que des « vérifications ponctuelles » pour la détection de certaines menaces⁵. En revanche, une certaine surveillance hybride à la fois stratégique et ciblée trouve à s'appliquer pour l'exploitation des correspondances ou des données de connexion qui peuvent concerner des zones géographiques ou

¹ Les finalités sont celles mentionnées aux 1° et 4° et a du 5° de l'article L. 811-3 du code de la sécurité intérieure.

² Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

³ Article L. 852-3 du code de la sécurité intérieure.

⁴ Cf. supra. §1 de la Section II du Chapitre I du Titre I.

⁵ Cf. supra. §3 de la Section II du Chapitre I du Titre I.

des organisations, des groupes de personnes ou des personnes¹. Comme pour les algorithmes, l'atténuation du principe d'individualisation n'a pas été questionnée par le Conseil constitutionnel qui a considéré que les mesures de surveillance ne portent pas d'atteinte manifestement disproportionnée au droit au respect de la vie privée en ce que « *le législateur a précisément défini les conditions de mise en œuvre de mesures de surveillance des communications électroniques internationales, celles d'exploitation, de conservation et de destruction des renseignements collectés ainsi que celles du contrôle exercé par la commission nationale de contrôle des techniques de renseignement* »². De même, il se pourrait que la CEDH adopte la même solution que le Conseil constitutionnel au regard de sa jurisprudence *Big Brother Watch et autres c. Royaume-Uni*³.

4. La portée limitée du principe d'individualisation

Enfin, on remarquera que si la loi place implicitement le principe d'individualisation au cœur de la procédure d'autorisation de « droit commun » de mise en œuvre des techniques de renseignement, il ressort de la jurisprudence nationale et internationale que ce principe ou la distinction entre surveillance ciblée et surveillance de masse ne constitue pas une garantie autonome et déterminante de la légalité des mesures de surveillance. Nos observations conduisent à conclure que l'individualisation des techniques de renseignement constitue davantage un critère renforçant le respect du principe de proportionnalité. Il en va de même pour les principes suivants de centralisation, de territorialité, de contingentement et de séparation dans les opérations matérielles qui permettent d'éviter opérationnellement les abus et dérives des services de renseignement et donc la proportionnalité du régime de surveillance.

¹ Article L. 854-2-III du code de la sécurité intérieure.

² Décision n° 2015-722 DC du 26 novembre 2015 (considérants 15).

³ En ce sens, voir M. -C. de Montecler, *La CEDH admet le principe de la surveillance électronique de masse*, op. cit..

C - La centralisation de l'exécution des techniques de renseignement

Considéré par les parlementaires¹ et la doctrine² comme un principe déterminant pour le contrôle effectif des techniques de renseignement ou, plus modestement selon le Conseil constitutionnel, comme un principe permettant de faciliter le contrôle de la CNCTR³, le principe de centralisation est essentiellement applicable aux renseignements collectés selon l'article L. 822-1 du code de la sécurité intérieure⁴. Pour autant, on retrouve ce principe en amont : d'abord avec la centralisation de l'ensemble des demandes relatives aux techniques de renseignement auprès du GIC qui est chargé de les transmettre pour avis à la CNCTR puis au Premier ministre⁵ ; ensuite, lors de l'exécution des techniques de renseignement. Le premier cas n'appelle pas de remarques particulières, hormis qu'il permet « *de pouvoir détecter d'éventuels doublons et de vérifier la réalité effective de la coopération interservices sur des thématiques communes ou connexes* »⁶. En revanche, il convient de préciser davantage l'application du principe de centralisation dans le second cas.

En effet, rappelons que la loi n° 91-646 du 10 juillet 1991 avait centralisé l'exécution des interceptions de sécurité au GIC, qui est un « service neutre »⁷, afin de procéder à une distinction entre le « service demandeur » et le « service collecteur ». Si cette distinction a été conservée avec la centralisation de l'exécution des techniques de recueils des données de connexion, de géolocalisation et des interceptions de sécurité chez les opérateurs⁸, il reste que la mise en œuvre des autres techniques consacrées depuis la loi relative au

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 42.

² Voir notamment C. Lazerges et H. Henrion-Stoffel, *Politique criminelle, renseignement et droits de l'homme, A propos de la loi du 24 juillet 2015 relative au renseignement*, op. cit. ; F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

³ Décision n° 2015-713 DC du 23 juillet 2015, Loi relative au renseignement (considérant 67).

⁴ Cf. infra. §3 de la Section I du Chapitre I du Titre II.

⁵ Sur ce point, voir J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 36 et 37.

⁶ A ce sujet, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 75 à 77.

⁷ Sur ce point, voir C. Lazerges et H. Henrion-Stoffel, *Politique criminelle, renseignement et droits de l'homme, A propos de la loi du 24 juillet 2015 relative au renseignement*, op. cit..

⁸ Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 76.

renseignement de 2015 sont directement opérées par les services¹. Une nouvelle distinction apparaît entre les techniques centralisées et les techniques décentralisées qui est de nature à atténuer le principe de centralisation. En outre, la décentralisation de certaines techniques de renseignement n'est pas sans soulever la question de la remise en cause de l'effectivité du contrôle. Bien que la loi ait introduit une atténuation au principe de centralisation dans l'exécution des techniques, il reste qu'elle exige une traçabilité des opérations et la centralisation des données recueillies même pour les techniques décentralisées². Enfin, on soulignera que le maintien de la centralisation auprès du GIC de l'exécution des techniques nécessitant l'intervention des opérateurs constitue toujours une garantie pertinente contre les risques d'abus ou de dérives dans la collaboration entre les services de renseignement et les acteurs du numérique.

D - Le principe de territorialité

Principe fondamental de l'encadrement des techniques de renseignement promu par le législateur en 2015, le principe de territorialité est l'application d'un critère géographique pour différencier « *les mécanismes d'autorisation et de contrôle selon que la technique vise ou non une surveillance nationale* »³.

C'est ainsi que les garanties de loi du 24 juillet 2015 relative au renseignement ne s'appliquent qu'aux techniques de renseignement mises en œuvre sur le territoire national⁴ et que la loi du 30 novembre 2015 est venue encadrer, dans des conditions moins rigoureuses, la surveillance des communications internationales. Autrement dit, les personnes surveillées bénéficient des différentes garanties des lois sur le renseignement en fonction de leur localisation ou de la localisation de leurs communications sur le territoire national ou à l'étranger, peu importe leur nationalité ou leur statut de résident ou d'étranger. Rappelons que cette approche se distingue nettement de l'approche américaine qui opère une discrimination entre les « USPER » (citoyens et résidents

¹ En ce sens, voir P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 67.

² Cf. infra. §3 de la Section I du Chapitre I du Titre II.

³ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 46.

⁴ Articles L. 801-1, L. 821-1 et L. 833-1 du code de la sécurité intérieure.

américains) et les « non-USPER » (les étrangers) dans les garanties applicables aux mesures de surveillance des communications situées à l'étranger¹.

Le principe de territorialité en vigueur nous semble suffisamment protecteur pour les libertés et conforme à la vocation universelle de la Déclaration des Droits de l'Homme et du Citoyen de 1789² qui constitue le fondement textuel de valeur constitutionnelle du respect du droit à la vie privée. Néanmoins, il a été tout de même proposé de compléter le critère géographique en matière de surveillance nationale. Dans le prolongement d'un amendement supprimé en 2015, Floran Vadillo a préconisé de favoriser « *l'application de la loi renseignement aux personnes de nationalité française ou résidant habituellement sur le territoire national* »³. Si l'auteur considère que cette solution suit la logique du régime dérogatoire du droit des étrangers et qu'elle permettrait de « *faciliter les opérations de contre-espionnage sur le territoire national* », il n'en demeure pas moins qu'elle constituerait une régression de la situation des étrangers déjà très critiquée par le Défenseur des droits⁴ et qu'elle soulève la question du régime applicable. En effet, selon la proposition de Floran Vadillo, les mesures de surveillance nationale visant des étrangers ne seraient pas soumises au contrôle *a priori* de la CNCTR. Dans ces conditions, il serait donc logique de rapprocher la surveillance des étrangers situés en France au régime de la surveillance internationale dont la loi du 30 novembre 2015 ne prévoit pas, en principe, d'avis préalable de la CNCTR, même si la proposition de Floran Vadillo ne formalise par ce rapprochement. Cette position renvoi d'ailleurs à la modification opérée par la loi de programmation militaire du 13 juillet 2018 à l'article L. 854-2-V avec la possibilité d'exploiter les données interceptées dans le cadre de la surveillance internationale pour la surveillance d'une personne située sur le territoire national⁵.

¹ Cf. supra. §3 de la Section II du Chapitre I du Titre I.

² En ce sens, voir J. Morange, « *La Déclaration et la proclamation des droits de l'homme* », Jean Morange éd., *La Déclaration des Droits de l'Homme et du Citoyen*. (26 août 1789). Presses Universitaires de France, 2002, pp. 11-54.

³ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

⁴ Cf. Le Défenseur des droits, *Les droits fondamentaux des étrangers en France*, mai 2016, p. 6.

⁵ Cf. supra. §3 de la Section II du Chapitre I du Titre I.

Cependant, il convient d'observer qu'une telle évolution irait à contre-courant des évolutions du droit du renseignement puisque la CNCTR exerce désormais un contrôle *a priori* des autorisations d'exploitation prévues au III et V de l'article L. 854-2¹. En outre, on relèvera que l'atténuation portée par l'article L. 854-2-V au principe de territorialité s'est accompagnée de l'application des garanties rigoureuses de la surveillance nationale. Par ailleurs, la position préconisée par Floran Vadillo pourrait avoir pour effet de remettre en cause non seulement le principe de territorialité retenu par la loi du 30 novembre 2015 mais également la définition de la surveillance internationale en droit français. Alors que la loi du 30 novembre 2015 s'inscrit dans « *la surveillance des activités qui se déroulent hors du territoire national que celle-ci soit réalisée depuis le territoire national ou à l'extérieur de celui-ci* », la proposition de Floran Vadillo peut s'interpréter dans le sens de la définition de la surveillance internationale selon laquelle il s'agit « *de la surveillance des activités conduites par des ressortissants étrangers ou pour le compte de puissances étrangères qu'elle se déroule sur le territoire national ou à l'étranger* »². Pour finir, l'établissement d'une discrimination entre les personnes de nationalité française ou résidant habituellement sur le territoire national et les étrangers dans les mesures de surveillance constituerait un rapprochement avec le droit américain.

E - Le contingentement des techniques

Au sens large, le contingentement peut être entendu comme une limitation des services autorisés à utiliser les techniques de renseignement et du nombre de techniques qui peuvent être déployées ainsi que des durées maximales de mise en œuvre de ces dernières et de conservation des données³. Dans le cadre de notre étude, le contingentement des services renvoi à la délimitation de leurs missions précédemment évoquées. S'agissant du contingentement des délais, il s'agit d'une condition directement rattachée au principe de proportionnalité pour apprécier le

¹ En dehors de la loi, la CNCTR s'était vue étendre son pouvoir de contrôle *a priori* aux autorisations prévues au III de l'article L. 854-2 par deux délibérations classifiées adoptées en formation plénière les 28 avril et 19 mai 2016 (cf. CNCTR, 1^{er} rapport annuel (2015-2016), p. 45 et 46). Par la suite, la loi de programmation militaire du 13 juillet 2018 a consacré dans la loi l'extension du contrôle de la CNCTR.

² Sur ce point, voir J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 47.

³ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

niveau d'ingérence dans la vie privée. Ainsi, nous ne retiendrons, ici, qu'une interprétation restrictive du contingentement des techniques qui, telle qu'il ressort des termes des lois sur le renseignement et de la jurisprudence constitutionnelle, correspond à la limitation du nombre maximal d'autorisations simultanées de mise en œuvre d'une technique de renseignement.

Initialement instauré pour les interceptions de sécurité en 1960 par décision du Premier ministre, le contingentement du nombre maximal d'interception pouvant être réalisées simultanément répondait aux contraintes techniques d'enregistrement des conversations sur des magnétophones avant d'être consacré dans la loi du 10 juillet 1991 comme une règle incitant les services à interrompre les interceptions inutiles afin d'en demander de nouvelles et à ne recourir à cette technique que de manière exceptionnelle¹. Fixé par arrêté du Premier ministre, le contingentement qui portait sur les moyens de communications ciblés a dû être régulièrement augmenté pour faire face à la multiplication de ces derniers jusqu'à ce que la CNCIS décide en 2008 de redéfinir le contingentement « *comme le nombre maximal de personnes cibles, et non plus comme celui des lignes téléphoniques – ou autres moyens de correspondance – placées sous écoute* »². Autrement dit, une autorisation d'interception concerne l'ensemble des moyens de communication d'une personne ciblée, ce qui devait permettre d'éviter l'augmentation continue du contingent. Si cette solution avait pour effet d'augmenter le nombre de moyens de communications pouvant être surveillés, une augmentation continue du quota d'interceptions pouvait entraîner une remise en cause de l'effectivité du contingentement comme une garantie pour les libertés publiques. Pourtant, on relèvera que le contingent des interceptions n'a cessé d'augmenter tout comme ceux qui ont été mis en place par les lois sur le renseignement depuis 2015 pour d'autres techniques de renseignement. Selon la CNCTR, ces augmentations demeurent raisonnées et équilibrées, les contingents étant régulièrement atteints ou disproportionnés au regard des finalités de la technique concernée³. Pour notre part, cette progression ne doit pas occulter le

¹ Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 70.

² A ce sujet, voir J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 21 et 22.

³ Cf. CNCTR, *4^{ème} rapport annuel (2019)*, p. 33 et suivantes.

renforcement du contingentement en tant que garantie du respect au droit à la vie privée.

Tout d'abord, la loi du 24 juillet 2015 relative au renseignement a soumis l'arrêté du Premier ministre de fixation du contingentement à un avis préalable de la CNCTR afin que cette dernière puisse contrôler la progression des contingents au regard du droit au respect à la vie privée¹. En outre, la loi de 2015 a étendu la règle au recueil de données de connexion par IMSI-catcher². A ce sujet, on remarquera que la loi de 2015 a consacré une deuxième définition du contingentement selon laquelle il s'agit du nombre maximal d'appareils ou de dispositifs techniques pouvant être utilisés simultanément. Toutefois, à la lecture des dispositions de la loi, il semblerait que cette seconde définition se confonde avec celle retenue pour les interceptions de sécurité puisque l'autorisation prévue à l'article L. 851-6 ne vaut que pour l'utilisation d'un seul IMSI-catcher³.

Ensuite, le contingentement a été élevé par le Conseil constitutionnel⁴ « *parmi les garanties essentielles permettant d'opérer une conciliation équilibrée entre la prévention des atteintes à l'ordre public et le respect du droit à la vie privée* » dans l'extension des techniques de renseignement à l'entourage⁵. Suite à cette décision, non seulement le législateur est contraint de prévoir un contingentement en cas d'extension d'une technique à l'entourage mais il a également étendu la règle à l'exploitation des correspondances des communications internationales de l'article L. 854-2-V, aux autorisations de recourir aux techniques des articles L. 852-2 et L. 853-1 dans le cadre de la surveillance pénitentiaire⁶ et aux

¹ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 42.

² Article L. 851-6 du code de la sécurité intérieure.

³ Notons que la CNCTR souligne que « *le recueil de données de connexion par IMSI-catcher fait partie des techniques de renseignement soumises au principe de contingentement en application duquel le nombre d'autorisations de mise en œuvre simultanément en vigueur ne peut excéder un maximum fixé par décision du Premier ministre après avis de la CNCTR* » (CNCTR, 5^{ème} rapport annuel (2020), p. 18).

⁴ Décision n° 2017-648 QPC du 4 août 2017, *La Quadrature du net et autres*.

⁵ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 65.

⁶ Article L. 855-1 du code de la sécurité intérieure.

interceptions satellitaires¹ afin de garantir au mieux l'individualisation des techniques et leur proportionnalité.

F - L'interdiction pour les services de réaliser les opérations matérielles de mise en œuvre des techniques chez les opérateurs

Le législateur de 2015 a affirmé une séparation dans les opérations matérielles nécessaires à la mise en place des techniques de renseignement mentionnées aux articles L. 851-1 à L. 851-4, L. 851-6, L. 852-1 et L. 853-2 du code de la sécurité intérieure en disposant que seuls des agents qualifiés des opérateurs peuvent effectuer ces opérations dans les installations de ces derniers sur ordre du Premier ministre². Autrement dit, la loi interdit aux services de renseignement d'installer directement leurs outils de surveillance dans les infrastructures des opérateurs. Quasiment absent dans la littérature juridique, cette interdiction nous semble pourtant constituer une garantie juridique et opérationnelle essentielle contre les risques d'écoutes sauvages et d'abus et dérives dans les relations entre les services et les opérateurs. D'ailleurs, le Conseil constitutionnel n'a pas manqué de rappeler la séparation opérée par le législateur dans les dispositions de l'article L. 871-6 du code de la sécurité intérieure dans sa décision n° 2015-713 DC du 23 juillet 2015 (considérant 51).

Notons que si l'interdiction en question est une garantie consacrée par la loi contre les dérives des services de renseignement, les dispositions réglementaires³ garantissent inversement à ces derniers que les opérateurs et leurs agents qualifiés assurent correctement les opérations matérielles nécessaires dans le respect de la réglementation relative au secret de la défense nationale⁴. Pour assurer le plus de clarté possible pour les opérateurs, il est prévu que l'ordre indique « *tous les éléments d'identification permettant de mettre en œuvre les techniques de renseignement conformément à l'autorisation accordée par*

¹ Article L. 852-3 du code de la sécurité intérieure.

² Article L. 871-6 du code de la sécurité intérieure.

³ Articles R. 872-1 à R. 872-6 du code de la sécurité intérieure.

⁴ On précisera que les agents qualifiés doivent être des agents techniquement compétents, habilités à connaître d'éléments couverts par le secret de la défense nationale et n'ayant fait l'objet d'aucune condamnation pénale inscrite au bulletin n° 2 du casier judiciaire. L'identité des agents doit être protégée par le responsable compétent pour recevoir l'ordre du Premier ministre et un officier de sécurité chargé du respect du droit du secret de la défense nationale doit être désigné par l'opérateur.

le Premier ministre »¹. Par ailleurs, les opérateurs se voient garantis par la loi une compensation financière de la part de l'Etat en cas de surcoûts identifiables et spécifiques². Les prestations et leurs tarifs sont fixés par un arrêté du Premier ministre³ qui précise concrètement les données pouvant être recueillies par les services de renseignement auprès des opérateurs⁴. En ce qui concerne les données mentionnées dans l'arrêté du Premier ministre, elles sont définies dans le cadre des garanties portant sur les renseignements collectés.

§3. Les garanties portant sur les renseignements collectés

Dans le prolongement des garanties applicables à la mise en œuvre des techniques de renseignement, le législateur a tenu à encadrer les renseignements collectés par ces dernières selon des principes de traçabilité et de centralisation des renseignements et des limitations dans leur conservation ainsi que dans leurs accès. Au préalable, il convient de s'attarder sur la définition des renseignements collectés, notamment sur la distinction opérée par la loi entre les données de connexion et les données de « contenu » qui constitue un critère fondamental à prendre en considération dans l'application des garanties portant sur les renseignements collectés.

A - La définition des renseignements collectés : données de connexion et données de « contenu »

Sur le plan technique, les renseignements collectés sont les « *données brutes recueillies dans le cadre d'une technique de renseignement* »⁵ qui peuvent « *prendre la forme d'extractions ou de transcriptions qui pourront être conservées tant qu'elles demeurent indispensables à la poursuite des finalités qui ont motivé leur réalisation* » afin d'intégrer les informations pertinentes dans les fichiers des

¹ Article R. 872-2 du code de la sécurité intérieure.

² Article L. 871-7 du code de la sécurité intérieure.

³ Article R. 873-2 du code de la sécurité intérieure.

⁴ Arrêté du 12 janvier 2018 portant application de l'article R. 873-2 du code de la sécurité intérieure fixant la tarification applicable aux demandes ayant pour objet la mise en œuvre des techniques de renseignement.

⁵ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 85.

services¹. Juridiquement, la loi du 24 juillet 2015 a distingué trois catégories de données brutes² :

- les « correspondances interceptées » ;
- les données recueillies dans le cadre des sonorisations et captation d'images et de données informatiques ;
- les « informations ou documents » relatifs aux communications électroniques.

L'identification des données concernées par les deux premières catégories ne présente pas de difficultés. La première porte sur le contenu des correspondances et la seconde sur des paroles, des images et des contenus traités par un système d'information et ses périphériques (sons, images, textes, etc.). En revanche, la troisième catégorie fait référence aux données de connexion qui peuvent être très nombreuses et difficiles à identifier. A ce titre, le législateur et l'exécutif ont fait le choix de définir négativement et positivement ces données dans le souci de garantir le droit au respect à la vie privée et la cohérence avec le droit du numérique.

1. La définition négative des données de connexion

De manière négative, les données de connexion désignent « *les données permettant l'acheminement d'une communication électroniques* » sans permettre d'accéder au contenu des échanges³. Reprenant la *summa divisio* du dispositif antérieur à 2015 « *entre, d'un côté, le contenu des correspondances et, de l'autre, les données techniques dont le recueil est en principe moins intrusif* »⁴, le législateur de 2015 a donc défini les données de connexion par opposition aux données de « contenu », notamment en subordonnant le recueil des données de connexion au respect de l'article 226-15 du code pénal⁵ protégeant le secret des

¹ CNCTR, 5^{ème} rapport annuel (2020), p. 73.

² Article L. 822-2 du code de la sécurité intérieure créé par la loi n° 2015-912 du 24 juillet 2015.

³ CNCTR, Délibération n° 1/2016 du 14 janvier 2016.

⁴ Conseil constitutionnel, commentaire des décisions n° 2015-713 DC et n° 2015-714 DC du 23 juillet 2015, p. 3.

⁵ Article L. 851-7 du code de la sécurité intérieure.

correspondances¹. Par cette exclusion, le législateur a entendu garantir une plus grande protection juridique aux données de contenu même si cette hiérarchisation n'est pas absolue selon l'arrêt *Big Brother Watch* de 2018 de la CEDH (§356)², ce qui aura notamment pour effet un traitement différencié des données dans leur régime de conservation³.

Cette définition négative a été retenue par le Conseil constitutionnel qui a réaffirmé la distinction avec les données de contenu en précisant que ces dernières portent sur « *le contenu de correspondances ou les informations consultés* »⁴. Ces précisions ont été reprises par les dispositions réglementaires relatives aux données de connexion pouvant être recueillies en application des dispositions de l'article L. 851-1 du code de la sécurité intérieure⁵. Et, dans le sillage de la jurisprudence constitutionnelle, le Conseil d'Etat a rappelé, entre autres, la définition négative des données de connexion pour affirmer en 2018 la légalité des dispositions de l'article R. 851-5 au regard de celles de l'article L. 851-1⁶. Pour sa part, la CNCTR a considéré en 2016 que les données de connexion définies positivement par le législateur et le pouvoir réglementaire respectaient la distinction garantie par la loi et la jurisprudence du Conseil constitutionnel à la suite d'une « *analyse globale, empirique, non exhaustive et non définitive* » s'appuyant sur la recommandation X.200 de l'Union internationale des télécommunications (UIT) portant sur les différentes couches de données identifiables dans les communications électroniques⁷. Pour autant, la définition positive des données de connexion nécessaire à la détermination de ce qui relève du contenant et du contenu fait débat.

¹ Sur ce point, voir J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 28.

² A ce sujet, voir B. Warusfel, *Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement*, *Le droit du renseignement*, op. cit., p. 74 et 75.

³ Cf. infra. *La conservation limitée des renseignements collectés*.

⁴ Décision n° 2015-713 DC du 23 juillet 2015 (considérant 55).

⁵ Article R. 851-5 du code de la sécurité intérieure.

⁶ Conseil d'Etat, 26 juillet 2018, *la Quadrature du Net*, *French Data Network* et *la Fédération des fournisseurs d'accès à internet associatifs* (n° 394922).

⁷ CNCTR, Délibération n° 1/2016 du 14 janvier 2016.

2. La définition positive des données de connexion

Dans la loi du 24 juillet 2015 relative au renseignement, les données de connexion sont « *des informations ou documents [des opérateurs] traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* »¹. A partir de cette définition globale, le décret du 29 janvier 2016 relatif aux techniques de renseignement a précisé les catégories de données visées par le législateur qui comprennent notamment les données conservées par les opérateurs mentionnées aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1^{er} décret n° 2011-219 du 25 février 2011 relatif à l'identification des personnes contribuant à la création d'un contenu en ligne. Ce sont les données mentionnées dans ces textes que la CNCTR a considéré conforme à la définition négative des données de connexion. Soulignons que le détail des données concernées a été remanié en 2021 au regard du droit européen de la protection des données personnelles sous l'autorité de la jurisprudence de la CJUE sans toutefois remettre en question les définitions négative et positive retenues par le législateur². En revanche, ces définitions tendent à être brouillées par l'introduction des URL par la seconde loi relative au renseignement du 30 juillet 2021 dans le périmètre des données traitées par les sondes et algorithmes des articles L. 851-2 et L. 851-3 du code de la sécurité intérieure.

3. Les données URL, un « brouillage » juridique

Techniquement, les données URL (adresses web ou « Uniform Resource Locator » en anglais) ont été définies sur le modèle de référence de l'UIT par la CNCTR dans sa délibération de n°1/2016 du 14 janvier 2016 comme des données mixtes, c'est-à-dire que ces données concernent à la fois le contenant et le contenu

¹ Article L. 851-1 du code de la sécurité intérieure.

² Cf. infra. Titre I de la Seconde Partie.

des correspondances ou des informations consultées sur internet. A ce titre, la Commission avait considéré que le recueil d'URL par les techniques d'accès aux données de connexion ne devait viser que les données relatives au chemin utilisé par les communications. Or, le législateur de 2021 a finalement autorisé le traitement des « *adresses complètes de ressources sur internet* » par les techniques algorithmiques et de sondes, ce qui remet en question la définition négative des données de connexion retenue par le Conseil constitutionnel puisque la définition des URL établie par la loi peut viser des données de contenu. Cette évolution pourrait donc être soumise à la censure des « Sages »¹. On remarquera néanmoins que la CNCTR et le Conseil d'Etat ne se sont pas opposée à l'extension envisagée par le législateur au regard des besoins de la lutte contre le terrorisme². En outre, on notera que le recueil des données URL comprenant des données de contenu pourrait s'avérer contraire à l'article L. 851-7 du code de la sécurité intérieure et constituer une infraction au sens de l'article 226-15 du code pénal même si l'on peut raisonnablement supposer que les services pourront bénéficier des dispositions de l'article 122-4 du code pénal relatives à l'irresponsabilité pénale du fait de la loi ou du règlement. Par ailleurs, il convient de préciser que les données URL ont été intégrées dans la même catégorie des renseignements collectés portant sur les données recueillies dans le cadre des sonorisations et captations d'images et de données informatiques³. En ce sens, les données URL pourraient être qualifiées globalement de données de contenu et non pas comme une catégorie *sui generis* des données de connexion comme relevé par la CNCTR⁴. Pour notre part, la solution retenue par le législateur de 2021 ne manque pas d'insécurité juridique. Il aurait pu être par exemple décidé d'opérer une distinction entre les données URL selon la doctrine de 2016 de la CNCTR ou mettre en place un régime d'autorisation spécifique applicable à ce type de données.

Enfin, on soulignera que la définition négative des données de connexion constitue une garantie essentielle pour la sécurité juridique du droit du renseignement numérique, notamment face à une définition positive de ces

¹ Cf. supra. §1 de la Section II du Chapitre I du Titre I.

² CNCTR, Délibération n° 2/2021 du 7 avril 2021 et Conseil d'Etat, Avis n° 402791 du 6 mai 2021.

³ Article L. 822-2 modifié par la loi n°2021-998 du 30 juillet 2021.

⁴ CNCTR, Délibération n° 2/2021 du 7 avril 2021, p. 6.

données nécessairement non définitive en fonction des évolutions technologiques¹ et pour assurer le respect des garanties légales de centralisation et de conservation des renseignements collectés.

B - La centralisation et la traçabilité des renseignements collectés

Afin de garantir le contrôle des techniques de renseignement, le législateur a promu un principe de centralisation des renseignements collectés applicable tant à la surveillance nationale² qu'à la surveillance internationale³. Selon la loi, le Premier ministre est chargé, d'une part, d'organiser la traçabilité du recueil des renseignements et, d'autre part, de définir les modalités de centralisation de ces derniers. Déjà consacré en matière d'interception et d'accès aux données de connexion, le principe de centralisation a pris une nouvelle dimension avec la légalisation de techniques directement mises en œuvre par les agents des services de renseignement par la loi du 24 juillet 2015, ce qui pose notamment « *la question nouvelle de la non-altération du renseignement transféré aux organismes de contrôle* »⁴. Dans ce contexte, la CNCTR a considéré que le respect des exigences légales de centralisation devait remplir trois conditions : la mise en place de systèmes d'information et de réseaux solides et sécurisés ; une capacité d'accès à distance aux données centralisées afin d'éviter des copies décentralisées hors de tout contrôle ; la limitation et le regroupement des lieux de stockage des données⁵.

Cette dernière condition a été la première à être formalisée dès 2015⁶ en réduisant au nombre de trois les points de centralisation des données : « *un à la DGSE pour les techniques qu'elle met en œuvre, un à la DGSI pour les techniques qu'elle met en œuvre, et un au GIC pour les autres services des premier et second cercles ainsi que pour les techniques dont la loi exige qu'elles soient centralisées au*

¹ CNCTR, Délibération n° 1/2016 du 14 janvier 2016.

² Article L. 822-1 du code de la sécurité intérieure.

³ Article L. 854-4 du code de la sécurité intérieure.

⁴ A ce sujet, voir Rapport n° 423 (Sénat, 2015-2016) et n° 3524 (Assemblée nationale, XVe législature), fait par M. Jean-Pierre Raffarin au nom de la délégation parlementaire au renseignement.

⁵ CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 78 à 80.

⁶ Ibid., p. 80.

GIC, comme les interceptions de sécurité »¹. Alors que certains auteurs avaient recommandé que les données devraient être impérativement stockées dans un lieu neutre², on peut regretter que la solution d'une centralisation au sein des infrastructures du GIC, organe neutre, n'ait pas été généralisée même si la loi n'interdit pas une centralisation réalisée par les services eux-mêmes et que la CNCTR « *dispose d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions (...) ainsi qu'aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements* »³. Toutefois, il pourrait toujours être envisagé de renforcer le rôle centralisateur du GIC, ce qui n'est pas sans soulever la question de la mise en place d'une agence technique unique de renseignement numérique⁴.

S'agissant des deux premières conditions, le GIC s'est efforcé depuis 2017, conformément à ses attributions fixées à l'article R. 823-1 du code de la sécurité intérieure⁵, à développer des applications informatiques de conservation centralisée des données collectées dans le cadre des techniques de renseignement directement mises en œuvre par les agents des services⁶. Il s'agit de techniquement contraindre les services collecteurs à utiliser des systèmes transmettant directement les données qu'ils recueillent dans les infrastructures du GIC d'où ils pourront réaliser les exploitations à distance⁷. Il ressort de ces considérations une obligation pour les services de recourir au dispositif de centralisation et d'accès aux données du GIC, sauf pour la DGSE et la DGSI⁸.

¹ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 178.

² En ce sens, voir notamment C. Lazerges et H. Henrion-Stoffel, *Politique criminelle, renseignement et droits de l'homme, à propos de la loi du 24 juillet 2015 relative au renseignement*, op. cit..

³ Article L. 833-2 du code de la sécurité intérieure.

⁴ En ce sens, voir F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

⁵ Le GIC est notamment chargé de « *contribuer à la centralisation des renseignements collectés lors de la mise en œuvre des techniques de recueil de renseignement* » et de « *concourir à la traçabilité de l'exécution des techniques de recueil de renseignement* ».

⁶ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 58 et suivantes.

⁷ A ce sujet, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 178 et suivantes.

⁸ Cf. CNCTR, *5^{ème} rapport annuel (2020)*, p. 75 et suivantes.

Dans le cadre d'une centralisation partagée entre le GIC, la DGSE et la DGSI, la traçabilité des renseignements collectés, corollaire du principe de centralisation, est alors une garantie primordiale d'effectivité du contrôle. En pratique, elle est assurée tant par le GIC que par les services eux-mêmes. Le service du Premier ministre « *tient un registre exhaustif des demandes et des autorisations, ainsi que des dates d'activation et de désactivation effective des moyens techniques correspondants* »¹. En outre, les outils numériques de centralisation qu'il développe et impose aux services constituent également un moyen matériel de traçabilité et de contrôle « puissant » des renseignements collectés. Au niveau des services, deux dispositifs doivent être distingués :

- d'une part, il a été mis en place des relevés ou « fiches de traçabilité » de mise en œuvre des techniques mentionnant les dates de début et de fin ainsi que la nature des renseignements collectés. Tenues à la disposition de la CNCTR, « *ces fiches sont en principe rédigées dès la fin de la mise en œuvre d'une technique ou, en l'absence de mise en œuvre, dès l'arrivée à échéance de l'autorisation* »² ;
- d'autre part, la DGSI et la DGSE ont développé des outils numériques de traçabilité permettant de suivre l'évolution des techniques de renseignement, du stade de la demande initiale formulée par l'agent enquêteur jusqu'à l'exploitation des données collectés. Ces outils tendent à être déployés au sein des autres services de renseignement³.

Les modalités de centralisation et de traçabilité des renseignements collectés n'ont pas été définies par le Premier ministre dans le code de la sécurité intérieure mais par les doctrines de la CNCTR et du GIC et revêtent, de ce fait, une portée contraignante relative pour les services et entrent en contradiction avec les dispositions des articles L. 822-1 et L. 854-4 du code de la sécurité intérieure. Si la CNCTR s'estime positive sur les progrès réalisés par le GIC et les services, il n'en demeure pas moins que le « rapport Larrivé » de juin 2020 a souhaité voir inscrire

¹ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 76.

² Cf. CNCTR, *5^{ème} rapport annuel (2020)*, p. 77.

³ A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 61 à 63 ; CNCTR, *5^{ème} rapport annuel (2020)*, p. 77 et 78.

dans le code de la sécurité intérieure les évolutions du principe de centralisation¹. Cependant, il convient de rappeler que les mesures envisagées jusqu'à présent sont d'ordre technique plus que juridique et que de nouvelles orientations peuvent être décidées au regard des évolutions administratives et technologiques. Il s'agit d'un chantier technique de numérisation des services et du GIC qui s'inscrit dans la durée, ce qui tend à rendre difficile de définir juridiquement les modalités issues de la pratique. Pour autant, il peut être envisagé d'instaurer, en référence aux outils imposés par le GIC, une obligation pour l'ensemble des services de renseignement, y compris la DGSE et la DGSI, d'utiliser ou de développer des outils de centralisation et de traçabilité certifiés conformes par le Premier ministre après avis de la CNCTR aux nécessités du contrôle des techniques de renseignement. L'inscription de ces modalités dans le code de la sécurité intérieure aurait pour intérêt de garantir juridiquement que les services ne définissent pas eux-mêmes les modalités de centralisation et de traçabilité tant sur le plan administratif que dans la programmation des outils numériques. A notre sens, il s'agirait de redonner au Premier ministre la responsabilité de l'application du principe de centralisation comme l'exige la loi. Enfin, curieusement rien n'est prévu en cas de refus d'application du principe de centralisation par le Premier ministre et l'administration. L'introduction de règles d'application de ce principe permettrait de remédier à cette lacune en permettant par exemple à la CNCTR d'opérer un véritable contrôle du respect du principe, voire de contester tout manquement à son application².

C - La conservation limitée des renseignements collectés

Principe cardinal dans la jurisprudence de la CEDH en matière de surveillance³ et déjà consacré par la loi du 10 juillet 1991 relative aux interceptions de sécurité, le principe de conservation limitée des renseignements collectés consiste à prévoir un délai légal au terme duquel les données recueillies doivent être détruites. Il constitue une garantie du respect du principe de proportionnalité précédemment évoqué ainsi qu'une application concrète de la

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 178 et 179.

² Cf. infra. §2 et §4 de la Section II du Chapitre II du Titre II.

³ Cf. CNCTR, 3^{ème} rapport annuel (2018), p. 102 et suivantes.

distinction opérée entre les données de connexion et les données de contenu. Avant de nous interroger sur la rationalité des délais adopté par le législateur depuis 2015, il convient de préciser que notre analyse portera uniquement sur les règles relatives aux données conservées par les services ou le GIC puisque la conservation des données par les opérateurs fait l'objet de règles spécifiques en droit du numérique¹. En droit du renseignement, il peut être distingué les délais de principe applicables pour les besoins de la surveillance des délais dérogatoires prévus pour d'autres besoins.

1. Les délais de principe liés à la surveillance

En se fondant sur la nature des renseignements collectés et leur degré d'atteinte à la vie privée², le législateur de 2015 a fixé la durée légale de conservation³ :

- à trente jours pour les correspondances et les paroles interceptées et cent vingt jours pour les images et données informatiques captées (données de contenu) ;
- à quatre ans pour les données de connexion.

On notera que les données recueillies par les algorithmes de détection d'une menace terroriste font l'objet d'un délai spécial d'exploitation de soixante jours⁴. Ces délais ont comme point de départ le recueil des renseignements et non leur exploitation comme initialement souhaité par les parlementaires, ce qui est plus protecteur pour le respect du droit à la vie privée selon le Conseil d'Etat et le Professeur Xavier Latour⁵. Cependant, lorsque les données sont chiffrées, le délai court à compter de leur déchiffrement dans un délai maximal de six ans à compter du recueil.

¹ Cf. infra. Titre I de la Seconde Partie.

² Voir à ce sujet J. -P. Raffarin, *Avis sur le projet de loi relatif au renseignement*, op. cit., p. 31.

³ Article L. 822-2 du code de la sécurité intérieure.

⁴ Article L. 851-3 du code de la sécurité intérieure.

⁵ Cf. J. -P. Raffarin, *Avis sur le projet de loi relatif au renseignement*, op. cit., p. 42 ; X. Latour, *La loi relative au renseignement : un Etat de surveillance ?*, op. cit..

Si la loi relative au renseignement de 2015 a retenu des délais plus longs que la loi du 10 juillet 1991¹, le Conseil constitutionnel a validé le dispositif en matière de surveillance intérieur mais il a, en revanche, jugé que le législateur n'avait pas épuisé sa compétence en renvoyant à un décret en Conseil d'Etat les conditions de conservation des renseignements collectés en matière de surveillance internationale². La loi du 30 novembre 2015 relative aux communications internationales a donc remédié à la censure du juge constitutionnel en adoptant toutefois un régime de conservation moins restrictif que la loi du 24 juillet 2015³ :

- *« douze mois à compter de leur première exploitation pour les correspondances, dans la limite d'une durée de quatre ans à compter de leur recueil » ;*
- *« six ans à compter de leur recueil pour les données de connexion » ;*
- *« pour ceux des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement. Ils ne peuvent être conservés plus de huit ans à compter de leur recueil ».*

Suivant le même raisonnement qu'en matière de surveillance nationale qui était fondé sur la proportionnalité des délais retenus par le législateur, les Sages ont également validé le régime de conservation spécifique à la surveillance internationale. Par ailleurs, on saluera le choix d'avoir soumis les communications « mixtes » interceptées au régime de conservation de la loi du 24 juillet 2015⁴.

En pratique, l'échelle des délais de conservation introduite en 2015 s'est révélée difficile à mettre en œuvre en ce qui concerne le cas particulier des paroles captées dans un dispositif de vidéo-surveillance. Dès 2016, il a été constaté qu'il n'était pas possible de dissocier les enregistrements audios et les images et donc

¹ La loi du 10 juillet 1991 avait fixé à 10 jours la durée légale de conservation des correspondances interceptées.

² Décision n° 2015-713 DC du 23 juillet 2015, loi relative au renseignement (considérants 38 et 39 ainsi que 76 à 79) et voir à ce sujet M. Verpeaux, *La loi sur le renseignement, entre sécurité et libertés. A propos de la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015*, op. cit..

³ Article L. 854-5 du code de la sécurité intérieure.

⁴ Article L. 854-8 du code de la sécurité intérieure.

de respecter strictement le délai de trente jours¹. Sans remettre en cause l'échelle établie par le législateur de 2015, la seconde loi relative au renseignement du 30 juillet 2021 a finalement aligné le délai de conservation des paroles sur celui de cent vingt jours applicables aux images. Ce dernier délai a également été retenu pour la conservation des URL². Pour aller plus loin dans la simplification des délais, Floran Vadillo proposait d'abandonner celui de trente jours applicables aux correspondances interceptées afin de ne retenir que deux types de délai : la durée de quatre ans pour les données de connexion et la durée de cent vingt jours pour les données de contenu³. Bien que l'échelle adoptée par le législateur soit plus protectrice que celle de Floran Vadillo, la proposition de simplification de ce dernier nous semble cohérente au regard de la jurisprudence constitutionnelle sur la distinction entre les données de connexion et les données de contenu.

En plus d'avoir fixé une échelle des délais maximal de conservation en fonction de la nature des renseignements collectés, la loi introduit également deux obligations de destruction de certaines données collectées lorsqu'elles se révèlent inutiles pour la surveillance.

D'abord, la loi prévoit une obligation de destruction des renseignements « *dès qu'il apparaît qu'ils ne sont pas en rapport avec l'autorisation de mise en œuvre* » dans le cadre des techniques d'IMSI-catcher et d'interception satellitaire. On notera que le législateur a pris soins de contraindre les opérations de destruction dans un délai déterminé : quatre-vingt-dix jours pour les données de connexion⁴ et trente jours pour les correspondances interceptées⁵. On retrouve une obligation similaire s'agissant de la technique algorithmique dont l'article L. 851-3 impose la destruction immédiate des « *données non détectées par les traitements comme susceptibles de révéler une menace à caractère terroriste* ».

Ensuite, les transcriptions et extractions réalisées sur les données brutes recueillies échappent aux délais prévus pour ces dernières et peuvent être

¹ Sur ce point, voir P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 78 et 79.

² Article L. 822-2 modifié par la loi n° 2021-998 du 30 juillet 2021.

³ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

⁴ Article L. 851-6 du code de la sécurité intérieure.

⁵ Article L. 852-1-II et L. 852-3 du code de la sécurité intérieure.

conservées « *tant qu'elles demeurent indispensables à la poursuite des finalités qui ont motivé leur réalisation* »¹. Dans ces conditions, la loi impose ainsi la destruction des transcriptions et extractions réalisées sur les renseignements collectés « *dès que leur conservation n'est plus indispensable à la poursuite des finalités mentionnées [à l'article L. 811-3]* »². En revanche, les opérations de destruction ne sont enfermées dans aucun délai mais doivent faire l'objet de relevés tenus à la disposition de la CNCTR pour que cette dernière puisse exercer son contrôle. On relèvera enfin que, dans le cadre de son contrôle, la CNCTR a pu constater des irrégularités relatives à une conservation des données au-delà de la durée légale mais que « *ces anomalies ont toutefois donné lieu à une régularisation immédiate par les services de renseignement concernés* »³.

2. Les délais dérogatoires non liés à la surveillance

Trois dérogations prévues à l'article L. 822-2 du code de la sécurité intérieure autorisent l'administration à conserver les renseignements collectés au-delà des délais précédemment étudiés. En premier lieu, les données peuvent être conservées plus longtemps « *dans une mesure strictement nécessaire aux besoins de l'analyse technique* » d'éléments de cyberattaque ou du chiffrement des données. En deuxième lieu, la consécration du contentieux des techniques de renseignement a amené le législateur à prévoir une dérogation de conservation « *pour les seuls besoins de la procédure devant le Conseil d'Etat* ». Enfin et en troisième lieu, la seconde loi relative au renseignement du 30 juillet 2021 permet aux services du premier cercle de conserver au-delà des durées légales les renseignements collectés « *aux seules fins de recherche et de développement en matière de capacités techniques de recueil et d'exploitation des renseignements* ». En outre, le dispositif en matière de recherche et de développement impose une destruction des renseignements collectés dans un délai maximal de cinq ans après leur recueil ou lorsqu'ils ne sont plus indispensables à la validation de capacités techniques de recueil et d'exploitation. Il est intéressant de relever que seul le dernier cas dérogatoire prévoit la destruction des données. A notre sens, les

¹ Cf. CNCTR, 3^{ème} rapport annuel (2018), p. 77.

² Article L. 822-3 du code de la sécurité intérieure.

³ A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 100.

dispositions relatives aux deux premiers cas devraient s'interpréter comme implicitement imposer aux services une destruction des renseignements lorsqu'ils ne sont plus indispensables aux besoins de l'analyse technique ou de la procédure devant le Conseil d'Etat. Néanmoins, il serait toujours préférable de prévoir cette obligation de destruction dans la loi.

D - Les restrictions d'accès aux renseignements collectés

Que ce soit dans la collecte des données ou dans leur exploitation, la loi prévoit deux types de restriction qui limitent l'accès aux données des personnes surveillées au sein des services de renseignement : d'une part, le nombre d'agents pouvant accéder aux données est limité et, d'autre part, la loi impose d'assurer techniquement la confidentialité de certaines données.

1. La limitation du nombre d'agents susceptibles d'accéder aux données

Au niveau de la collecte, seuls des agents individuellement désignés et habilités des services peuvent mettre en œuvre les techniques de renseignement soumises à autorisation et donc accéder aux données recueillies lors de cette mise en œuvre¹. Les différents décrets d'application relatif à la désignation des services autorisés à mettre en œuvre les techniques de renseignement n'ont pas manqué de rappeler systématiquement cette exigence législative. En outre, on retrouve la même exigence dans les dispositions relatives à l'utilisation du IMSI-catcher² ou des appareils de captations de paroles, d'images et de données informatiques³. Par ailleurs, seuls des agents qualifiés des opérateurs répondant aux demandes des services de renseignement peuvent accéder aux données sollicitées⁴.

S'agissant des opérations portant sur les renseignements collectés (destructions, transcriptions et extractions), là encore la loi exige qu'elles doivent être effectuées par des agents individuellement désignés et habilités⁵.

¹ Article L. 821-1 du code de la sécurité intérieure.

² Article L. 851-6 du code de la sécurité intérieure.

³ Article L. 853-1 et L. 853-2 du code de la sécurité intérieure.

⁴ Article L. 871-6 du code de la sécurité intérieure.

⁵ Article L. 822-4 du code de la sécurité intérieure.

Enfin, l'accès aux données conservées aux fins de recherche et développement est réservée à des agents spécialement habilités des services de renseignement et du ministère de la défense¹ ou du GIC².

2. L'exigence de mesures techniques de confidentialité applicable à certaines données

Dans trois cas la loi oblige l'administration à recourir à des mesures techniques visant à préserver la confidentialité des renseignements collectés et restreindre ainsi leur accessibilité. Premièrement, les dispositions relatives à la technique algorithmique de détection d'une menace terroriste imposent à ces traitements de données de ne pas permettre l'identification des personnes lors de leur mise en œuvre tout en offrant la possibilité de lever l'anonymat sur les personnes en cas de détection³. Si ces dispositions ont pu être considérées comme une mesure d'anonymisation des données⁴, elles peuvent s'interpréter comme une mesure de pseudonymisation des données selon Floran Vadillo⁵. Il est vrai que cette dernière approche nous semble la plus probable au regard des définitions proposées par la CNIL dans le cadre du RGPD : « *l'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible* » alors que « *la pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire* » et « *permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe* », ce qui implique que « *l'opération de pseudonymisation est également réversible, contrairement à l'anonymisation* »⁶.

¹ Article L. 822-2-III du code de la sécurité intérieure.

² Article L. 822-2-1 du code de la sécurité intérieure.

³ Article L. 851-3 du code de la sécurité intérieure.

⁴ A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, DPR, 11 juin 2020, p. 72.

⁵ F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, Livret #12, L'Hétairie, 9 mars 2020.

⁶ Cf. [L'anonymisation de données personnelles | CNIL](https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles) (<https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles>).

Deuxièmement, les données conservées à des fins de recherche et développement ont vocation à être anonymisées¹, notamment en faisant disparaître les motifs et les finalités liés à la collecte des données concernées et en ne permettant pas de rechercher l'identité des personnes concernées². Notons que la solution de la pseudonymisation aurait pu être privilégiée pour la recherche en matière d'IA de renseignement car « *dans la plupart des cas, le principe d'anonymisation n'est pas pertinent : il aboutit en pratique à appauvrir ou à détruire au préalable l'information précisément utile à l'opération de modélisation par apprentissage* »³. Cependant, la solution de l'anonymisation nous semble plus protecteur et adaptée aux besoins de la recherche en renseignement d'Etat, notamment en ce que cette mesure technique permet d'éviter tout impact sur la vie privée des personnes concernées et donc d'exploiter et de partager plus facilement les gisements de données⁴. En revanche, il convient de rappeler qu'une anonymisation absolue des données est impossible en l'état actuel de la technique⁵, ce qui devrait faire l'objet d'une attention particulière de la part du Premier ministre et de la CNCTR dans le cadre des autorisations sur les paramètres techniques applicables à chaque programme de recherche.

Troisièmement, la seconde loi relative au renseignement du 30 juillet 2021 a prévu une obligation de chiffrement en matière de centralisation des interceptions des correspondances satellitaires : « *cette centralisation intervient dès l'interception des communications, sauf impossibilité technique. Dans ce cas, les données collectées font l'objet d'un chiffrement dès leur collecte et jusqu'à leur centralisation effective au sein du service du Premier ministre* »⁶. Selon l'étude

¹ Sur ce point, voir Etude d'impact du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative du 11 mai 2021, p. 152.

² Article L. 822-2-III du code de la sécurité intérieure.

³ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 107.

⁴ Cf. [L'anonymisation de données personnelles | CNIL](https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles) (<https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles>).

⁵ En ce sens, voir V. -L. Benabou, *L'extension du domaine de la donnée*, LEGICOM, vol. 59, no. 2, 2017, pp. 3-17.

⁶ Article L. 852-3-III du code de la sécurité intérieure.

d'impact sur le projet de loi, il s'agit d'un chiffrage asymétrique des flux de données « *dont seul le GIC aura la clé* »¹.

Il peut être intéressant de relever que, par ces trois mesures techniques imposées par les lois sur le renseignement (pseudonymisation, anonymisation et chiffrage des données), le droit du renseignement participe à « *l'essor d'une régulation technique des données* » qui a pu être observé avec l'entrée en vigueur du RGPD².

SECTION II : Le régime répressif, l'abus de la surveillance numérique constitutive d'une faute

Lorsque les agents des services de renseignement mettent en œuvre des moyens numériques de surveillance en dehors du cadre du régime préventif, ils sont susceptibles d'engager la responsabilité administrative de l'Etat pour faute simple du fait du renseignement numérique (§1) mais également d'être pénalement poursuivis selon un régime atypique de responsabilité pénale (§2).

§1. La responsabilité administrative de l'Etat pour faute simple du fait du renseignement numérique

Tout en créant un contentieux des techniques³ et des fichiers de renseignement⁴, la loi du 24 juillet 2015 a consacré un régime de responsabilité administrative de l'Etat du fait du renseignement numérique. En effet, la formation spécialisée du Conseil d'Etat peut être amenée à statuer sur des recours en plein contentieux sur la légalité et la proportionnalité des techniques de renseignement soumises à autorisation et sur la mise en œuvre des fichiers des services⁵. A ce

¹ Voir à ce sujet Etude d'impact du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative du 11 mai 2021, p. 171.

² En ce sens, voir E. Petit-Prévost-Weygand, *L'activité extraterritoriale des services de renseignement numérique : recherche de solutions technico-juridiques de protection des données*, Journal du droit international (Clunet) n° 3, juillet 2021, var. 7.

³ Article L. 841-1 du code de la sécurité intérieure.

⁴ Article L. 841-2 du code de la sécurité intérieure.

⁵ Voir en ce sens P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 70.

titre, le juge administratif peut condamner l'Etat à indemniser le préjudice subi en cas d'illégalité constatée¹.

On relèvera que si le régime de responsabilité de l'Etat du fait des techniques de renseignement s'applique aux techniques soumises à autorisation du Premier ministre, il semble que, depuis la loi SILT du 30 octobre 2017, les mesures de surveillance relevant de l'exception hertzienne ne soient pas exclues des recours en plein contentieux devant la formation spécialisée du Conseil d'Etat. La compétence de cette dernière s'étendrait à l'ensemble des techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure selon l'article L. 841-1 du même code, ce qui comprend les dispositions du chapitre V du titre V relatives à l'exception hertzienne. En outre, ce dernier chapitre ne prévoit aucune dérogation au contentieux des techniques de renseignement tout en permettant à la CNCTR d'exercer un contrôle sur la mise en œuvre de l'exception hertzienne.

Afin d'engager la responsabilité de l'Etat du fait des techniques de renseignement ou des fichiers des services, la loi exige d'abord qu'une illégalité ait été commise dans la mise en œuvre des techniques ou dans l'exploitation des renseignements collectés ou des données conservées dans les fichiers. Ensuite, le requérant qui souhaite se voir ouvrir un droit à indemnisation doit saisir le juge administratif de conclusions en ce sens en justifiant que l'illégalité en question est à l'origine d'un préjudice. On retrouve ainsi les conditions communes du droit de la responsabilité : une faute, un préjudice et un lien de causalité. S'agissant du préjudice subi et du lien de causalité, ces conditions ne devraient pas poser de difficultés car il résulte nécessairement un préjudice d'atteinte à la vie privée en cas de violation de la loi dans la mise en œuvre des moyens numérique de renseignement. En revanche, la détermination de la nature de la faute est moins évidente en matière de renseignement.

En dehors du contentieux consacré par la loi du 24 juillet 2015, le juge administratif a consacré un régime de responsabilité de l'Etat du fait de l'activité des services de renseignement dans le cadre de l'affaire *Merah*. Après un désaccord entre les juges du fond sur la nature de la faute², le Conseil d'Etat a

¹ Articles L. 773-7 et 773-8 du code de justice administrative.

² Voir à ce sujet F. Eddazi, *La responsabilité de l'Etat en matière de renseignement : affirmation et construction d'un régime*, Droit Administratif n° 11, novembre 2017, étude 16.

finalement jugé en 2018 qu'il doit être retenu un régime de responsabilité pour faute lourde en cas de défaillances des services de renseignement¹. Cependant, cette solution a pu être interprétée comme ne s'appliquant pas à l'ensemble des activités des services de renseignement, le régime de la faute simple pouvant être retenu dans le cadre du contentieux des techniques et des fichiers de renseignement². A notre sens, les dispositions des articles L. 773-7 et L. 773-8 du code de justice administrative relatives au droit à indemnisation en cas de surveillance illégale laissent une certaine marge d'appréciation au juge administratif pour déterminer la nature de la faute susceptible d'engager la responsabilité de l'Etat mais il nous semble raisonnable et cohérent d'affirmer qu'une illégalité constatée par la formation spécialisée du Conseil d'Etat réponde au régime de la faute simple.

Pour finir, on relèvera que l'engagement de la responsabilité de l'Etat du fait des techniques de renseignement peut également entraîner la saisine du procureur de la République lorsque l'illégalité constatée est susceptible de constituer une infraction³, ce qui nous amène à étudier les règles relatives à la responsabilité pénale des agents qui ont été retenues en droit du renseignement dans le cadre de la surveillance numérique.

§2. Un régime atypique de responsabilité pénale des agents

Avant l'entrée en vigueur de la loi du 24 juillet 2015 relative au renseignement, il était communément admis que l'usage de moyens spéciaux en dehors de tout cadre légal pouvait constituer des infractions pénales comme la violation de la vie privée ou du secret des correspondances susceptibles d'engager la responsabilité pénale des agents ou directeurs des services⁴. Sous l'empire de la loi du 10 juillet 1991 relative aux interceptions de sécurité, l'engagement de la responsabilité pénale de l'ancien directeur de la DCRI, Bernard Squarcini, pour

¹ Conseil d'Etat, 18 juillet 2018, *ministre de l'Intérieur c. consorts Chennouf et autres* (requête n° 411156).

² En ce sens, voir C. -E. Minet, *La responsabilité de l'Etat envers les victimes d'actes de terrorisme à raison des carences des services de renseignement n'est engagée qu'en cas de faute lourde*, La Semaine Juridique Administrations et Collectivités territoriales n° 51-52, 26 décembre 2018, 2347.

³ Alinéa 3 de l'article L. 773-7 du code de justice administrative.

⁴ Voir en ce sens J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 37 et suivantes.

collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite avait ainsi permis de contester la légalité de la mise en œuvre de l'exception hertzienne¹ dans le cadre de l'affaire des « *fadettes du Monde* »².

La loi du 24 juillet 2015 est venue réaffirmer cette position dans l'article L. 862-2 du code de la sécurité intérieure qui dispose que « *les agents des services spécialisés de renseignement sont pénalement responsables de leurs actes dans les conditions définies au titre II du livre Ier du code pénal* ». Autrement dit, le droit commun de la responsabilité pénale est applicable aux agents des services lorsqu'ils mettent en œuvre des moyens numériques de renseignement, ce qui implique :

- d'une part, qu'aucune immunité pénale de principe n'a été consacrée par la loi, ce que le Conseil constitutionnel³ a rappelé en reconnaissant que les agents des services pouvaient être poursuivis pour violation du secret professionnel en cas de révélations de renseignements ou données collectés à caractère secret⁴ ;
- d'autre part, l'application de l'article 122-4 du code pénal qui prévoit l'irresponsabilité pénale des agents qui accomplissent « *un acte prescrit ou autorisé par des dispositions législatives ou réglementaires* » ou « *un acte commandé par l'autorité légitime, sauf si cet acte est manifestement illégal* »⁵.

Les dispositions de l'article L. 862-2 du code de la sécurité intérieure permettent ainsi de protéger pénalement les agents dans le cadre des techniques de renseignement sans pour autant exclure leur responsabilité en cas de mise en œuvre d'une technique en dehors de l'autorisation du Premier ministre ou dans le cas d'une autorisation « manifestement illégale ». Dans ce dernier cas, on relèvera que la chambre criminelle de la Cour de cassation a jugé en 2008 dans l'affaire des

¹ Trib. corr. Paris, 8 avril 2014, n° 11010023019.

² Cf. S. Lavric, « *Fadettes du Monde* » : condamnation pour collecte illicite de données personnelles, Dalloz actualité, 17 avril 2014.

³ Décision n° 2015-713 DC du 23 juillet 2015, considérants 31 à 37.

⁴ A ce sujet, voir N. Catelan, *Les nouveaux textes relatifs au renseignement : un moindre mal*, op. cit..

⁵ Sur ce point, voir B. Warusfel, *Le cadre juridique incertain des actions spéciales*, publication sur le blog Hestia.hypothèses.org, 9 mars 2016.

« écoutes de l'Elysée » que « le commandement de l'autorité légitime ne peut être retenu en faveur d'un officier supérieur de la gendarmerie et de hauts fonctionnaires, dès lors que ne leur était imposée aucune obéissance inconditionnelle à des ordres manifestement illégaux »¹.

En revanche, on peut douter de la portée générale des dispositions de l'article L. 862-2 en matière de renseignement numérique². En effet, l'affirmation des excuses pénales spécifiques aux cyber-patrouilles administratives³ et aux mesures de piratage informatique à l'étranger⁴ atténuent clairement l'application du droit commun de la responsabilité pénale. Plus encore, on remarquera que les conditions d'application de ces mesures de surveillance non soumises à autorisation du Premier ministre ne sont pas sans rappeler certaines garanties exigées par le régime préventif. Dans les deux cas, la loi exige notamment que les mesures soient mises en œuvre pour répondre aux finalités de l'article L. 811-3 du code de la sécurité intérieure par des agents individuellement désignés et habilités des services. S'agissant particulièrement des cyber-patrouilles administratives, on rappellera que l'intervention d'un agent superviseur ou coordonnateur caractérisait un régime d'autorisation selon le législateur⁵. En ce qui concerne l'excuse pénale de l'article 323-8 du code pénal, on retrouve l'application du principe de territorialité consacré par la loi n° 2015-1556 du 30 novembre 2015 puisque les mesures de piratage concernées doivent viser des systèmes d'information situés hors du territoire national⁶.

Dans ces conditions, il est vrai que les agents des services bénéficient d'un régime atypique de responsabilité pénale qui n'est pas sans interroger sur une possible requalification des excuses pénales en techniques de renseignement. Si une telle opération juridique peut être envisagée pour les cyber-patrouilles administratives, elle nous semble peu raisonnable pour les mesures de l'article

¹ Cass. crim., 30 septembre 2008, *affaire des écoutes de l'Elysée* (n° 07-82249).

² En ce sens, voir R. Parizot, *Surveiller et prévenir... à quel prix ?*, Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, op. cit..

³ Article L. 863-1 du code de la sécurité intérieure.

⁴ Article 323-8 du code pénal.

⁵ Cf. supra. §2 de la Section II de la Chapitre I du Titre I.

⁶ Cf. supra. §3 de la Section II du Chapitre I du Titre I.

323-8 du code pénal au regard des contraintes du renseignement d'Etat, de l'espionnage international et de la lutte contre la cybercriminalité¹.

Pour finir, on remarquera que les régimes préventif et répressif s'enchevêtrent malgré leur ambivalence puisque l'illégalité d'une technique de renseignement soumise à autorisation ou un fichage illégal peuvent entraîner des sanctions en responsabilités administrative et pénale. Nous verrons par la suite que l'usage illégal d'un moyen numérique de renseignement est susceptible de constituer des infractions relevant du droit pénal du numérique².

Afin de veiller à ce que les deux régimes s'appliquent de manière concrète à l'administration et ses agents dans l'emploi des moyens numériques de renseignement, des mécanismes de contrôle sont spécifiquement prévus.

¹ Cf. supra. §2 et 3 de la Section II du Chapitre I du Titre I.

² Cf. infra. Chapitre II du Titre I de la Seconde Partie.

CHAPITRE II

LA SPECIALISATION DU CONTROLE SUR LES MOYENS NUMERIQUES

En adaptant ses règles aux moyens numériques utilisés par les services, le droit du renseignement a également spécialisé les mécanismes et instances de contrôle sur les enjeux numériques, que ce soit dans les contrôles internes (**Section I**) ou dans les contrôles externes (**Section II**).

SECTION I : Les contrôles internes

Dans le sillage de la procédure de mise en œuvre des techniques de renseignement, une formalisation d'un contrôle hiérarchique du renseignement numérique s'est révélée indispensable (§1) comme il a été réaffirmé le rôle technico-juridique incontournable du GIC (§2). En outre, au regard des acteurs impliqués dans cette procédure et de leur proximité avec les outils de surveillance numérique, le législateur n'a pas manqué de prévoir un contrôle ministériel des opérateurs du numérique (§3) et un mécanisme spécifique de lanceur d'alerte de la surveillance numérique (§4). Enfin, il ne faut pas oublier que l'Exécutif oriente et évalue les moyens numériques à dispositions des services (§5).

§1. La formalisation d'un contrôle hiérarchique du renseignement numérique

En reprenant et en généralisant le mécanisme de la loi du 10 juillet 1991 d'autorisation préalable du Premier ministre dans la mise en œuvre des techniques de renseignement, la loi du 24 juillet 2015 « *a imposé une structuration de l'exécutif pour recevoir et traiter les demandes d'autorisation* »¹. Il en ressort un véritable contrôle hiérarchique strict de légalité et d'opportunité des techniques².

¹ Voir à ce sujet F. Vadillo, *Quand l'Etat de droit rencontre l'Etat secret : cadre et garanties du recours aux techniques de recueil de renseignement*, Le droit du renseignement, op. cit..

² Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 24.

Plus précisément, la loi exige qu'une demande d'autorisation soit vérifiée et validée, au minimum, à trois niveaux hiérarchiques : la direction du service concerné, le cabinet du ministre de tutelle et, enfin, celui du Premier ministre qui représente l'échelon sommital¹. On soulignera que ce contrôle hiérarchique formalisé par la loi a été considéré comme essentiel pour le respect du droit à la vie privée dans la mise en œuvre des techniques de renseignement par le Conseil constitutionnel qui a censuré le dispositif « d'urgence opérationnelle » ayant pour objet d'outrepasser l'autorisation du Premier ministre². Par ailleurs, on rappellera qu'en dehors des techniques soumises à autorisation le législateur de 2015 a également tenu à soumettre à un contrôle hiérarchique les « cyber-patrouilles administratives » qui sont placées sous l'autorité d'un agent superviseur ou coordonnateur³. La loi relative au renseignement a ainsi réduit le risque d'autonomisation opérationnelle des services dans la surveillance numérique⁴.

Comme le souligne Renaud Vedel, il s'agit là d'un contrôle hiérarchique fort et prégnant puisqu'il implique une dialectique entre responsabilité administrative et responsabilité politique qui incite chaque autorité à bien contrôler les techniques de renseignement⁵. Au sein des services, la loi du 24 juillet 2015 a entraîné un « changement culturel » et un bouleversement organisationnel pour répondre aux nécessités du contrôle hiérarchique, notamment avec la mise en place de cellules de conformité spécialisées⁶. A titre d'exemple, on peut citer le recrutement d'un agent dédié à la gestion des techniques de renseignement au sein de la DNRED ou encore le renforcement de la structure d'appui et de contrôle des techniques à la DGSI et la création d'un guichet unique au niveau de l'administration centrale pour traiter les demandes du SCRT⁷. Si la charge procédurale induite par la loi a pu susciter des inquiétudes sur les risques de

¹ Articles L. 821-1 à L. 821-4 du code de la sécurité intérieure.

² Décision n° 2015-713 DC du 23 juillet 2015 (considérant 27 à 30).

³ Voir sur ce point P. Bas, *Rapport sur le projet de loi relatif au renseignement et sur la proposition de loi organique relative à la nomination du président de la CNCTR*, op. cit., p. 101.

⁴ En ce sens, voir B. Warusfel, *Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement*, *Le droit du renseignement*, op. cit..

⁵ Cf. R. Vedel, *Les contrôles internes, Le droit du renseignement*, op. cit..

⁶ Ibid.

⁷ Voir à ce sujet C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 50 et 51.

renoncement aux techniques de renseignement, il semble que les services eux-mêmes excluent toute remise en question sur l'efficacité de la politique publique du renseignement¹. D'ailleurs, on relèvera que le renoncement peut davantage porter sur la complexité technique des outils à déployer plutôt que sur la lourdeur des procédures selon la DGSE². On remarquera alors qu'au-delà de l'encadrement juridique du renseignement la complexité de la technologie elle-même joue un rôle pratique dans la régulation de l'usage de la surveillance numérique.

Dans ces conditions, on ne peut donc que souscrire à la préconisation de Floran Vadillo selon laquelle il pourrait être envisagé de renforcer le formalisme du contrôle hiérarchique avec « *l'émergence de véritables (sous-)directions de la conformité et de la légalité au sein de chacun des services* » et la mise en place d'une instance spécialisée auprès de chaque ministre concerné à l'image du Bureau réservé du ministère des Armées³. Nous ajouterons qu'il serait pertinent de prévoir un contrôle hiérarchique interne et spécialisé sur les techniques de collecte décentralisée des renseignements afin de s'assurer, de façon continue, de la non-altération du renseignement transféré aux autres organismes de contrôle⁴. Pour le recours à ces techniques, l'intervention d'un agent superviseur ou coordonnateur, à l'instar des cyber-patrouilles, chargé notamment d'effacer les renseignements inutiles durant la collecte pourrait être envisagée et formalisée⁵.

Enfin, il convient de rappeler que l'adaptation des services et des cabinets des ministres concernés aux besoins du contrôle hiérarchique des techniques de renseignement doit se faire en cohérence avec le GIC qui exerce un contrôle au niveau interministériel.

¹ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 51 et 52.

² Ibid.

³ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

⁴ Sur ce point, voir J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 43.

⁵ Notons qu'en pratique, les services assurent déjà l'effacement des renseignements inutiles collectés par des techniques décentralisées (cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 178).

§2. Le rôle technico-juridique incontournable du Groupement interministériel de contrôle

Créé en 1960 par décision non publiée du Premier ministre, Michel Debré, le Groupement interministériel de contrôle (GIC) est un « service technique neutre » chargé de la centralisation des techniques de renseignement sans compétences en matière d'exploitation des renseignements qu'il collecte¹. Initialement institué pour mettre fin à l'anarchie des écoutes administratives réalisées par les différents services, le GIC s'est vu reconnaître officiellement un rôle central dans la mise en œuvre des interceptions de sécurité avec la loi du 10 juillet 1991². Néanmoins, ce n'est que par un décret n° 2002-497 du 12 avril 2002 que l'existence juridique du GIC et ses fonctions de contrôle des demandes d'interceptions ainsi que des renseignements collectés ont été formalisées. Il convient de remarquer qu'en pratique le GIC n'a pas toujours joué un rôle central dans le contrôle des écoutes depuis sa création, notamment dans les années 1980 avec l'affaire des écoutes de l'Elysée³. En revanche, le dispositif issu de la loi relative au renseignement de 2015 a entraîné un véritable changement de dimension pour ce service qui a été réorganisé pour constituer « *l'instrument principal du Premier ministre pour assurer la gestion, la mise en œuvre et la traçabilité de techniques de renseignement intrusives* »⁴. En effet, le GIC s'est vu renforcé ses attributions en étant chargé de :

« 1° Enregistrer les demandes de mise en œuvre des techniques de recueil de renseignement mentionnées à l'article L. 821-2 et aux II et III de l'article L. 854-2 ;

¹ Cf. J. Poirot, GIC (Groupement interministériel de contrôle), Dictionnaire du renseignement, Perrin, 2018, p. 433 à 436.

² P. Chambon, Analyse et commentaire de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, Recueil Dalloz 1991, p. 173 ; J. Pradel, un exemple de restauration de la légalité criminelle : le régime des interceptions de correspondances émises par la voie des télécommunications, Recueil Dalloz 1992, p. 49.

³ Lors de son premier septennat, le Président de la République, François Mitterrand, a créé une cellule *ad hoc* d'écoutes à l'Elysée pour procéder à des interceptions de sécurité en dehors du GIC, ce qui a conduit à des condamnations pour atteinte à la vie privée par le tribunal correctionnel de Paris le 9 novembre 2005 (Cf. J. -M. Delarue, Renseignement et sphère privée, Archives de politique criminelle, vol. 43, no. 1, 2021, p. 73-89).

⁴ Cf. C. Cambon, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020, DPR, 11 juin 2020, p. 56.

2° Enregistrer les autorisations de mise en œuvre des techniques de recueil de renseignement mentionnées à l'article L. 821-4 et aux I, II et III de l'article L. 854-2 ;

3° Recueillir et conserver les informations ou documents mentionnés à l'article L. 851-1 dans les conditions fixées au chapitre Ier du titre V du présent livre ;

4° Centraliser l'exécution des interceptions de sécurité autorisées en application du I de l'article L. 852-1 et de l'article L. 854-8 ainsi que les opérations de transcription et d'extraction des communications interceptées ;

5° Contribuer à la centralisation des renseignements collectés lors de la mise en œuvre des techniques de recueil de renseignement autres que celles mentionnées aux 3° et 4° ;

6° Concourir à la traçabilité de l'exécution des techniques de recueil de renseignement »¹.

Afin de clarifier le positionnement institutionnel du GIC et de répondre à l'extension de ses missions ainsi qu'à l'augmentation des techniques de renseignement, il a été décidé d'en faire un service à compétence nationale sous la tutelle du Secrétariat général de la Défense et de la Sécurité nationale (SGDSN)². Depuis 2016, le GIC n'est donc plus un simple service technique d'écoutes mais le service qui « *met en œuvre les surveillances numériques en s'interposant entre les opérateurs et les services de renseignement* » et qui « *en contrôle l'exploitation, détruit les données au terme du délai légal et interrompt les surveillances qui s'écarteraient de l'autorisation accordée* »³. Le GIC s'affirme alors comme un acteur technico-juridique incontournable du contrôle de la mise en œuvre des techniques de renseignement. En effet, le service du Premier ministre constitue le service chargé de mettre en cohérence le droit et la technique et, à ce titre, il « *est devenu le correspondant privilégié de la CNCTR dans l'exercice de ses missions de contrôle*

¹ Article R. 823-1 du code de la sécurité intérieure.

² Décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

³ Cf. SGDSN, *Rapport d'activité 2019-2020*, p. 40 et 41.

aussi bien a priori qu'a posteriori »¹. Ces considérations ne sont pas sans interroger sur la nécessité de renforcer les capacités de contrôle du GIC.

A - Le contrôle de la mise en œuvre des techniques de renseignement

Centralisant l'ensemble des demandes des techniques de renseignement, le GIC constitue la dernière instance de contrôle interne chargée de transmettre les demandes à la CNCTR pour avis avant de les soumettre à l'autorisation du Premier ministre². Dans ce contexte, le GIC doit non seulement s'assurer de la légalité et de l'opportunité des demandes et de leur renouvellement, dans la continuité du contrôle hiérarchique, mais aussi de leur conformité avec les avis de la CNCTR. Il est également chargé de veiller à ce que les identifiants techniques surveillés correspondent bien aux cibles visées ainsi qu'à la bonne répartition des surveillances numériques. Il est vrai que ces deux aspects technico-juridiques relèvent davantage de la compétence du GIC que des services. Enfin, l'exploitation des techniques de renseignement n'échappent pas à son contrôle tout comme l'exécution des techniques décentralisées.

1. La correspondance entre identifiants techniques et cibles

Dans le cadre de son contrôle, le GIC s'assure, d'une part, que les identifiants techniques souhaitant être interceptés par le service demandeur sont bien utilisés par la personne ciblée par la mesure et, d'autre part, que l'utilisation de ces identifiants techniques soit effective afin de détecter des anomalies dans la surveillance et de supprimer, si nécessaire, les identifiants inutiles ou qui ne sont pas en relation avec la cible³. Ainsi par exemple en matière d'interception de sécurité, il s'agit de savoir si le numéro de téléphone mentionné par le service demandeur est utilisé par la personne ciblée et si la ligne téléphonique est en état de fonctionnement.

¹ Cf. CNCTR, *4^{ème} rapport d'activité (2019)*, p. 78.

² Voir à ce sujet, C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 38.

³ Cf. CNCTR, *4^{ème} rapport annuel (2019)*, p. 79 et 80.

2. La répartition des surveillances numériques

Avant de transmettre les demandes à la CNCTR, le GIC veille également à détecter les éventuels doublons entre les différents services¹, notamment afin d'assurer le respect de l'article L. 811-3 du code de la sécurité intérieure dont les dispositions relatives aux missions des services s'opposent à ce que ces derniers déposent des demandes similaires pour une même cible².

Par ailleurs, la CNCTR veille à l'application de la primauté de l'autorité judiciaire consacrée par l'article 66 de la Constitution de 1958 par les services de renseignement, ce qui implique pour le GIC, en vertu du principe de centralisation, de contrôler et de mettre fin aux éventuelles interférences entre les techniques de police judiciaire et les techniques de renseignement³. En matière de répartition des surveillances numériques, il convient de préciser que le GIC est aussi chargé de surveiller les contingents des techniques de renseignement fixés par le Premier ministre⁴.

3. L'exploitation des techniques de renseignement

A posteriori de la mise en œuvre des techniques, le GIC exerce le contrôle interne des transcriptions et extractions conformément aux dispositions de l'article L. 822-3 du code de la sécurité intérieure, c'est-à-dire qu'il s'assure que « *seuls les renseignements qui se rattachent aux finalités légales peuvent faire l'objet d'une telle transcription ou extraction et donc par conséquent d'une exploitation et d'une conservation* »⁵. En pratique, ces opérations sont réalisées dans les locaux du GIC et les transmissions des productions aux services sont soumises à la validation du service du Premier ministre qui peut les refuser. A l'occasion de ce contrôle, on relèvera que le GIC adopte une « vigilance particulière » sur les transcriptions et extractions qui impliquent des cibles exerçant une profession ou un mandat

¹ Voir à ce sujet G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 75 à 77.

² En ce sens, voir F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

³ Cf. CNCTR, *4^{ème} rapport annuel (2019)*, p. 79 à 82.

⁴ Cf. CNCTR, *5^{ème} rapport annuel (2020)*, p. 20.

⁵ En ce sens, voir R. Vedel, *Les contrôles internes*, *Le droit du renseignement*, op. cit..

protégé par la loi¹. Par ailleurs, le GIC devrait voir son contrôle étendu aux transmissions de renseignements collectés entre les services prévues par les nouvelles dispositions de l'article L. 822-3 issues de la loi relative au renseignement du 30 juillet 2021. Là encore, le GIC est amené à jouer un rôle incontournable dans la coopération technique inter-services.

4. La difficulté du contrôle des techniques décentralisées

Depuis la loi de 2015, certaines techniques de renseignement sont déclenchées par les agents des services sans passer par l'intermédiaire du GIC. Directement déployés lors d'opérations de surveillance, les balises, IMSI-catchers et autres dispositifs de captation de sons, vidéos et de données informatiques restent néanmoins soumises au principe de centralisation². En vertu de ce dernier, il revient donc au GIC, en droit, d'assurer un contrôle. Pour autant, un tel contrôle peut se révéler plus délicat à s'exercer en pratique au regard de l'autonomie technique dont peuvent désormais disposer les services³, notamment la DGSI et la DGSE qui ont été habilitées à centraliser elles-mêmes les techniques décentralisées⁴. Les réponses à ces difficultés tiennent alors aux capacités de contrôle du GIC et à leur nécessaire renforcement.

B - Le renforcement nécessaire des capacités de contrôle du Groupement interministériel de contrôle

L'augmentation des techniques et des demandes des services qui doivent être rapidement traitées ou encore le suivi juridique et technique de l'exécution des autorisations alors même que certaines techniques s'exécutent sans intervention préalable du GIC sont des défis auxquels ce dernier a dû répondre pour assurer un contrôle interne effectif. Depuis 2015, les capacités du service du Premier ministre ont ainsi été nécessairement renforcées dans le cadre d'une réorganisation technologique, ce qui a conduit la CNCTR à envisager une extension

¹ Cf. CNCTR, *4^{ème} rapport annuel (2019)*, p. 81 et 82.

² Article L. 822-1 du code de la sécurité intérieure.

³ Voir à ce sujet J. -M. Delarue, *Renseignement et sphère privée*, Archives de politique criminelle, vol. 43, no. 1, 2021, p. 73-89.

⁴ Sur ce point, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 178 et 179.

des prérogatives du GIC en proposant de lui déléguer son contrôle des mesures les moins intrusives.

1. Une réorganisation technologique

Dès 2016, le GIC s'est rapidement réorganisé afin de « *faire preuve de réactivité opérationnelle* » et de « *disposer d'une capacité d'innovation* » face aux enjeux technologiques, notamment en développant ou en administrant des outils numériques de centralisation des renseignements¹. Ces outils ont particulièrement vocation à permettre au GIC de suivre l'exécution des techniques décentralisées via une alerte archivée sur leur activation ou désactivation et d'acheminer les données collectées dans ses infrastructures de manière sécurisée pour en contrôler leur légalité². L'obligation pour les services autres que la DGSE et la DGSi d'utiliser les outils du GIC constitue, selon nous et Renaud Vedel³, un moyen technique puissant de contrôle interne. Comme proposé dans le cadre du principe de centralisation⁴, cette obligation utile à l'effectivité du contrôle du GIC pourrait être étendue à l'ensemble des services sous la forme d'une obligation de recourir à des outils certifiés par le GIC et le Premier ministre.

En outre, on relèvera que, dans son avis de 2015 sur le projet de loi relative au renseignement, le sénateur, Jean-Pierre Raffarin, avait proposé « *de déployer des cellules du GIC directement auprès des services* » pour « *garantir une traçabilité sans défaut de l'exécution de l'ensemble des techniques autorisées* » et, par là même, renforcer le contrôle interne⁵. Cette solution fait néanmoins doublons, selon nous, avec le développement de cellules internes de conformité dans les services mais présenterait un intérêt pour le contrôle des techniques décentralisées. Reprenant l'idée évoquée dans le cadre du contrôle hiérarchique, un agent du GIC pourrait effectivement être chargé, au sein des services, d'assurer le rôle d'agent superviseur chargé de l'effacement des renseignements inutiles collectés par les

¹ Cf. SGDSN, *Rapport d'activité 2019-2020*, p. 40 et 41.

² Voit à ce sujet G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 76.

³ Cf. R. Vedel, *Les contrôles internes*, Le droit du renseignement, op. cit..

⁴ Cf. supra. §3 de la Section I du Chapitre I du Titre II.

⁵ Cf. J. -P. Raffarin, *Avis sur le projet de loi relatif au renseignement*, op. cit., p. 41 et 42.

techniques décentralisées puisqu'il s'agit d'une mission généralement dévolue au GIC.

Cependant, l'adaptation du GIC aux besoins numériques du renseignement nécessite pour le service du Premier ministre de disposer d'infrastructures d'hébergement capables d'accueillir d'important volumes de données, de se doter de personnels compétents et d'adopter des pratiques de développement informatique conforme à l'évolution des normes techniques. Or, si le SGDSN a annoncé la création de nouvelles infrastructures¹, la DPR a considéré que la réorganisation du GIC demeure encore insuffisante pour répondre aux enjeux techniques dénonçant même « *des pratiques de développement non conformes aux règles de l'art* »². Pour autant, la CNCTR a pleinement reconnu les compétences technico-juridiques de contrôle du GIC à tel point d'envisager de lui déléguer la quasi-totalité de son contrôle de la technique dite de « l'annuaire inversé ».

2. La question d'une délégation possible du contrôle de la Commission nationale de contrôle des techniques de renseignement

Les demandes d'identification d'abonnés ou de recensement de numéros d'abonnement sont soumises à un régime dérogatoire car directement transmises pour avis à la CNCTR par les agents concernés des services³. Considérant ces mesures comme des mesures préparatoires faiblement intrusives, la Commission exerce un contrôle réduit « d'erreur manifeste d'appréciation » qu'elle propose de déléguer au GIC, sauf lorsque ces mesures concernent des personnes particulièrement protégées par la loi (parlementaires, magistrats, avocats et journalistes)⁴. Si cette proposition s'inscrit dans un objectif d'amélioration pratique du contrôle de la CNCTR en s'appuyant sur les compétences technico-juridiques du GIC, elle nous semble insatisfaisante. En effet, on ne peut que

¹ Cf. SGDSN, *Rapport d'activité 2019-2020*, p. 40 et 41.

² Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 58.

³ Alinéa 2 de l'article L. 851-1 du code de la sécurité intérieure.

⁴ Cf. CNCTR, *3^{ème} rapport annuel (2018)*, p. 44 à 49 ; G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 176 et suivantes.

souscrire aux critiques formulées par la DPR¹ et le « rapport Larrivé »² soulevant, d'une part, l'insécurité juridique, au niveau constitutionnel, d'une concentration du contrôle de la technique de l'annuaire inversé au sein du GIC qui demeure un opérateur technique de la surveillance et, d'autre part, l'absence d'une évolution positive de la procédure pour les services voire le risque d'une charge trop lourde pour le service du Premier ministre. Au demeurant, il nous semble peu recommandable, de manière générale, d'opérer une quelconque délégation du contrôle de la CNCTR, qui est un contrôle externe, vers le GIC, qui reste un contrôle interne.

Si le GIC est un maillon incontournable dans la chaîne du contrôle hiérarchique des techniques de renseignement (légalité et opportunité), il exerce un contrôle interne plus particulier sur la faisabilité technique de la surveillance, le développement informatique des services ainsi que sur l'exécution des techniques via les opérateurs. Ces prérogatives conduisent ce service technico-juridique neutre à placer le modèle français de renseignement dans une situation singulière où se distingue surveillance technique produite par les services et technique de la surveillance opérée sous le contrôle du GIC, ces fonctions étant habituellement confondues au sein des différents services ou dans une agence autonome de renseignement numérique. La distinction posée par le modèle français présente assurément une garantie contre les risques de dérives des services puisque ces derniers agissent dans un cadre exigeant et contraint tant sur le plan juridique que technique. Pour autant, l'augmentation continue des moyens numériques de renseignement autorisés par la loi et la réorganisation technologique du GIC pour renforcer ces capacités soulèvent inévitablement la question du basculement vers un modèle d'agence autonome à l'instar de la NSA américaine ou du GCHQ britannique³.

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 55.

² Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 176 et suivantes.

³ En ce sens, voir F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

§3. Le contrôle du ministre chargé des communications électroniques sur les opérateurs du numérique

Chargés d'effectuer sur leurs réseaux les opérations matérielles nécessaires à la mise en place des techniques de renseignement sur ordre du Premier ministre¹, les opérateurs du numériques se soumettent également à un contrôle interne exercé par le ministre chargé des communications électroniques. En effet, l'article L. 871-3 du code de la sécurité intérieure prévoit que, dans le cadre de ses attributions qui lui sont conférées par le livre II du code des postes et des communications électroniques, le ministre contrôle la bonne application des dispositions relatives aux techniques de renseignement et au respect du secret de la défense nationale par les opérateurs.

On aurait pu raisonnablement penser que ce contrôle interne aurait été plus à même d'être exercé par le GIC en raison de sa proximité avec les opérateurs. Toutefois, on remarquera une certaine cohérence entre le code de la sécurité intérieure et le code des postes et des communications électroniques, ce dernier disposant que :

« L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur : [...] e) Les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre et celles qui sont nécessaires pour répondre, conformément aux orientations fixées par l'autorité nationale de défense des systèmes d'informations, aux menaces et aux atteintes à la sécurité des systèmes d'information des autorités publiques et des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense »².

Et à ce titre, l'article L. 32-1 du même code confirme que la fonction de régulation du secteur des communications électroniques est, en partie, exercée

¹ Article L. 871-6 du code de la sécurité intérieure.

² Article L. 33-1-I-e) du code des postes et des communications électroniques.

par le ministre chargé des communications électroniques¹. Pour autant, nul doute en fait que le GIC opère également un contrôle de la bonne application matérielle des techniques de renseignement par les opérateurs, ce qui devrait nécessairement conduire à un dialogue entre le service du Premier ministre et les agents du ministre chargé des communications électroniques.

Dans le cadre de ses attributions conférées par le livre II du code des postes et des communications électroniques, le ministre peut recueillir des informations et documents et procédé à des enquêtes dans les locaux des opérateurs pour contrôler les mesures adoptées par ces derniers en matière de techniques de renseignement. Plus particulièrement en ce qui concerne le respect du secret de la défense nationale, on relèvera que :

- d'une part, « *le ministre chargé des communications électroniques peut imposer à tout opérateur de soumettre ses installations, réseaux ou services à un contrôle de leur sécurité et de leur intégrité effectué par un service de l'Etat ou un organisme qualifié indépendant désigné par le ministre chargé des communications électroniques et de lui en communiquer les résultats* »² ;
- d'autre part, que ses agents enquêteurs sont en mesure de relever, le cas échéant, des infractions pénales³, notamment relatives aux atteintes au secret de la défense nationale dans le cadre du contrôle des techniques de renseignement.

On notera que le renvoi express à l'obligation de respect du secret de la défense nationale par les opérateurs dans les dispositions de l'article L. 871-3 du code de la sécurité intérieure visait à clarifier aux opérateurs « *la nature des dispositions à adopter* » selon Jean-Jacques Urvoas⁴ ou, autrement dit, à leur rappeler le risque de poursuites pénales en cas de défaillance observée par le ministre chargé des communications électroniques.

¹ La seconde partie de la régulation du secteur des communications électroniques est assurée par l'ARCEP.

² Article L. 33-10 du code des postes et des communications électroniques.

³ Article L. 40 du code des postes et des communications électroniques.

⁴ Cf. La loi n° 2015-912 du 24 juillet 2015 relative au renseignement. *3 questions à Jean-Jacques Urvoas, député (PS) du Finistère, président de la commission des lois de l'Assemblée nationale, Communication Commerce électronique n° 10, Octobre 2015, entretien 9.*

Par ailleurs, ce dernier fixe et contrôle donc la liste des responsables auprès des opérateurs qui sont compétents pour recevoir l'ordre du Premier ministre de mise en œuvre des techniques de renseignement¹.

Enfin, s'il est vrai que les opérateurs apparaissent fortement contrôlés par le gouvernement, il reste que les contrôles opérés par le ministre chargé des communications électroniques répondent à des exigences de cybersécurité et de protection du secret de la défense nationale légitimes eu égard à la montée en puissance des risques de cyberattaques et d'actes d'espionnage numérique. Par l'ampleur de leurs activités publiques et privées, les opérateurs peuvent constituer une cible stratégique de premier plan pour les adversaires de la France et une faille non négligeable pour la politique publique du renseignement.

§4. La reconnaissance des lanceurs d'alerte de la surveillance numérique

Au-delà des interrogations sur le respect de la vie privée et la surveillance de masse, les révélations d'Edward Snowden sur les programmes de surveillance numérique de la NSA en 2013 n'ont pas manqué de poser la question du statut des lanceurs d'alerte en matière de renseignement².

La loi du 24 juillet 2015 relative au renseignement a ainsi consacré un statut et à un mécanisme spécifique de lanceur d'alerte au profit des agents des services dont les dispositions ont été codifiées à l'article L. 861-3 du code de la sécurité intérieure. On notera qu'un statut général des lanceurs d'alerte a été défini en décembre 2016 dans la loi dite « Sapin II »³ et renforcé par une nouvelle loi en 2022⁴ mais qui ne concerne pas les faits couverts par le secret de la défense nationale, ce qui implique que ce statut général n'a pas vocation à s'appliquer au renseignement.

Selon Renaud Vedel, la reconnaissance d'un statut de lanceur d'alerte par la loi relative au renseignement permet aux agents des services de participer « à une

¹ Article R. 872-3 du code de la sécurité intérieure.

² Voir notamment J. Mafart, *Lanceur d'alerte*, Dictionnaire du renseignement, op. cit., p. 501 à 504.

³ Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

⁴ Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

action de contrôle interne »¹. Si l'on peut y voir alors une avancée indéniable pour l'Etat de droit, cette reconnaissance ne doit pas, pour autant, occulter certaines atténuations qui peuvent être soulevées tout au long des dispositions de l'article L. 861-3 et certaines réflexions sur l'extension du mécanisme.

A - Les atténuations du mécanisme de l'article L. 861-3 du code de la sécurité intérieure

Il est possible de distinguer trois items pouvant faire l'objet de remarques sur le mécanisme envisagé par les dispositions de l'article L. 861-3 : les personnes visées par le statut, les faits qui peuvent être relevés et la procédure et ses effets.

1. Les personnes visées par le statut

Selon le texte, le statut de lanceur d'alerte en matière de renseignement vise seulement les agents des services désignés aux articles L. 811-2 et L. 811-4 du même code, c'est-à-dire les agents des services spécialisés de renseignement et des services du second cercle (au sens large) autorisés à recourir aux techniques de renseignement. Bien que des agents puissent désormais participer directement à la mise en œuvre de certaines techniques de renseignement (IMSI-catcher, balise, outils de sonorisation et de captation d'images ou de données) et relever, à cette occasion, des illégalités, il reste que la majorité des techniques sont exécutées via le GIC et les opérateurs numériques. Les agents des services ne sont donc pas toujours les mieux positionnés pour rendre le mécanisme de lanceur d'alerte effectif dans l'exécution des techniques. En outre, les règles du secret de la défense nationale, notamment la règle du « besoin d'en connaître », pourraient rendre difficile l'exercice de lanceur d'alerte pour les agents des services et font obstacles à ce que les personnels des opérateurs agissant dans la mise en œuvre des techniques puissent bénéficier du statut général de lanceur d'alerte².

2. Les faits pouvant être relevés

Les alertes doivent porter sur des « *faits susceptibles de constituer une violation manifeste* » des dispositions du code de la sécurité intérieure relative au renseignement. Si cette formulation présente l'intérêt de concerner toutes les

¹ Cf. R. Vedel, *Les contrôles internes*, Le droit du renseignement, op. cit., p. 159.

² En ce sens, voir X. Latour, *La loi relative au renseignement : un Etat de surveillance ?*, op. cit..

techniques de renseignement, y compris les mesures non soumises à autorisation préalable du Premier ministre (piratage informatique à l'étranger et cyber-patrouilles administratives), il n'en demeure pas moins que c'est bien spécifiquement l'utilisation des moyens numériques de recherche et de collecte des renseignements qui sont visés par le mécanisme¹. La DPR avait finalement regretté cette limitation du champ d'intervention des lanceurs d'alerte en déplorant que le mécanisme ne couvre pas l'ensemble des activités des services, considérant même cette situation comme une « lacune législative » porteuse de risque d'alertes « sauvages » portée à la connaissance de personnes non habilités².

3. La procédure et ses effets

Seule la CNCTR peut être alertée par les agents des services d'une violation manifeste. La Commission en avise alors le Premier ministre et use, le cas échéant, de ses pouvoirs de contrôle afin d'établir la réalité des allégations. En cas de violation constatée, elle est en droit de saisir le Conseil d'Etat dans le cadre du contentieux des techniques de renseignement et d'aviser le procureur de la République si la violation concerne une infraction ainsi que la Commission du secret de la défense nationale (CSDN) pour la transmission de documents classifiés³.

Pour l'agent agissant « de bonne foi », le respect de cette procédure lui confère une protection juridique, non seulement, contre toutes poursuites pénales mais aussi contre toutes sanctions disciplinaires ou statutaires, le texte affirmant même que tout acte de l'administration préjudiciable à l'agent, comme par exemple une décision de rupture du contrat de travail, fondé sur l'alerte doit être considéré comme « nul et non avenue ». En outre, il revient à l'administration la charge de prouver qu'une mesure statutaire ou une sanction disciplinaire prise à l'égard d'un agent lanceur d'alerte a été justifiée par des « *éléments objectifs étrangers à la déclaration ou au témoignage de l'agent intéressé* ». A l'inverse, lorsque l'agent agit « de mauvaise foi » ou « avec l'intention de nuire », il ne

¹ Sur ce point, voir P. Bas, *Rapport sur le projet de loi relatif au renseignement et sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, op. cit., p. 98 et 99.

² Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 192 à 195.

³ Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p.85 et suivantes.

bénéficie plus de la protection accordée par l'article L. 861-3 du code de la sécurité intérieure et peut être poursuivi pour le délit de dénonciation calomnieuse prévu à l'article 226-10 du code pénal¹.

Alors que le mécanisme de lanceur d'alerte protège les signalements ou témoignages, on pourra là encore regretter, comme pour un certain nombre d'auteurs, que le législateur n'ait pas prévu la possibilité pour les agents des services de transmettre à l'appui de leurs allégations des informations classifiés². Néanmoins, une telle transmission pourrait s'avérer contraire au droit positif du renseignement dans le cas où des informations classifiées ne concernant pas les techniques de renseignement seraient transmises à la CNCTR, ce qui excéderait les compétences de la Commission et constituerait une violation des règles du secret de la défense nationale.

Enfin, on soulignera que les rapports successifs de la CNCTR nous informent qu'aucune procédure d'alerte n'a été déclenchée depuis la création du mécanisme en 2015, ce qui pourrait être, en partie, dû aux atténuations soulevées sur les dispositions de l'article L. 861-3. Il nous semble que ce mécanisme est perfectible et qu'il pourrait faire l'objet d'une extension.

B - L'extension possible du mécanisme de l'article L. 861-3 du code de la sécurité intérieure

En réponse aux atténuations soulevées précédemment, il pourrait être envisagé une extension du statut de lanceur d'alerte à d'autres acteurs du renseignement numérique et, selon la DPR, d'étendre le mécanisme à l'ensemble des activités de renseignement.

1. Etendre le statut à d'autres acteurs du renseignement numérique

A notre sens, le statut de lanceur d'alerte prévu par l'article L. 861-3 pourrait également concerner, du moins, les agents du GIC. Il nous semble, qu'en matière de violation manifeste des dispositions relatives aux techniques de renseignement, la participation des agents du GIC au mécanisme de contrôle

¹ Sur ce point, voir P. Bas, *Rapport sur le projet de loi relatif au renseignement et sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, op. cit., p. 98 et 99.

² Voir à ce sujet R. Parizot, *Surveiller et prévenir... à quel prix ?*, op. cit. ; E. Alt, *De nouvelles protections pour les lanceurs d'alerte*, La Semaine Juridique Edition Générale n° 4, 23 janvier 2017, doctr. 90 ; N. Catelan, *Les nouveaux textes relatifs au renseignement : un moindre mal*, op. cit..

interne qu'implique les lanceurs d'alerte soit, tout autant si ce n'est plus que les agents des services, pertinent au regard de leurs missions technico-juridiques opérées au plus près de la mise en œuvre des techniques.

Au plus, il pourrait être également étendu le statut aux personnels des opérateurs du numérique habilités au secret de la défense nationale. Cette extension ne nous semble pas une idée baroque dans la mesure où la CNCTR peut, à des fins de contrôle, se voir communiquer des informations par ces derniers et accéder à leurs locaux utilisés pour les techniques de renseignement¹.

2. Etendre le mécanisme à l'ensemble des activités de renseignement

Déplorant le champ limité d'intervention des lanceurs d'alerte en matière de renseignement, la DPR s'est montrée favorable à l'extension du mécanisme à l'ensemble des activités de renseignement. Le nouveau dispositif envisagé par les parlementaires consiste à une saisine directe par les agents concernés de la DPR « *pour toutes les questions liées à l'activité des services, à l'exclusion de celles des techniques de renseignement déjà couverte par la loi du 24 juillet 2015* » ou a pouvoir saisir la Commission de vérification des fonds spéciaux (CVFS) qui émane de la DPR « *pour toute les questions relatives à l'emploi des fonds spéciaux* »².

Au lieu d'ajouter un nouveau dispositif à celui déjà prévu par la loi relative au renseignement, il pourrait être proposé de modifier la portée du mécanisme de l'article L. 861-3 qui concernerait alors l'ensemble de la politique publique du renseignement. Dans ce cas, la modification pourrait introduire la possibilité pour les agents de transmettre des informations classifiées à la CNCTR ainsi que de signaler des violations en matière de fichiers de renseignement. Néanmoins, ces propositions reviendraient à devoir nécessairement étendre le périmètre de contrôle de la Commission à l'ensemble des activités de renseignement ou encore à prévoir une éventuelle intervention de la CNIL.

Quoi qu'il en soit, une extension du mécanisme des lanceurs d'alerte à l'ensemble des activités de renseignement ne peut être envisagée qu'à travers la saisine de la CNCTR ou de la DPR. Comme souligné par cette dernière, la

¹ Article L. 871-4 du code de la sécurité intérieure.

² Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 196 et 197.

Coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) ou l'Inspection des services de renseignement ne peuvent recevoir les alertes en raison de leur manque d'indépendance vis-à-vis de l'Exécutif¹.

§5. L'orientation et l'évaluation des moyens numériques par l'Exécutif

Si la loi relative au renseignement de 2015 a pris soins d'affirmer l'application du principe de légalité aux activités des services spécialisés de renseignement, elle a également tenu à rappeler que ces derniers agissent « *sous l'autorité du Gouvernement et conformément aux orientations déterminées par le Conseil national du renseignement* »². Autrement dit, le recours aux techniques de renseignement et, plus largement, à des moyens numériques font l'objet d'un contrôle interne par l'Exécutif, c'est-à-dire autant par le Président de la République que par le gouvernement au regard de l'organisation de la communauté française du renseignement.

Ce contrôle se manifeste par une orientation des moyens numériques de renseignement par le Conseil national du renseignement (CNR) et d'un suivi par le Coordonnateur national du renseignement. De façon plus restreinte, il se présente sous la forme d'une évaluation réalisée par l'Inspection des services de renseignement sur mandat du Premier ministre.

A - Le Conseil national du renseignement et le Coordonnateur national du renseignement

Institué par un décret du 24 décembre 2009³ à la suite des propositions du Livre blanc sur la sécurité et la défense nationale de 2008, le Conseil national du renseignement (CNR) est une formation spécialisée du Conseil de défense et de sécurité nationale tenue par le Président de la République qui fixe les grandes orientations stratégiques de la politique publique du renseignement⁴. L'ordre du

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 196 et 197.

² Article L. 811-2 du code de la sécurité intérieure.

³ Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au Secrétariat général de la Défense et de la Sécurité nationale.

⁴ Voit à ce sujet J. Poirot, *Conseil national du renseignement*, Dictionnaire du renseignement, op. cit., p. 178 à 180.

jour de ce conseil, son secrétariat ainsi que le suivi des décisions qui y sont prises sont traités, avec le concours du SGDSN, par le Coordonnateur national du renseignement qui est un conseiller du Président de la République¹. En outre, le Coordonnateur « *s'assure de la bonne coopération entre les services spécialisés, qui lui rendent compte de leur activité, et leur transmet les instructions du Président de la République, obtenant en retour les renseignements destinés au chef de l'État et au Premier ministre* »². Sans refaire l'histoire de la coordination des services³, il est désormais acquis que ces derniers sont assujettis au chef de l'Etat tant du point de vue institutionnel, avec la création du CNR et du Coordonnateur, que juridique au regard des dispositions de l'article L. 811-2 du code de la sécurité intérieure.

Alors que ce dernier article semble logiquement charger le chef de l'Etat et le Coordonnateur de veiller à orienter les services dans l'utilisation des techniques de renseignement, les textes relatifs au CNR et à la coordination vont plus loin en matière de numérisation du renseignement. En effet, il revient au CNR de planifier les moyens techniques des services selon l'article R* 1122-6 du code de la défense. Quant au Coordonnateur, l'article R* 1122-8-1 du même code dispose qu'il doit favoriser, sous le contrôle du Président de la République et du Premier ministre, l'utilisation des techniques de renseignement et, plus largement, « *la mutualisation des moyens technologiques entre les services spécialisés* ». En dehors des décisions du CNR et de la coordination quotidienne des services par le Coordonnateur, le respect de ces exigences trouve notamment une traduction dans deux documents qui obligent les services : la Stratégie nationale du renseignement (SNR) produite par la présidence de la République et le Plan national d'orientation du renseignement (PNOR) soumis par le Coordonnateur.

1. La Stratégie nationale du renseignement

« Feuille de route du Renseignement », la Stratégie nationale du renseignement (SNR) est un document prévu par la loi de programmation militaire du 18 décembre 2013 qui n'a pas manqué de souligner que « *les défis technologiques constituent également une priorité pour la communauté du*

¹ Article R*1122-8 du code de la défense.

² Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 33.

³ Pour en savoir plus, voir G. Inchaurreaga, *Coordonnateur national du renseignement*, Dictionnaire du renseignement, op. cit., p. 210 à 214.

Renseignement » et de préciser trois enjeux majeurs à relever pour les services en plus de la mutualisation de leurs moyens techniques :

« o la diffusion de l'expertise entre les services pour permettre à chacun de s'approprier les nouveaux outils ;

o la valorisation des données, de plus en plus volumineuses et hétérogènes ;

o la conception de nouveaux outils en anticipant les évolutions technologiques et en s'appuyant sur une culture de l'innovation en lien avec la Recherche et l'industrie »¹.

On relèvera que le troisième enjeu renvoi à notre analyse sur les innovations numériques sur les données, notamment aux perspectives d'un cadre spécifique à la recherche en renseignement en matière d'IA permettant à la communauté du renseignement de bénéficier des expertises du secteur privé et de la recherche pour le développement de solutions souveraines².

2. Le Plan national d'orientation du renseignement

« Première étape du cycle du renseignement », le PNOR est élaboré par le Coordonnateur et approuvé par le CNR pour « *orienter l'action des services de renseignement* »³. Dans le cadre de ce document protégé par le secret de la défense nationale, le Coordonnateur détermine de manière opérationnelle les exigences de planification et de mutualisation des moyens numériques des services en s'attachant, selon la DPR, « *à la réalisation d'un environnement juridique bien adapté à leurs besoins* »⁴.

Cette dernière information nous invite à souligner deux remarques : d'une part, il nous semble impératif que le Coordonnateur veille à assurer l'encadrement juridique des services dans la planification et la mutualisation des moyens numériques puisqu'il s'agit là d'une exigence légale découlant de l'article L. 811-2 du code de la sécurité intérieure qui dispose, rappelons-le, que les services doivent

¹ Stratégie nationale du renseignement, « Les nouveaux enjeux de la coordination : partage, mutualisation, intégration », juillet 2019, p. 11.

² Cf. supra. Section II du Chapitre II du Titre I.

³ Sur ce point, voir P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 27.

⁴ Cf. P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 30.

agir, avant tout, dans le respect de la loi ; d'autre part, il apparaît que le Coordonnateur ait pour mission d'évaluer et/ou de proposer des possibilités de réformes du cadre juridiques des services, notamment en ce qui concerne les besoins numériques. Sur ce dernier point, le Coordonnateur peut s'appuyer sur les travaux de l'Inspection des services de renseignement.

B - L'Inspection des services de renseignement

Créée par le décret n° 2014-833 du 24 juillet 2014, l'Inspection des services de renseignement (ISR) « *réalise des missions de contrôle, d'audit, d'étude, de conseil et d'évaluation* » des services et de l'académie du renseignement. Elle est placée sous l'autorité du Premier ministre et effectue ses missions sur instructions de ce dernier. Ses travaux font l'objet d'un rapport qui est remis au Premier ministre, aux ministres concernés et au Coordonnateur national du renseignement. On relèvera que, selon la CNCTR, « *l'inspection veille au respect de la légalité, de l'éthique et de la déontologie des services concernés* »¹. Les sujets de contrôle de l'ISR intéressent l'ensemble des activités des services et, en ce qui nous concerne comme le souligne Renaud Vedel, « *peuvent porter sur les conditions de recueil, d'exploitation ou de conservation des données et informations acquises par le biais des techniques de renseignement* »². D'ailleurs, on relèvera que l'ISR est particulièrement sollicitée pour évaluer les besoins numériques des services :

- en 2015, l'ISR a réalisé un rapport sur la mise en œuvre de la loi de 2015 en matière de techniques de recueil de renseignement³ ;
- à plusieurs reprises⁴, la DPR a demandé que l'ISR réalise une étude sur l'utilisation des fichiers de souveraineté par les services ;
- dans son rapport d'activité 2019-2020, la DPR a formulé la proposition de confier une mission de contrôle de l'ISR sur la traçabilité des techniques de renseignement⁵.

¹ Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 24 et 25.

² Cf. R. Vedel, *Les contrôles internes*, Le droit du renseignement, op. cit., p. 158.

³ Voir à ce sujet P. Adam, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016, DPR, 2 mars 2017, p. 25.

⁴ Voir sur ce point les propositions des rapports d'activité de la DPR pour les années 2014, 2015 et 2016.

⁵ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 61 et 62.

Par ailleurs, il semblerait que l'ISR ait un rôle à jouer en matière de conseil et de contrôle des capacités des services dans le domaine de la cyberdéfense, notamment pour le partage du renseignement d'intérêt cyber (RIC) que le Coordonnateur a pour mission de favoriser conformément à ses prérogatives définies par les textes réglementaires, à la SNR ainsi qu'à la stratégie nationale de cyberdéfense¹.

En ce qui concerne les moyens de l'Inspection, on retiendra qu'elle dispose, en plus de pouvoir accéder aux locaux des services et aux informations et documents utiles à sa mission, d'un personnel compétent sur les questions technologiques car les inspecteurs qui la compose peuvent être choisis parmi les fonctionnaires experts sur ces questions du contrôle général des armées ou du conseil général de l'économie, de l'industrie, de l'énergie et des technologies². Pour aller plus loin et dans la continuité de la désignation d'un Secrétaire général permettant une « *permanence et la possibilité d'une programmation de longue durée* »³, il pourrait être envisagé la mise en place d'un contrôle continu des besoins numériques des services pour veiller, dans un premier temps, au respect des règles de l'état de l'art des technologies en plus du respect de la légalité, de l'éthique et de la déontologie et, dans un second temps, pour proposer des réponses aux évolutions technologiques.

Enfin, au regard des orientations du SNR, de la mission du Coordonnateur qui consiste à renforcer l'utilisation des techniques et la mutualisation des moyens numériques ainsi que des évaluations de l'ISR pour le compte de l'Exécutif, il nous apparaît opportun de rappeler que le contrôle ainsi exercé par ce dernier sur les services de renseignement, quand bien même il est exercé au plus haut sommet de l'Etat, ne doit pas conduire à orienter les services dans une logique de surveillance numérique liberticide. Dans tous les cas, l'Exécutif comme les services de renseignement font l'objet de contrôles externes très attentifs sur les moyens numériques des services.

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 255.

² Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 24 et 25.

³ A ce sujet, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 76 à 78.

SECTION II : Les contrôles externes

Au cœur de l'organisation et du fonctionnement de la politique publique du renseignement, les moyens numériques des services font logiquement l'objet d'un contrôle politique par le Parlement (§1). En ce qui concerne la légalité de l'utilisation de ces moyens, la CNCTR voit nécessairement son contrôle se renforcer dans le cadre des techniques de renseignement (§2) alors que le contrôle de la CNIL en matière de fichiers tend à être remis en question en raison de ses limites (§3). Enfin, bien que les techniques et les fichiers de renseignement n'échappent plus au contrôle du juge, on peut regretter que les contentieux portés devant la formation spécialisée du Conseil d'Etat s'articule de manière « trop spécialisée » (§4).

§1. Le contrôle politique des moyens numériques par le Parlement

Malgré sa tardive mise en place en 2007 par rapport à la majorité des démocraties libérales¹, le contrôle parlementaire du renseignement d'Etat en France, incarné par la Délégation parlementaire au renseignement (DPR), n'a cessé de se renforcer au fil des textes encadrant les services. Initialement cantonnée au suivi de l'activité générale des services spécialisés, la délégation parlementaire s'est vu confier par la loi de programmation militaire du 18 décembre 2013 un véritable rôle de contrôle de l'action du gouvernement et d'évaluation de la politique publique du renseignement plus en conformité avec l'article 24 de la Constitution de 1958². Par la suite, les lois relatives au renseignement de 2015 et de 2021 ont étendu les prérogatives de la DPR, jusqu'à lui confier également une mission de « *suivi des enjeux d'actualité et des défis à venir en matière de renseignement* »³.

Définies à l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958, les prérogatives de la DPR lui permettent d'opérer un contrôle politique

¹ En ce sens, voir J. -C. Cousseran et P. Hayez, *Leçon sur le Renseignement*, op. cit., p. 359 à 367.

² Voir en ce sens Y. Braun-Pivet, *Dix ans de contrôle parlementaire du renseignement : l'exigence démocratique est-elle satisfaite ?*, *Le droit du renseignement*, op. cit., p. 139 à 146.

³ Voir sur ce point P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement*, op. cit..

dans le domaine de la numérisation du renseignement. Plus encore, les lois relatives au renseignement ont même organisé un suivi continu du Parlement sur l'application des techniques numériques de recueil des renseignements.

A - Le cadre général du contrôle de la politique publique du renseignement

Le renseignement numérique n'échappe pas au périmètre de contrôle de la DPR et, selon les rapports de cette dernière, se révèle être une problématique récurrente du contrôle parlementaire. On remarquera d'ailleurs que les moyens de contrôle de la délégation parlementaire portent, de manière non négligeable, sur le renseignement numérique.

1. Un périmètre de contrôle couvrant le renseignement numérique

Depuis sa création, la DPR a toujours été compétente pour exercer un suivi technologique des services de renseignement. La majorité de ses travaux sont notamment consacrés à l'évaluation de leurs besoins numériques. Ainsi, on relèvera que la DPR a contribué à mettre en place le système PNR au niveau national à partir de 2014¹. De façon évidente, elle s'est consacrée en 2015 à l'examen du projet de loi relatif au renseignement et notamment sur « *le renforcement des moyens de contrôle de la mise en œuvre des techniques de recueil du renseignement* » et « *l'accroissement des moyens humains et techniques des services de renseignement* »². Plus récemment, la DPR s'est saisie de la question des activités de renseignement dans le cyberspace et dans l'organisation de la cyberdéfense tout en prolongeant son évaluation sur le cadre juridique des techniques de renseignement, y compris au regard du contentieux porté devant la CJUE en matière de protection des données personnelles³.

Il convient cependant de rappeler que la DPR n'est pas en droit de pouvoir contrôler les opérations en cours, les méthodes opérationnelles ainsi que les échanges internationaux de renseignement selon la jurisprudence

¹ Cf. P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 19 et suivantes.

² Cf. J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 16.

³ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 21 et suivantes.

constitutionnelle¹. En ce qui nous concerne, cette jurisprudence fait obstacle à ce que la DPR puisse accéder aux détails des procédures et outils techniques utilisés par les services dans la numérisation de leurs activités (codes sources des algorithmes par exemple) même si elle peut connaître des activités opérationnelles achevées depuis la loi de programmation militaire de 2013². Si la DPR a pu juger utile de proposer d'intégrer les procédures et méthodes opérationnelles dans le champ de son contrôle³, il nous semble préférable de conserver la solution du Conseil constitutionnel en matière de capacités technologiques des services dans la mesure où, eu égard à l'importance stratégique des moyens numériques, les risques de compromission des procédures et méthodes dans ce domaine constitue aujourd'hui un enjeu majeur de souveraineté et de capacité d'action des services. En revanche, la DPR dispose légalement de moyens lui permettant d'être tenue informée sur l'utilisation des techniques de renseignement et sur les orientations technologiques du renseignement d'Etat.

2. Des moyens de contrôle portant sur le renseignement numérique

L'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 a été complété à plusieurs reprises pour étendre les moyens de la DPR, notamment par les textes qui ont renforcé les moyens techniques des services. Ces moyens relatifs à l'accès de la DPR à certains documents et informations et aux auditions des acteurs du renseignement sont, pour une large part, consacrés à l'évaluation du renseignement numérique.

Les documents et informations accessibles

La loi de programmation militaire de 2013 a tout d'abord obligé le gouvernement à communiquer à la DPR : la SNR, des éléments d'information sur le PNOR ainsi que deux rapports annuels portant sur une synthèse des crédits consacrés au renseignement et sur l'activité et l'organisation des services. Sans revenir sur la SNR et le PNOR déjà évoqués précédemment, il convient de préciser que les deux rapports annuels comportent des éléments relatifs aux ressources

¹ Décision n° 2001-456 DC du 27 décembre 2001.

² Cf. P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017*, op. cit., p. 21.

³ Ibid., p. 40.

techniques des services, notamment sur les crédits alloués aux techniques de renseignement. On relèvera cependant que la DPR souhaiterait obtenir également « *des éléments relatifs aux capacités de traitement de l'information qui devient un enjeu des politiques publiques de renseignement : compte tenu de l'abondance des données collectées* »¹ ou encore davantage d'informations concrètes sur les « *coopérations techniques et fonctionnelles* »². Si ces enjeux peuvent être considérés comme relevant des procédures et méthodes opérationnelles protégées par la jurisprudence constitutionnelle, il n'en demeure pas moins qu'ils concernent effectivement l'organisation et le fonctionnement des services au regard de la montée en puissance du renseignement numérique.

Ensuite, la première loi relative au renseignement de 2015 a introduit la possibilité pour la DPR de se voir communiquer « *les observations que la Commission nationale de contrôle des techniques de renseignement adresse au Premier ministre en application de l'article L. 833-10 dudit code ainsi qu'une présentation, par technique et par finalité, des éléments statistiques figurant dans le rapport d'activité de la commission mentionné à l'article L. 833-9 du même code* »³. On ajoutera que la loi SILT du 30 octobre 2017 permet à la CNCTR de communiquer des recommandations et observations à la DPR sur l'application du régime dérogatoire de la surveillance hertzienne⁴. En outre, la loi de 2015 a également prévu un pouvoir de saisine de la CNCTR pour avis par les présidents de l'Assemblée nationale et du Sénat et la DPR⁵. La seconde loi relative au renseignement de 2021 a continué de renforcer les prérogatives de la DPR en lui permettant d'accéder régulièrement (base semestrielle) à liste des rapports de l'ISR et des autres inspections générales portant sur les services ainsi que de solliciter l'accès à tout ou partie de ces rapports mais aussi à « tout autre

¹ Cf. P. Bas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017*, op. cit., p. 28.

² Cf. Y. Braun-Pivet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018*, op. cit., p. 32.

³ 5° du I. de l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

⁴ Article L. 855-1 C du code de la sécurité intérieure.

⁵ Article L. 833-11 du code de la sécurité intérieure.

document, information et élément d'appréciation nécessaire à l'accomplissement de sa mission », dans la limite du besoin d'en connaître.

Les auditions

On rappellera que, de manière générale, la DPR peut entendre le Premier ministre, les ministres concernés, le secrétaire du SGDSN, le Coordonnateur national du renseignement, le directeur de l'Académie du renseignement, les directeurs des services sur des questions relevant du renseignement numérique. Plus particulièrement sur ces questions, on relèvera que la délégation parlementaire peut auditionner les personnes spécialement déléguées par le Premier ministre pour délivrer des autorisations de mise en œuvre des techniques de renseignement ou encore le président de la CNCTR, notamment pour lui présenter le rapport d'activité de la Commission. Depuis la seconde loi relative au renseignement du 30 juillet 2021, une avancée significative a été consacrée en permettant à la DPR d'entendre des personnes exerçant des fonctions de direction au sein du GIC mais aussi dans l'ensemble des services de renseignement, ce qui peut viser des directeurs de services techniques. Enfin, on soulignera par ailleurs que les membres de la délégation parlementaire peuvent élargir leurs auditions à d'autres directeurs des autres administrations centrales et qu'ils ont usé de cette faculté pour entendre le chef d'état-major des armées, le commandant de la cyberdéfense ou encore le directeur de l'ANSSI sur « *la question de la cyberdéfense et du renseignement militaire dans l'espace* »¹.

B - Le cadre spécifique de l'application des techniques de renseignement

Les deux lois relatives au renseignement de 2015 et de 2021 ont spécialement prévu un contrôle parlementaire de l'application des techniques de renseignement. Ainsi, l'article 27 de loi du 24 juillet 2015 a confié au Parlement une mission d'évaluation de l'application des dispositions de cette même loi dans un délai maximal de cinq ans après son entrée en vigueur. Cette obligation légale a été suivie d'effet en 2020 avec l'adoption du rapport d'information présidé par le député Guillaume Larrivé sur l'évaluation de la loi du 24 juillet 2015 relative au

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 23.

renseignement qui traite pour une grande partie sur la numérisation du renseignement et ses défis technologiques. Plus spécialement, l'article 25 de la loi de 2015 a contraint le gouvernement à adresser au Parlement, au plus tard le 30 juin 2018, un rapport sur l'application des dispositions relatives à la technique algorithmique de détection des menaces terroristes¹. Cependant, le législateur est intervenu à deux reprises, en 2017 et en 2020, pour repousser la remise du rapport avant le 31 juin 2021². Finalement, le dispositif de l'article L. 851-3 a été prolongé et renforcé par la loi seconde loi relative au renseignement relative au du 30 juillet 2021 qui, en raison notamment de l'intégration des données URL dans le dispositif, a également prévu la transmission d'un nouveau rapport par le gouvernement au Parlement avant le 31 juillet 2024. En outre, l'article 13 de loi de 2021 exige également la production d'un rapport du gouvernement au Parlement sur l'application des dispositions relatives aux nouvelles interceptions satellitaires³ avant le 31 juillet 2025.

Enfin, on ne manquera pas de souligner que la DPR a été destinataire d'un rapport classifié en 2020 sur l'application de la technique algorithmique alors même qu'aucun texte ne le prévoyait⁴. A notre sens, cette solution pratique, qui s'inscrit dans la nécessité de contrôler fortement le recours aux techniques de renseignement, participe au renforcement du contrôle parlementaire du renseignement initié depuis la création de la DPR. Face à l'importance croissante du renseignement numérique, c'est aussi le renforcement du contrôle exercé par le CNCTR qui est apparu nécessaire.

¹ Article L. 851-3 du code de la sécurité intérieure.

² Voir sur ce point B. Warusfel, *Quelles réformes pour le droit du renseignement ?*, op. cit., 2021, p. 148.

³ Article L. 852-3 du code de la sécurité intérieure.

⁴ Cf. F. Dumas et F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021, DPR*, op. cit., p. 15.

§2. Le renforcement nécessaire du contrôle de la Commission nationale de contrôle des techniques de renseignement

La Commission nationale de contrôle des techniques de renseignement (CNCTR) est l'autorité la plus spécialisée dans le contrôle du renseignement numérique. En effet, elle est une autorité administrative indépendante (AAI) spécialement chargée d'assurer le respect des principes régissant la mise en œuvre des techniques de renseignement du code de la sécurité intérieure¹.

Héritière de la Commission nationale de contrôle des interceptions (CNCIS), la CNCTR a été créée par la loi du 24 juillet 2015 en réponse à la montée en puissance des techniques numériques de renseignement par cette même loi². Non plus seulement chargée du contrôle des interceptions de sécurité et des accès administratifs aux données de connexion, la CNCTR a vu son rôle largement se renforcer et s'affirmer pour appréhender les nouveaux moyens numériques consacrés depuis 2015. Cependant, l'exercice de son contrôle souffre encore de certaines limitations qui interrogent sur un dépassement nécessaire de son cadre d'intervention.

A - L'affirmation du contrôle sur le renseignement numérique

Dans le prolongement de la régulation de la numérisation croissante des activités de renseignement, la CNCTR a acquis juridiquement des pouvoirs étendus tout en disposant de moyens de contrôle plus adaptés à cette numérisation.

1. Des pouvoirs étendus

Tout d'abord, il convient d'observer que la loi n'a cessé d'élargir la compétence de la CNCTR aux activités numériques des services de renseignement. Ensuite, soulignons que la Commission a bénéficié de pouvoirs très importants, notamment sous l'impulsion du droit européen de la protection des données, entraînant alors une véritable rupture avec la CNCIS et non plus une « continuité relative »³.

¹ Article L. 801-1 du code de la sécurité intérieure.

² Sur ce point, voir Etude d'impact, *Projet de loi relatif au renseignement*, op. cit., p. 56 et 57.

³ En ce sens, voir C. Guerrier, *La CNCTR, une rupture ou une continuité avec la CNCIS ?*, Revue Le Lamy Droit de l'immatériel, n° 117, 1^{er} juillet 2015.

Les moyens numériques soumis au contrôle

Le périmètre du contrôle de la CNCTR a été étendu à la quasi-totalité des moyens numériques attentatoires à la vie privée, au secret des correspondances et à la protection des données personnelles prévus par la loi. Ainsi, la Commission a pour mission de veiller à la légalité :

- des techniques de recueil de renseignement mises en œuvre sur le territoire national¹. Son contrôle s'exerce aussi bien sur les demandes (*a priori*) que sur la mise en œuvre (*a posteriori*) ;
- des mesures de surveillance des communications électroniques internationales autorisées en vertu des dispositions de l'article L. 854-2 du code de la sécurité intérieure. Si le contrôle exercé par la CNCTR était initialement limité à un contrôle *a posteriori*, la Commission s'est vu reconnaître un pouvoir de contrôle *a priori* en pratique² avant que celui-ci soit affirmé par la loi de programmation militaire du 13 juillet 2018 pour ce qui concerne les demandes mentionnées aux III et V de l'article L. 854-2 ;
- depuis 2017³, des mesures de surveillance des communications hertziennes « ouvertes »⁴ dans le cadre d'un contrôle *a posteriori* du respect des champs d'application des dispositions relatives à ces mesures et aux techniques de renseignement mises en œuvre sur le territoire national⁵ ;
- depuis 2021⁶, des paramètres techniques applicables aux programmes de recherche en IA sur les renseignements collectés⁷ et des échanges de

¹ Article L. 833-1 du code de la sécurité intérieure.

² Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 45.

³ Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

⁴ Article L. 855-1 C du code de la sécurité intérieure.

⁵ Cf. CNCTR, *3^{ème} rapport annuel (2018)*, p. 79.

⁶ Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

⁷ Article L. 822-2 du code de la sécurité intérieure.

renseignements entre services français¹. Sur ces exploitations de données, la CNCTR exerce un contrôle *a priori* et *a posteriori*.

Il est intéressant de relever que le contrôle de la CNCTR s'est élargi au renseignement extérieur et aux techniques numériques non soumises à autorisation de l'exception hertzienne alors que, dans la continuité de la CNCIS, la procédure d'autorisation préalable de mise en œuvre de techniques intrusives sur le territoire national constituait le cadre principal de son intervention. Dans ces conditions, on peut s'interroger sur le maintien de l'exclusion du contrôle de la CNCTR sur les cyber-patrouilles administratives² et sur les actions clandestines de cyberespionnage à l'étranger³. Pour les premières, le dispositif pourrait faire l'objet, selon nous, d'un contrôle *a posteriori* par la Commission au regard des risques d'atteinte à la vie privée des personnes visée par la technique et à la suite de l'évolution juridique de cette même technique en matière judiciaire⁴. Pour les secondes, aucun texte ne fait obstacle à ce qu'un contrôle *a posteriori* du respect des dispositions du code pénal et du code de la sécurité intérieure par la CNCTR puisse être envisagé. Ce contrôle viserait par exemple les cas où les mesures concernées seraient prises à partir du territoire national ou encore à éviter que de telles mesures soient prises depuis l'étranger vers la France. Ainsi, la Commission pourrait se voir accéder aux outils utilisés par les services et aux données collectées afin de déterminer si les mesures prises n'entrent pas dans le champ d'application des techniques de renseignement (comme la captation de données informatiques prévue à l'article L. 853-2 du code de la sécurité intérieure) à l'instar du contrôle de l'exception hertzienne⁵.

¹ Article L. 822 du code de la sécurité intérieure.

² Article L. 861-3 du code de la sécurité intérieure.

³ Article 323-8 du code pénal.

⁴ Depuis la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, l'enquête judiciaire sous pseudonyme a été placée sous le contrôle du procureur de la République ou du juge d'instruction (cf. §2 de la Section II du Chapitre I du Titre I).

⁵ Dans le cadre du contrôle de l'exception hertzienne, la CNCTR « s'est fait présenter les capacités d'interception et a pu consulter les transcriptions et les extractions réalisées à partir des données recueillies » (cf. CNCTR, 3^{ème} rapport annuel (2018), p. 79).

La rupture avec la Commission nationale de contrôle des interceptions de sécurité

Tenant compte des normes nationales, internationales et européennes et des jurisprudences judiciaire, administrative et internationale sur le respect du droit à la vie privée¹, la CNCTR contrôle la légalité et la proportionnalité² des demandes d'autorisation des techniques de renseignement relevant de sa compétence et de leur mise en œuvre³. Notons qu'elle peut être amenée à exercer son contrôle sur réclamation des particuliers⁴. Pour exercer ses missions, la loi reconnaît à la Commission, de manière générale, un droit de communication et d'information sur tous les éléments utiles à son contrôle ainsi qu'un droit d'« accès permanent, complet et direct » aux dispositifs et locaux utilisés pour la mise en œuvre des techniques de renseignement et le stockage des données collectées⁵, ce qui peut également concerner les opérateurs du numérique⁶. On soulignera que le secret de la défense nationale ne lui est pas opposable⁷ et que la loi relative au renseignement de 2015 n'a pas manqué de prévoir des sanctions pénales en cas d'entrave à son action⁸. Pour l'objet de notre étude, on saluera particulièrement le souci du législateur sur l'intégrité des données contrôlées dans sa volonté de sanctionner les communications des transcriptions ou d'extractions non conformes au contenu des renseignements collectés lors de la formulation de la demande⁹.

En ce qui concerne plus spécifiquement le contrôle *a priori*, le législateur de 2015 a donc consacré dans la loi la procédure d'avis préalable de l'AAI qui était pratiquée par la CNCIS. Dans son avis, on relèvera que la CNCTR peut être amenée à poser des restrictions aux autorisations, comme par exemple recommander la

¹ Sur ce point, voir F. Delon, *la Commission nationale de contrôle des techniques de renseignement*, Le droit du renseignement, op. cit., p. 125 à 132.

² Article L.801-1 du code de la sécurité intérieure.

³ Article L. 833-5 du code de la sécurité intérieure.

⁴ Article L. 833-4 du code de la sécurité intérieure.

⁵ Article L. 833-2 du code de la sécurité intérieure.

⁶ Article L. 871-4 du code de la sécurité intérieure.

⁷ Article L. 832-5 du code de la sécurité intérieure.

⁸ Article L. 833-3 du code de la sécurité intérieure.

⁹ Article L. 833-3-2° du code de la sécurité intérieure.

diminution de la durée de validité de l'autorisation pour « *limiter l'usage de la technique à la durée d'un évènement ponctuel* »¹. Néanmoins, l'affirmation dans la loi du contrôle *a priori* par la CNCTR n'a pas été exempte de critiques. En l'absence de caractère contraignant de ses avis, l'autorité de la Commission a pu être questionnée par un certain nombre de commentateurs² qui ont parfois qualifié l'AAI de « magistrature morale »³ ou de « *géant du contrôle passablement désarmé et condamné à la magistrature d'influence* »⁴. Plus encore, si le choix de faire intervenir une AAI à la place du juge judiciaire n'est pas contraire à la jurisprudence du juge constitutionnel relative au droit au respect de la vie privée qui considère que ce droit est rattaché à l'article 2 de la DDHC de 1789 et non pas à l'article 66 de la Constitution de 1958⁵, il n'en demeure pas moins que la jurisprudence constitutionnelle⁶ n'aurait pas non plus systématiquement fait obstacle à ce que la CNCTR soit dotée d'un pouvoir d'avis conforme⁷. On relèvera d'ailleurs que la CNCDH s'était prononcée en faveur de cette possibilité dans son avis sur le projet de loi relative au renseignement de 2015⁸. Pour le Professeur Xavier Latour, « *le législateur aurait pu être plus imaginatif* » en précisant que « *le juge administratif aurait été légitime à intervenir en amont de la décision de police administrative, seul ou en formation collégiale* »⁹ même s'il convient de rappeler que la loi prévoit que la CNCTR n'agit pas seule en lui permettant notamment de saisir le Conseil d'Etat en cas de désaccord avec le Premier ministre¹⁰, ce qui peut

¹ Cf. CNCTR, *1^{er} rapport annuel (2015-2016)*, p. 64.

² Voir en ce sens M. -H. Gozzi, *Sed quis custodiet ipsos custodes ?*, op. cit. ; J. B. de Gubernatis et M. Martin, *La loi relative au renseignement : la victoire de la peur sur l'idéal de protection des droits et libertés ?*, Les Cahiers Portalis, 2016/1 (n°3), p. 75 à 85.

³ En ce sens, voir X. Latour, *La loi relative au renseignement, un Etat de surveillance ?*, op. cit..

⁴ En ce sens, voir O. Desaulnay et R. Ollard, *Le renseignement français n'est plus hors-la-loi*, op. cit..

⁵ Voir sur ce point X. Latour, *La loi relative au renseignement, un Etat de surveillance ?*, op. cit..

⁶ Décision n° 2006-544 DC du 14 décembre 2006, Loi de financement de la sécurité sociale pour 2007.

⁷ A ce sujet, voir C. Lazerges et H. Henrion-Stoffel, *Politique criminelle, renseignement et droits de l'homme*, op. cit..

⁸ CNCDH, ass. plén., *avis sur le projet de loi relatif au renseignement dans sa version enregistrée le 1^{er} avril 2015 à la Présidence de l'Assemblée nationale*, 16 avr. 2015..

⁹ Cf. X. Latour, *La loi relative au renseignement, un Etat de surveillance ?*, op. cit..

¹⁰ Voir sur ce point J. -J. Urvoas, *Était-il tolérable que la France soit le seul État européen où les services de renseignement agissaient en dehors de tout cadre juridique ?*, La Semaine Juridique Administrations et Collectivités territoriales n° 40, 5 Octobre 2015, 2285.

apparaître comme le seul véritable pouvoir significatif de la nouvelle Commission par rapport à la CNCIS¹.

Finalement, les arrêts *Tele2 Sverige de 2016* et *La Quadrature du Net de 2020* de la CJUE fondés sur la protection des données personnelles, confirmés ensuite par l'arrêt *French Data Network* du Conseil d'Etat du 21 avril 2021, entérinent le débat juridique en obligeant le législateur français à instaurer une procédure d'avis préalable contraignante. La loi relative au renseignement du 30 juillet 2021 a donc réaménagé la procédure d'autorisation en introduisant un avis conforme de la CNCTR et une saisine automatique du Conseil d'Etat en cas d'autorisation du Premier ministre après un avis défavorable ainsi que la procédure d'urgence absolue permettant d'outrepasser la censure préalable en l'abrogeant notamment pour la technique algorithmique de l'article L. 851-3 du code de la sécurité intérieure², marquant alors une rupture définitive avec le cadre du contrôle de la CNCIS. On observera, ici, une certaine manifestation, et pas des moindres, de l'affirmation de l'application du droit du numérique au renseignement d'Etat³.

S'agissant du contrôle *a posteriori*, il permet à la Commission un suivi de l'exécution des techniques autorisées et d'apprécier leur bien-fondé⁴. En disposant « *d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions, extractions et transmissions mentionnés au présent livre, aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements en application de l'article L. 822-1 ainsi qu'aux renseignements mentionnés au III de l'article L. 822-2* »⁵, la CNCTR serait en mesure d'exercer « un contrôle complet et effectif »⁶. Cependant, si le contrôle de la Commission couvre l'ensemble du cycle de vie des renseignements collectés, de la collecte des données à leur destruction, il reste que l'AAI ne dispose que d'un

¹ En ce sens, voir E. Daoud et G. Péronne, *Loi renseignement : regards croisés en France-Etats-Unis, Sécurité et stratégie*, 2015/3 (20), p. 16 à 23.

² Sur ce point, voir P. Rousseau et F. Rousseau, *Prévention d'actes de terrorisme et renseignement*, op. cit..

³ Cf. infra. Titre I de la Seconde Partie.

⁴ Cf. CNCTR, *5^{ème} rapport annuel (2020)*, p. 51 à 54.

⁵ Article L. 833-2-2° du code de la sécurité intérieure.

⁶ Cf. F. Delon, *la Commission nationale de contrôle des techniques de renseignement*, op. cit., p. 125 à 132.

pouvoir de recommandation dans le cadre de son contrôle *a posteriori* qui ne lui permet pas d'ordonner l'interruption d'une technique, la destruction de données et, plus généralement, de remédier à une irrégularité. L'inverse aurait davantage crédibiliser son rôle selon Xavier Latour¹, la question de l'affirmation d'un tel pouvoir de décision méritant d'être à nouveau posée depuis la réforme de 2021. Cependant, il nous semble que la logique générale du contrôle adoptée par la CNCTR, qui « *affirme ne pas s'inscrire dans une logique de contrôles-sanctions, mais bien d'interaction permanente avec les services en vue d'améliorer l'appréhension du cadre légal par l'ensemble des acteurs* »², incite à conserver un rôle de « magistrature morale » dans le contrôle *a posteriori* pour deux raisons : d'abord, parce que les recommandations de la CNCTR ont « un effet contraignant indirect » puisque le Premier ministre se doit d'y répondre et que la Commission peut saisir le Conseil d'Etat ou, en cas d'infraction, le procureur de la République³ ; ensuite, car les conditions du contrôle *a posteriori* s'inscrivent dans le cadre d'un régime répressif où l'intervention du juge administratif ou de l'autorité judiciaire nous semble la plus juste pour trancher un litige sur une technique de renseignement. En revanche, la CNCTR pourrait se voir doter d'un pouvoir contraignant s'agissant de l'obligation de destruction des données conservées au-delà de la durée légale.

Dans ces conditions, le seul réel pouvoir de la CNCTR réside dans le déclenchement de la saisine du juge pour reprendre les termes de Pascale Gonod⁴. Pour autant, il convient de ne pas minimiser le rôle de la CNCTR car elle est l'institution de contrôle externe placée au cœur du renseignement numérique et la mieux à même de prévenir tout risque de dérive, ce qui est loin d'être négligeable dans un champ d'intervention de l'Etat couvert par le secret et très sensible pour le respect de la démocratie et des libertés. Cela étant dit, l'efficacité de la Commission dépend de ses moyens de contrôle pour répondre aux inquiétudes relatives à l'augmentation des techniques et au volume important des

¹ Cf. X. Latour, *La loi relative au renseignement, un Etat de surveillance ?*, op. cit..

² En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 99.

³ A ce sujet, voir O. Desaulnay et R. Ollard, *Le renseignement français n'est plus hors-la-loi*, op. cit. ; M. -H. Gozzi, *Sed quis custodiet ipsos custodes ?*, op. cit..

⁴ Cf. P. Gonod, *Loi du 24 juillet 2015 relative au renseignement : quels contrôles ?*, Procédures n° 11, novembre 2015, étude 10.

données collectées¹. A ce sujet, on observera une adaptation des moyens de l'AAI qui confirme l'affirmation de son contrôle sur le renseignement numérique.

2. L'adaptation des moyens

Pour faire face au changement de dimension du renseignement numérique, l'expertise technique de la CNCTR s'est renforcée tout en ajustant ses méthodes et outils de contrôle.

L'acquisition d'une expertise technique

Dans le sillage des recommandations du Conseil d'Etat sur la nécessité de « *faire de la CNCIS une autorité de contrôle des services de renseignement dotée de moyens humains renforcés sur le plan quantitatif et qualitatif, avec des compétences de haut niveau en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données* »², il a été décidé d'intégrer une « personnalité qualifiée » en matière de communications électroniques parmi les membres de la nouvelle CNCTR³. En résonnance avec cette nouvelle composition de l'autorité administrative indépendante, on ajoutera que la CNCTR peut consulter l'ARCEP en tant que de besoin⁴ dans les limites du secret de la défense nationale pour éclairer ses observations.

Bien qu'une expertise technique soit affichée par les liens établis entre la CNCTR et l'ARCEP, la seule nomination d'une « personnalité qualifiée » n'a pas levé toutes les incertitudes « *quant à la capacité réelle de la CNCTR à appréhender des sujets d'une grande complexité technique* » selon Xavier Latour⁵. De son côté, le Professeur Bertrand Warusfel avait fait part de son vœu que la Commission puisse se doter d'une importante équipe d'experts techniques, notamment en mesure de contrôler régulièrement l'application de la technique algorithmique de l'article L.

¹ En ce sens, voir C. Lazerges et H. Henrion-Stoffel, *Politique criminelle, renseignement et droits de l'homme*, op. cit..

² Cf. Rapport public du Conseil d'État, étude annuelle 2014, *Le numérique et les droits fondamentaux*, p. 30.

³ Article L. 831-1-4° du code de la sécurité intérieure. Notons que la personnalité qualifiée est nommée sur proposition du président de l'ARCEP.

⁴ Article L. 833-11 du code de la sécurité intérieure.

⁵ Cf. X. Latour, *La loi relative au renseignement, un Etat de surveillance ?*, op. cit..

851-3¹. Ces remarques ont rapidement été suivies d'effets avec le recrutement d'agents reconnus pour leurs connaissances juridiques ou techniques dès 2015-2016². Selon l'ancien président de la CNCTR³ et la DPR⁴, une vingtaine de juristes et ingénieurs assistent quotidiennement la Commission au sein « d'un système de permanences » qui, soulignons-le, fait preuve de réactivité pour rendre des avis dans les délais fixés par la loi. On suggèrera qu'il serait souhaitable, au regard du renforcement continu des techniques de renseignement avec l'adoption de la seconde loi relative au renseignement du 30 juillet 2021, de maintenir la dynamique de montée en puissance de l'expertise technique de la CNCTR et de ne pas remettre en question ses moyens aussi bien humains que matériels.

Des méthodes et outils ajustés

Si la CNCTR contrôle l'ensemble des demandes d'autorisation, elle est dans « l'impossibilité évidente de contrôler l'intégralité des techniques mises en œuvre, des données collectées et des extractions et transcriptions réalisées », pour reprendre les mots de la DPR, ce qui l'a conduit à dimensionner matériellement son contrôle *a posteriori* en fonction de la nature des techniques concernées⁵.

Pour les techniques de surveillance nationale, la CNCTR exerce un contrôle par ciblage sur des dossiers identifiés au stade du contrôle *a priori*. De manière quotidienne, la CNCTR exerce un contrôle à distance via les outils informatiques du GIC sur les techniques que ce dernier centralise. Ce type de contrôle a été plus développé avec la pandémie de Covid-19 et devrait s'accroître avec la possibilité pour la Commission et les services de communiquer de nombreuses données par des moyens sécurisés même si les services se montrent encore réticents⁶. Parallèlement, la CNCTR réalise des contrôles sur pièces et sur place au sein des services et du GIC (au moins une à deux fois par mois pour la DGSE et la DGSI par

¹ Cf. B. Warusfel, *Les enjeux du nouveau cadre juridique du renseignement*, 3^{ème} colloque annuel de l'Association française de droit de la sécurité et de la défense (AFDSD), op. cit., p. 405-423.

² Cf. CNCTR, 1^{er} rapport annuel (2015-2016), p. 60.

³ Cf. F. Delon, *la Commission nationale de contrôle des techniques de renseignement*, op. cit., p. 125 à 132.

⁴ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 95 et 97.

⁵ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 98.

⁶ Cf. CNCTR, 5^{ème} rapport d'activité (2020), p. 60 et suivantes.

exemple), ce qui lui permet d'avoir notamment accès directement aux serveurs et applications informatiques utilisés pour les techniques et le traitement des données collectés¹. Ces modalités de contrôle n'ont pas cessé de se renforcer ces dernières années face à une augmentation du recours aux techniques les plus intrusives et à la nécessité de prévenir certaines anomalies récurrentes dans l'exploitation des renseignements collectés (durée légale de conservation dépassée, transcriptions abusives ou encore exploitation non conforme à l'autorisation)². En matière de recueil de données informatiques³, on soulignera que cette technique a fait l'objet d'une vigilance particulière de la CNCTR qui a « *décidé d'assortir ses avis favorables de restrictions destinées à encadrer les capacités de collecte de données afin de mieux assurer le respect du principe de proportionnalité et de protéger les libertés individuelles* », notamment au regard des multiples possibilités offertes par ce type de technique⁴. Afin de prévenir les risques de détournement abusif du dispositif, l'accès à l'information tend à être amélioré pour le contrôle *a posteriori* de la CNCTR avec la transmission des données statistiques sur la mise en œuvre de la technique et le volume de données recueillies ou encore l'organisation d'une capacité technique de centralisation dédiée au recueil de données informatiques⁵.

Pour les techniques de surveillance internationale, la Commission exerce un contrôle par échantillonnage. A ce titre, elle s'est rapidement dotée d'outils informatiques spécifiques de contrôle sur pièces et sur place des renseignements collectés et dispose d'un accès aux outils informatiques des agents exploitant les communications internationales interceptées⁶.

La CNCTR nous apparaît en bonne voie pour prévenir les risques d'abus de la numérisation du renseignement et appréhender sa complexité technique. Toutefois, certaines limites à l'exercice de son contrôle nous invitent à réfléchir au

¹ Cf. CNCTR, 5^{ème} rapport d'activité (2020), p. 54 à 56.

² Cf. CNCTR, 8^{ème} rapport d'activité (2023), p. 31 à 41 et 50 à 75.

³ Article L. 853-2 du code de la sécurité intérieure.

⁴ Cf. CNCTR, 8^{ème} rapport d'activité (2023), p. 76 à 78.

⁵ Cf. CNCTR, 8^{ème} rapport d'activité (2023), p. 78 à 81.

⁶ Cf. CNCTR, 1^{er} rapport annuel (2015-2016), p. 82 et 83.

dépassement de son cadre d'intervention et au passage d'un contrôle des techniques à celui des activités du renseignement.

B - Le dépassement du cadre d'intervention de la Commission nationale de contrôle des techniques de renseignement

Les limites à l'exercice du contrôle de la CNCTR interrogent sur la mutation d'un contrôle des techniques vers un contrôle des activités du renseignement.

1. Les limites à l'exercice du contrôle

Sur le fondement de l'article L. 833-2 du code de la sécurité intérieure qui interdit la Commission à connaître d'éléments communiqués par des services étrangers ou organismes internationaux ou de l'identité des sources des services français, la CNCTR se voit opposer la possibilité, d'une part, de contrôler les échanges de données avec des services étrangers et, d'autre part, d'accéder directement aux fichiers de renseignement.

Dans le premier cas, on rappellera que « *la CNCTR estime qu'une réflexion doit être menée sur l'encadrement légal des échanges de données entre les services de renseignement français et leurs partenaires étrangers* », notamment du fait que ces échanges peuvent contrevenir aux dispositions législatives françaises applicables aux renseignements collectés¹. Comme nous l'avons évoqué précédemment dans le cadre de l'encadrement du partage d'information², un contrôle de la CNCTR par dérogation à l'article L. 833-2 ne semble pas totalement à exclure et pourrait être aménagé par la loi et des accords bilatéraux ou multilatéraux dans le respect de la règle du « tiers service ».

Dans le second cas concernant les fichiers de renseignement, la CNCTR a considéré que la loi lui garantit un accès aux renseignements collectés « *quels que soient les supports, fichiers ou documents comportant des éléments obtenus grâce à la mise en œuvre d'une technique de renseignement* » afin de vérifier le respect des finalités pour lesquels ils ont été recueillis, ce qui impliquerait un accès aux fichiers de renseignement³. Cependant, elle s'est vu refuser par les services l'accès direct

¹ Cf. CNCTR, 3^{ème} rapport annuel (2018), p. 50 et suivantes.

² Cf. supra. §4 de la Section I du Chapitre II du Titre I.

³ Cf. CNCTR, 4^{ème} rapport annuel (2019), p. 75 et suivantes.

auxdits fichiers sur le fondement de l'article L. 833-2¹. Or, la DPR a également émis le souhait que la Commission puisse se voir ouvrir un droit d'accès ponctuel aux fichiers de renseignement dans le cas notamment d'une réclamation en ce sens par un particulier dans un souci du respect du droit au recours effectif devant le Conseil d'Etat². Pour le Professeur Bertrand Warusfel, la proximité tant opérationnelle que procédurale entre les techniques et les fichiers de renseignement et le fait que la CNIL dispose déjà d'un accès direct à ces derniers tendent en faveur de la proposition de la CNCTR ou, du moins, à une coopération entre les deux AAI « *pour mener des contrôles coordonnés* » en l'absence de réforme législative³. Néanmoins, il convient de préciser que cette coordination ne peut s'exercer que dans le cadre d'une réclamation individuelle, la CNIL n'ayant pas compétence pour exercer un contrôle *a posteriori* général sur les fichiers de renseignement⁴.

A travers ces limites, on retrouve la problématique du contrôle plus large des activités de renseignement qui avait été soulevée lors de l'élaboration de la loi relative au renseignement de 2015.

2. Un contrôle plus large des activités du renseignement

L'idée d'un contrôle des activités du renseignement et pas seulement des techniques de renseignement soumise à autorisation avait été déjà préconisée par Jean-Jacques Urvoas et Patrice Verchère dans leur rapport de 2013 sur l'évaluation du cadre juridique applicable aux services de renseignement avec la création d'une Commission de contrôle des activités du renseignement (CCAR)⁵. Le rapport de la DPR pour l'année 2014 avait, quant à lui, suggéré de transférer le contrôle des fichiers de renseignement à la futur CNCTR en modifiant la loi informatique et libertés⁶. Plus récemment, le Professeur Bertrand warusfel invite à « *passer*

¹ Cf. CNCTR, 5^{ème} rapport annuel (2020), p. 74.

² A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 100 et 101.

³ Cf. B. Warusfel, *Quelles réformes pour le droit du renseignement ?*, op.cit., p. 156.

⁴ Cf. infra. §3 de la Section II du Chapitre II du Titre II.

⁵ Cf. J. -J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, op. cit., p. 66 et suivantes.

⁶ Cf. J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 31 et 32.

progressivement d'un contrôle des moyens à celui des activités de renseignement » depuis que le renseignement constitue une politique publique¹. Certes, cette invitation vise particulièrement le contrôle parlementaire mais elle peut aussi concerner la CNCTR au regard de ses évolutions et des propositions d'amélioration.

A défaut d'envisager un contrôle global des activités du renseignement par la CNCTR, il nous semble pertinent de passer à un contrôle de la surveillance numérique. Il s'agirait de pouvoir contrôler l'ensemble des moyens numériques mobilisés par les services. Ainsi, la CNCTR pourrait être compétente pour contrôler les techniques non soumises à autorisation comme nous l'avons proposé au sujet des cyber-patrouilles et des actions de piratage informatique à l'étranger.

En outre, il pourrait être pertinent de réfléchir sur le développement d'un contrôle de la CNCTR plus abouti du principe de centralisation qui est une exigence légale relevant de la responsabilité du Premier ministre, d'autant plus que ce principe conditionne l'efficacité du contrôle de la Commission et qu'il tend à se préciser dans son application². Il nous semble que la CNCTR devrait pouvoir être en mesure de contester le refus d'application du principe de centralisation par le Premier ministre et l'administration.

Enfin, un contrôle de la surveillance numérique impliquerait de concentrer le contrôle des techniques et des fichiers de renseignement auprès de la CNCTR, notamment depuis l'attribution du contentieux de ces moyens de surveillance à la formation spécialisée du Conseil d'Etat et au regard de la faible valeur ajoutée du contrôle de la CNIL en matière de renseignement.

¹ Cf. B. Warusfel, *Quelles réformes pour le droit du renseignement ?*, op. cit., p. 161.

² Cf. supra. §3 de la Section I du Chapitre I du Titre II.

§3. Le contrôle limité de la Commission nationale de l'informatique et des libertés

Seconde autorité administrative indépendante spécialisée dans le contrôle des moyens numériques utilisés par les services de renseignement, la Commission nationale de l'informatique et des libertés (CNIL) a pour mission de vérifier que les fichiers des services respectent les principes de la protection des données personnelles de la loi « informatique et libertés ». Dans le même schéma que la CNCTR, la CNIL opère, en principe, un contrôle *a priori* sur les projets d'arrêtés ou de décrets créant des traitements de données en matière de sécurité et de défense ainsi qu'un contrôle *a posteriori* de leur mise en œuvre (sur pièces et sur place) tout en s'assurant du respect des droits des personnes concernés¹.

Le droit positif ne fait aucun doute sur la place incontournable qu'occupe la CNIL dans le contrôle des fichiers de renseignement puisqu'elle est la seule autorité indépendante compétente à pouvoir vérifier que les données d'une personne ne soient pas irrégulièrement traitées dans ces fichiers sans compromettre le secret de la défense nationale². Et depuis la loi relative au renseignement de 2015, la saisine de la CNIL constitue l'étape préalable à une requête devant la formation spécialisée du Conseil d'Etat dans le cadre du contentieux du droit d'accès indirect en matière de renseignement³. Cependant, il a pu être soutenu qu'ici l'intervention de la CNIL apparaît « *comme un filtre inutile* » en raison du fait que la saisine de l'autorité administrative indépendante « *ne fait que retarder la procédure du droit d'accès indirect* » en n'ayant que pour effet de permettre de contester devant le juge administratif la décision de refus de l'administration du droit d'accès⁴. Aussi, on ajoutera que seule la formation spécialisée du Conseil d'Etat dispose des pouvoirs nécessaires à un contrôle effectif des fichiers de renseignement et pour faire respecter les droits des

¹ Voir à ce sujet J. -M. Cotteret et E. Denécé, *Le renseignement au service de la démocratie*, op. cit., p. 172 à 189.

² Sur ce point, voir J. Mafart, *CNIL*, Dictionnaire du renseignement, op. cit., p. 158 à 160.

³ Article L. 841-2 du code de la sécurité intérieure.

⁴ En ce sens, voir J. Schmitz, *Le juge administratif et le contentieux du droit d'accès indirect aux fichiers de renseignement*, op. cit..

personnes sur la maîtrise de leurs données dans le cadre du contentieux du droit d'accès indirect¹.

Bien plus problématique, il convient de rappeler que les fichiers de renseignement bénéficient d'un régime dérogatoire avec notamment une exemption de contrôle *a posteriori* pour la plupart d'entre eux². Il s'ensuit qu'un contrôle uniquement opéré par « carottage », c'est-à-dire seulement porté sur les données d'une personne à l'occasion de l'exercice de son droit d'accès indirect, remet en question le rôle de la CNIL dans le contrôle du renseignement. En effet, cette dernière autorité n'a pas manqué de regretter l'absence d'un contrôle effectif *a posteriori* sur les fichiers de renseignement³ et de relever que : « *il en résulte une situation paradoxale : les fichiers constitués à partir des données ainsi collectées sont pleinement soumis aux principes de la loi Informatique et Libertés (principe de finalité, proportionnalité des données collectées, exigence d'exactitude et de mise à jour, etc.), mais aucun contrôleur externe n'est désigné pour en assurer, de manière générale, le respect* »⁴. On peut comprendre que la CNIL n'ait pas un accès direct et permanent aux fichiers de renseignement pour des raisons relatives au secret des sources des services et aux échanges internationaux de données de renseignement protégés par la règle du « tiers service »⁵. Cependant, cette limitation du contrôle, qui s'applique également à la CNCTR pour les mêmes raisons, est difficilement acceptable au regard du droit de la protection des données personnelles garanti tant par la loi « Informatique et libertés » que la loi relative au renseignement⁶ mais aussi à la lumière des réflexions sur le droit du renseignement applicable aux exploitations de données⁷.

Dans ce contexte juridique en évolution, il nous semble pertinent de revoir les pouvoirs de la CNIL dans le dispositif de contrôle du renseignement numérique. L'autorité administrative indépendante revendique elle-même la possibilité de

¹ Cf. infra. §4 de la Section II du Chapitre II du Titre II.

² Cf. supra. §1 de la Section I du Chapitre II du Titre I.

³ Cf. CNIL, 36^{ème} rapport d'activité (2015), p. 6.

⁴ Cf. CNIL, 38^{ème} rapport d'activité (2017), p. 78.

⁵ Voir en ce sens J. Mafart, *CNIL*, Dictionnaire du renseignement, op. cit., p. 158 à 160.

⁶ Article L. 801-1 du code de la sécurité intérieure.

⁷ Cf. supra. Chapitre II du Titre I.

réaliser un véritable contrôle *a posteriori* des fichiers de renseignement et pourrait, à ce titre, bénéficier d'un cadre juridique similaire à la CNCTR lui permettant aussi de saisir le Conseil d'Etat comme suggéré par Floran Vadillo¹. Pour notre part, il serait plus juste de transférer le contrôle des fichiers de renseignement à la CNCTR qui serait alors en mesure d'assurer la protection des données personnelles, de manière continue, tout au long du cycle du renseignement, d'autant plus si le droit du renseignement est amené à régir l'ensemble des traitements de données relatifs au renseignement (création de nouveaux fichiers ou modification de ceux existant ou encore interconnexions et partages des données). On ajoutera que ce transfert de compétence aurait le mérite de simplifier les réclamations individuelles puisque la CNCTR constituerait un guichet unique. Enfin, cette harmonisation du contrôle du renseignement numérique pourrait également s'accompagner d'une simplification du contentieux devant la formation « trop spécialisée » du Conseil d'Etat.

§4. Le contrôle juridictionnel « trop spécialisé » du Conseil d'Etat

Indéniablement, l'immixtion du juge dans les affaires secrètes de l'Etat ayant pour objet la surveillance des individus constitue l'avancée juridique majeure de la loi du 24 juillet 2015 relative au renseignement². La création d'une formation spécialisée au sein du Conseil d'Etat dont les membres sont habilités à qualifier au secret de la défense nationale permet désormais aux justiciables et à la CNCTR, dans le cadre d'une procédure juridictionnelle dérogatoire précisément définie par le législateur³, de mettre en cause les services de renseignement, ce contrôle juridictionnel constituant alors une « pression inédite » pour ces derniers selon la DPR⁴. Cependant, le législateur a strictement délimité la compétence du juge administratif à deux types de contentieux : les techniques et les fichiers de

¹ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit..

² En ce sens, voir B. Warusfel, *Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement*, *Le droit du renseignement*, op. cit., p. 80 à 82.

³ Cf E. Prada-Bordenave, *Le contrôle juridictionnel : un contrôle précisément défini par le législateur et confié à une formation spécialisée du Conseil d'Etat*, *Le droit du renseignement*, op. cit., p. 133 à 138.

⁴ Cf. J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 35.

renseignement. Bien que ces contentieux aient directement pour objet le contrôle des moyens numériques des services que nous pouvons que saluer dans le cadre de notre sujet d'étude, nos réflexions nous conduisent à envisager de faire sortir la formation spécialisée du Conseil d'Etat de la logique de cloisonnement qui s'applique aux contentieux du renseignement.

A - Une formation juridictionnelle spécialisée sur les techniques et les fichiers de renseignement

Dans le cadre de recours de plein contentieux, la formation spécialisée du Conseil d'Etat est amenée à se prononcer, en premier et dernier ressort, sur des litiges portant sur les techniques de renseignement¹ ou sur le droit d'accès indirect aux fichiers de souveraineté relevant de sa compétence².

1. Le contentieux des techniques de renseignement

L'article L. 841-1 du code de la sécurité intérieure ouvre un recours juridictionnel : à toute personne ayant procédé à une réclamation devant la CNCTR pour « *vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard* » ; à la CNCTR lorsque notamment ses recommandations ne sont pas suivies d'effets³ ; ou, à titre préjudiciel, aux juridictions administratives et judiciaires. On relèvera que l'éviction des associations a pu interroger à plusieurs reprises le Professeur Xavier Latour⁴. Il est vrai qu'il existe un certain nombre d'associations qui œuvrent activement pour la défense des droits et libertés face à la surveillance numérique telles que La Quadrature du Net qui s'est notamment distinguée pour avoir remis en cause le droit français du renseignement devant le juge de l'Union européenne. Pour autant, il reste difficile de déterminer un intérêt à agir pour les associations en vertu du principe selon lequel « nul ne plaide par procureur » dans la mesure où la procédure contentieuse concerne des techniques de renseignement mises en œuvre à l'encontre d'individus en particulier.

¹ Article L. 841-1 du code de la sécurité intérieure.

² Article L. 841-2 du code de la sécurité intérieure.

³ Article L. 833-8 du code de la sécurité intérieure.

⁴ Cf. X. Latour, *La loi relative au renseignement : un État de surveillance ?*, op. cit. ; X. Latour, *Premiers enseignements sur le contrôle juridictionnel des activités de renseignement*, La Semaine Juridique Edition Générale n° 46, 14 Novembre 2016, 1199.

S'agissant d'ailleurs des techniques litigieuses, il s'agit principalement de celles soumises à autorisation sur le territoire national. Néanmoins, les mesures de surveillance des communications internationales n'échappent pas totalement au contrôle du juge administratif. Initialement ouvert à la seule CNCTR, un recours juridictionnel direct a logiquement été accordé aux particuliers par la LPM 2019-2025 du 13 juillet 2018¹ pour les autorisations d'exploitation des communications rattachables à la France interceptées dans le cadre de la surveillance internationale². Plus radicale, la CNCTR s'est montrée favorable à un droit d'accès direct au juge pour l'ensemble des mesures de surveillance internationale et donc pour une remise en cause de la distinction entre les procédures contentieuses fondée sur un critère géographique³. De son côté, la DPR n'a pas estimé nécessaire de procéder à une telle modification au regard de la position du Conseil constitutionnel⁴ qui avait validé le dispositif de recours indirect via la CNCTR mis en place par la loi relative aux mesures de surveillance des communications électroniques internationales⁵. D'un point de vue juridique, on regrettera cette approche alors même que l'ancien président de la formation spécialisée du Conseil d'Etat, Edmond Honorat, avait confirmé que la proposition de la CNCTR permettrait de répondre aux interrogations sur l'effectivité des recours tout en précisant qu'une telle évolution pourrait peut-être nécessiter de renforcer les moyens de la formation spécialisée⁶.

Pour aller plus loin, la question peut être soulevée du contrôle juridictionnel de l'exception hertzienne dans la continuité du contrôle exercé par la CNCTR en vertu de l'article L. 855-1 C du code de la sécurité intérieure. Si le texte ne prévoit pas explicitement un recours devant la formation spécialisée du Conseil d'Etat, la combinaison des articles L. 801-1, L. 841-1, L. 855-1 C et L. 833-8 du code de la sécurité intérieure pourrait s'interpréter largement comme ouvrant un droit

¹ Article L. 854-9 du code de la sécurité intérieure.

² Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 102 et 103.

³ Cf. CNCTR, *3^{ème} rapport annuel (2018)*, p. 43.

⁴ Décision n° 2015-722 DC du 26 novembre 2015, considérant 18.

⁵ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 102 et 103.

⁶ Voir en ce sens G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 96 et 97.

à la CNCTR de contester devant le juge administratif des mesures de surveillance hertzienne prises sur le fondement de l'article L. 855-1 A du code de la sécurité intérieure qui entreraient dans le champ d'application des techniques soumises à autorisation dans le cas où le Premier ministre refuserait de suivre les recommandations de la Commission au sujet de cette irrégularité. En conséquence, une modification de l'article L. 855-1 C pour y introduire un recours contentieux n'est pas impensable. Par ailleurs, une interprétation extensive de l'article L. 833-8 du code de la sécurité intérieure nous conduit à penser, dans le silence de la loi, que la CNCTR pourrait également saisir le Conseil d'Etat en cas de litige avec le Premier ministre portant sur la suspension ou l'interruption d'un programme de recherche en intelligence artificielle¹. Enfin, dans l'hypothèse d'un contrôle global des moyens de renseignement par la CNCTR mais aussi des règles d'application du principe de centralisation, l'article L. 833-8 en lien avec des modifications législatives ou réglementaires spécifiques pourrait toujours servir de fondement à la possibilité d'un recours juridictionnel. Autrement dit, chaque fois que la CNCTR est compétente pour relever un manquement aux exigences légales ou réglementaires, la formation spécialisée du Conseil d'Etat devrait pouvoir être saisie lorsque l'administration refuse de suivre les recommandations de la Commission.

A l'issue d'une procédure contentieuse adaptée au secret de la défense nationale et dérogatoire aux principes des droits de la défense et du droit au procès équitable (instruction non contradictoire couverte par le secret de la défense nationale, audience séparée, décision limitée à son dispositif par exemple)², la formation spécialisée du Conseil d'Etat peut relever d'office tout moyen³ pour annuler l'autorisation d'une techniques de renseignement et ordonner la destruction des renseignements irrégulièrement collectés⁴. Statistiquement, ce contentieux demeure faible et n'a pour le moment abouti à aucune condamnation. Selon la DPR, « *il semble que le dispositif de recours administratif préalable devant la CNCTR permette d'assurer un premier filtre et*

¹ Article L. 822-2 du code de la sécurité intérieure.

² Articles L. 773-1 à L. 773-8 du code de la justice administrative.

³ Article L. 773-5 du code de justice administrative.

⁴ Article L. 773-7 du code de justice administrative.

d'éviter un nombre de recours trop important devant le juge »¹. On notera également que les recommandations de la CNCTR ont toujours été suivies d'effets. Dans le domaine des techniques de renseignement, il incombe encore au Conseil d'Etat « *de démontrer sa capacité à s'opposer à l'Etat en le condamnant* » pour reprendre les termes employés par le Professeur Xavier Latour en 2016². En revanche, le contentieux du droit d'accès indirect devant la formation spécialisée s'est révélé plus important et réellement effectif.

2. Le contentieux du droit d'accès indirect

Spécifique à la protection des données personnelles, ce contentieux est ouvert à toute personne justifiant d'une saisine préalable de la CNIL afin de vérifier la conformité à la loi « Informatique et libertés » du traitement de ses données dans les fichiers de renseignement visé par la réclamation³. Il convient de préciser que le contrôle de la formation spécialisée est strictement limité aux « *traitements ou parties de traitements intéressant la sûreté de l'Etat dont la liste est fixée par décret en Conseil d'Etat* »⁴. En conséquence, les demandeurs peuvent être confrontés à des difficultés pour saisir le juge compétent en ce qui concerne les fichiers dits « partagés » qui relèvent à la fois de la compétence du juge administratif de droit commun et de la formation spécialisée en fonction de la nature des données. Dénonçant cette situation, le rapport « Larrivé » de 2020 n'a pas manqué de proposer une simplification du droit même si « *le Conseil d'Etat et le tribunal administratif ont mis au point des procédures d'information réciproque afin de permettre, si nécessaire, un ré-aiguillage des requêtes* »⁵. Le rapport estime qu'il conviendrait d'appliquer le droit d'accès indirect à tous les fichiers systématiquement restreints en pratique par l'administration (tels que le PASP et le GIPASP) et de préciser le cadre contentieux dans les textes réglementaires applicables aux fichiers concernés, ce à quoi nous ne voyons aucun inconvénient.

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 104.

² Cf. X. Latour, *Premiers enseignements sur le contrôle juridictionnel des activités de renseignement*, op. cit..

³ A ce sujet, voir J. Schmitz, *Le juge administratif et le contentieux du droit d'accès indirect aux fichiers de renseignement*, op. cit..

⁴ Article L. 841-2 du code de la sécurité intérieure.

⁵ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 124 et 125.

Sur l'aspect procédural, il a pu être relevé que si le principe du contradictoire est adapté aux seules exigences du secret de la défense nationale¹, il peut sembler injuste que l'article R. 773-20 du code de justice administrative exclut des débats les informations qui simplement « *soit divulguent des éléments contenus dans le traitement de données, soit révèlent que le requérant figure ou ne figure pas dans le traitement* »². Pour notre part, cette extension de la dérogation au principe du contradictoire nous apparaît s'inscrire raisonnablement dans le prolongement de la protection du secret de la défense nationale même si elle ne facilite pas l'exercice du droit d'accès indirect du requérant qui ne peut être en mesure de formuler une demande concrète et précise sur une rectification, une mise à jour ou l'effacement de ses données comme le prévoit normalement le droit de la protection des données personnelles.

En ce qui concerne l'étendu du contrôle de la formation spécialisée du Conseil d'Etat, l'article L. 773-8 du code de justice administrative dispose qu'elle s'assure que les données du requérant ne sont pas « *inexactes, incomplètes, équivoques ou périmées* » ou que « *la collecte, l'utilisation, la communication ou la conservation* » des données n'est pas interdite. En outre, il ressort de l'analyse des décisions de la formation spécialisée que le juge administratif contrôle l'acte réglementaire portant création du fichier litigieux et procède à « un entier contrôle » sur les données personnelles du requérant, c'est-à-dire sur leur existence dans le fichier, leur pertinence, leur adéquation et leur proportionnalité comme notamment exigé par la jurisprudence de la CEDH³. En revanche, la formation spécialisée ne semble pas opérer un contrôle du refus de communication des données et ne dispose pas de la faculté d'ordonner l'accès à ces dernières, ce qui peut conduire à penser que le « droit d'accès indirect » constitue, ici, un abus de langage⁴. En effet, le Conseil d'Etat ne peut qu'ordonner

¹ Article L. 773-3 du code de justice administrative.

² En ce sens, voir J. Schmitz, *Le juge administratif et le contentieux du droit d'accès indirect aux fichiers de renseignement*, op. cit..

³ En ce sens, voir X. Latour, *La première injonction d'effacement de données dans un fichier intéressant la sûreté de l'Etat : une victoire à la Pyrrhus ?*, op. cit..

⁴ Voir en ce sens J. Schmitz, *Le juge administratif et le contentieux du droit d'accès indirect aux fichiers de renseignement*, op. cit..

la rectification, la mise à jour ou l'effacement des données¹, son contrôle s'apparentant alors à un contrôle *a posteriori* ciblé des fichiers de renseignement plus qu'à un contrôle du droit d'accès censé matérialiser la maîtrise des personnes sur leurs données.

Comme l'affirmait Xavier Latour, la frustration du requérant peut être consolée par la possibilité de sanctionner les dérives du fichage secret², d'autant plus que le Conseil d'Etat n'a pas manqué de condamner à plusieurs reprises l'administration en ordonnant l'effacement de données dans les fichiers de la DRSD³, de la DRM⁴ et de la DGSI⁵. Il n'en demeure pas moins que la solution ainsi retenue par le droit du renseignement, comme celle de cloisonner les deux contentieux du renseignement, tend à un déséquilibre en faveur de la protection du secret de la défense nationale qui s'éloigne de l'esprit de l'article L. 801-1 du code de la sécurité intérieure sur la conciliation entre les activités de renseignement et le respect de la vie privée et la protection des données personnelles. Un rééquilibrage pourrait être envisagé dans le rapprochement des deux contentieux, la protection des données personnelles pouvant servir de fondement à des améliorations du contrôle juridictionnel.

B - Sortir la formation spécialisée de la logique du cloisonnement des contentieux du renseignement

Juge du droit de la protection des données personnelles, la formation spécialisée du Conseil d'Etat doit veiller au respect de ce droit que ce soit dans le contentieux des techniques de renseignement selon l'article L. 801-1 du code de la sécurité intérieure ou dans celui des fichiers de souveraineté en vertu de l'article L. 841-2 du même code. Cependant, en cloisonnant ces deux contentieux, le législateur a manqué de cohérence non seulement avec la loi « informatique et libertés » mais aussi avec les dispositions du code de la sécurité intérieure. Il

¹ Article 773-8 du code de justice administrative.

² Cf. X. Latour, *La première injonction d'effacement de données dans un fichier intéressant la sûreté de l'Etat : une victoire à la Pyrrhus ?*, op. cit..

³ Conseil d'Etat, 5 mai 2017, n° 396669.

⁴ Conseil d'Etat, 8 novembre 2017, n° 3964549.

⁵ Conseil d'Etat, 31 juillet 2019, n° 417109.

conviendrait donc d'harmoniser le contentieux du renseignement numérique dans le prolongement de notre analyse sur les contrôles exercés par la CNCTR et la CNIL.

1. L'incohérence du cloisonnement

Le contrôle de la protection des données personnelles s'intéresse aux traitements numériques de ces dernières, ce qui comprend notamment leur collecte. Le contrôle de la collecte des données est l'objet même du contentieux des techniques de renseignement et se retrouve également dans le contentieux des fichiers de renseignement, l'article L. 773-8 du code de justice administrative mentionnant expressément la collecte interdite des données personnelles dans le traitement des requêtes par la formation spécialisée du Conseil d'Etat.

Or, il se pourrait que des données conservées dans des fichiers de renseignement puissent être collectées dans le cadre de techniques de renseignement illégalement mises en œuvre, ce qui constituerait une collecte interdite au sens de l'article L. 773-8. Cependant, il semblerait, qu'en l'état actuel du contentieux des techniques de renseignement, le Conseil d'Etat ne pourrait pas ordonner l'effacement des données conservées dans un fichier de renseignement alors qu'elles auraient été collectées irrégulièrement par une technique jugée illégale. Inversement, le juge administratif ne semble pas pouvoir non plus contrôler la légalité d'une technique de renseignement ayant servi à collecter les données litigieuses dans le cadre du contentieux des fichiers, aucun dispositif n'est prévu en ce sens. Il en résulte un risque d'incohérence entre les décisions de la formation spécialisée du Conseil d'Etat qui pourrait statuer de manière différente sur la légalité de mêmes renseignements collectés qui seraient soumis aux deux contentieux. Dans ces conditions, la mise en place d'un dispositif d'interaction entre les deux contentieux du renseignement numérique nous apparaît bienvenue.

2. L'harmonisation du contentieux du renseignement numérique

Afin d'assurer un véritable contrôle juridictionnel de la protection des données en matière de renseignement, il peut être proposé, dans le prolongement des réflexions sur le renforcement du contrôle de la CNCTR, de permettre à la formation spécialisée, saisie dans le cadre du contentieux des techniques, d'accéder aux fichiers conservant les renseignements collectés litigieux et d'ordonner leur effacement en cas d'irrégularité. Dans l'autre sens, saisi d'une

requête sur les fichiers, le Conseil d'Etat pourrait être amené à contrôler l'existence d'une technique de renseignement ayant servi à la collecte des données litigieuses et sa légalité en vertu de l'article L. 773-8 modifié pour envisager cette possibilité¹ et de l'article L. 773-5 qui permet à la formation de jugement de relever d'office tout moyen.

Une autre solution consisterait à s'aligner sur notre proposition de faire de la CNCTR l'unique contrôleur des techniques et fichiers de renseignement ainsi que le guichet unique des réclamations en matière de renseignement numérique². La CNCTR assurerait notamment le contrôle *a posteriori* des fichiers de renseignement et aurait la faculté de saisir le Conseil d'Etat soit sur les techniques ou les fichiers, soit sur les deux lorsqu'ils concernent les mêmes renseignements collectés. S'agissant des réclamations et des recours des particuliers, la CNCTR et le Conseil d'Etat pourraient être saisi plus largement sur l'ensemble des moyens numériques (techniques et fichiers) susceptibles d'avoir été utilisés pour surveiller le requérant.

Ces réflexions sur la compétence du Conseil d'Etat en matière de renseignement numérique nous incite à confirmer la nécessité de consacrer un véritable droit de visite sur place dans les services de renseignement³ tout comme la possibilité pour la formation spécialisée de recourir à plus d'expertise technique⁴.

Enfin, si notre analyse sur l'harmonisation du contentieux du renseignement numérique tend à s'éloigner du contentieux spécifique du droit d'accès indirect, elle nous apparaît plus adaptée aux enjeux juridiques de la surveillance numérique secrète. Cependant, il n'est pas impossible d'imaginer une évolution de la procédure contentieuse allant dans le sens du droit d'accès aux

¹ Selon l'article L. 773-8 du code de justice administrative, la formation spécialisée du Conseil d'Etat doit se fonder sur les éléments contenus dans le traitement litigieux. Cette disposition pourrait être modifiée afin de prévoir que le Conseil d'Etat puisse également se fonder sur une autorisation d'une technique de renseignement et sa mise en œuvre lorsque les données ont été collectées de cette manière.

² Cf. supra. §2 de la Section II du Chapitre II du Titre II.

³ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 177 et 178.

⁴ Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 106 et 107.

données en introduisant, comme proposé par le Professeur Bertrand Warusfel¹ mais aussi la CNCTR², des « avocats spéciaux habilités » à accéder aux audiences fermées de la formation spécialisée du Conseil d'Etat pour permettre une défense plus adaptée. En effet, la procédure actuelle ne permet pas au requérant de discuter de l'exactitude de ces données figurant dans un fichier, ce qui est contraire à la logique du contentieux du droit d'accès³. Cette situation demeure insatisfaisante bien que le juge administratif soit en mesure de relever d'office tout moyen et que cette faculté ait été relevée par le Conseil constitutionnel comme une garantie procédurale importante dans les aménagements des principes du contradictoire et du droit au procès équitable⁴. Le justiciable n'a pas d'autre choix que de faire confiance au juge alors même que ce dernier pourra difficilement se substituer au requérant pour apprécier la nécessité de rectifier ou de mettre à jour les données litigieuses qui sont des demandes tout à fait particulières⁵.

¹ Cf. B. Warusfel, *Quelles réformes pour le droit du renseignement ?*, op. cit., p. 162 et 163.

² Cf. CNCTR, *8^{ème} rapport d'activité (2023)*, p. 85 et 86.

³ En ce sens, voir G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 97.

⁴ Décision n° 2015-713 DC du 23 juillet 2015, Loi relative au renseignement (considérants 80 à 92).

⁵ Certains recours relatifs au droit d'accès indirect peuvent s'inscrire dans le cadre d'un contentieux avec l'administration portant sur la carrière des personnels d'emplois publics ou privés nécessitant une habilitation. Dans ce cas, le requérant ne cherche pas systématiquement l'effacement de ses données mais plutôt à vérifier l'exactitude des informations le concernant et leur rectification ou leur mise à jour.

CONCLUSION DU TITRE

La légalisation du renseignement initiée en France depuis les années 1990 et véritablement assumée en 2015 s'est principalement attachée à construire un régime juridique applicable aux techniques de renseignement en adoptant des procédures et mécanismes de contrôle ainsi que des régimes de responsabilité spécifiques aux enjeux numériques.

Dans ces considérations, les garanties ainsi consacrées par le droit du renseignement pour concilier le respect du droit à la vie privée et les activités de renseignement nous amènent à questionner l'organisation et le fonctionnement même de la communauté française du renseignement et continue de nous interroger sur la distinction entre l'encadrement des techniques de renseignement et celui des fichiers.

Comme nous avons pu l'observer, la mise en œuvre des techniques de renseignement est étroitement liée aux missions et compétences respectives des services de renseignement. Cependant, l'engagement de la communauté française du renseignement dans son adaptation à la cyberdimension pour disposer de capacités de renseignement d'origine cyber (ROC) tout en faisant du renseignement d'intérêt cyber (RIC) une nouvelle « finalité » (même si elle n'a pas été consacrée au titre des finalités de l'article L. 811-3 du code de la sécurité intérieure), le rôle incontournable technico-juridique du GIC ainsi que l'affirmation du principe de centralisation ne sont pas sans soulever la question du transfert de l'intégralité du recours aux techniques de renseignement au sein même du GIC voire de la création d'une agence de renseignement numérique autonome sur le modèle de la NSA ou du GCHQ.

Cette évolution pourrait présenter l'avantage de simplifier le droit du renseignement en permettant, par exemple, d'affirmer un véritable droit de la centralisation du renseignement numérique en adoptant plus facilement des règles d'application de ce principe. En outre, elle peut être une manière de renforcer le contrôle du renseignement numérique en plaçant un interlocuteur unique en face des instances de contrôle. Néanmoins, il convient de relever que le transfert de l'ensemble des techniques au sein d'une agence pourrait remettre en cause, au regard de la jurisprudence européenne notamment, la distinction entre

renseignement intérieur et extérieur en matière numérique mais aussi le principe d'individualisation consacré en droit français dans le cadre d'une tendance à légaliser des mécanismes de surveillance massive. Par ailleurs, si ce transfert se réalise au profit du GIC, il doit être souligné qu'il enterre possiblement la neutralité du service du Premier ministre et donc une garantie pourtant jugée importante contre les risques de dérives. Aussi, on peut craindre que cette solution entraîne la disparition d'une autre garantie tout aussi importante, la séparation entre les services de renseignement et les opérateurs du numérique.

En ce qui concerne la distinction entre les techniques et les fichiers de renseignement que nous avons déjà eu l'occasion de questionner dans le cadre du renforcement des moyens numériques en droit du renseignement, la proximité, notamment relevée par le Professeur Bertrand Warusfel¹, tant opérationnelle que procédurale et contentieuse entre les deux types d'outil numérique (régime d'autorisation, garanties portant par exemple sur les finalités, la conservation des données ou encore sur l'accès aux données, contentieux devant la formation spécialisée du Conseil d'Etat) nous confirme la nécessité de réfléchir sérieusement à un rapprochement plus avancé entre la loi « Informatique et libertés » et le droit du renseignement. Pour notre part, il serait judicieux de prévoir une harmonisation au sein des dispositions relatives au renseignement du code de la sécurité intérieure sans oublier de prendre en considération les spécificités du droit de la protection des données personnelles afin de faire émerger un droit du renseignement porté sur le numérique avec un régime juridique et un contentieux aisément identifiable pour les justiciables comme pour les acteurs du monde du renseignement. On rejoint alors la position de Fabien Lafouasse, juriste spécialiste de l'espionnage en droit international, qui partage également l'idée d'une matière juridique dédiée au « droit du renseignement numérique »².

Toutefois, si on peut relever une tendance allant vers une autonomisation du droit du renseignement numérique par rapport au droit du renseignement et au droit du numérique, il reste que l'autonomie recherchée de ce droit doit être relativisée dans la régulation de la numérisation du renseignement. Comme nous

¹ Cf. B. Warusfel, *Quelles réformes pour le droit du renseignement ?*, op. cit..

² Cf. F. Lafouasse, *Fasc. 1210 : Droit du renseignement numérique*, JurisClasseur Communication, 1^{er} janvier 2022.

l'avons constaté à plusieurs reprises, le droit du renseignement numérique ne concerne qu'une partie, certes primordiale, de la numérisation en n'encadrant que les moyens numériques de surveillance. Mais surtout, la « vague réglementaire » qui déferle sur l'ensemble des activités numériques a pour conséquence d'affirmer l'application, parfois à marche forcée, du droit du numérique à la transformation digitale des services de renseignement.

SECONDE PARTIE

L'APPLICATION DU DROIT DU NUMERIQUE AU RENSEIGNEMENT

« Le cyberspace désigne l'univers des réseaux numériques comme lieu de rencontres et d'aventures, enjeu de conflits mondiaux, nouvelle frontière économique et culturelle »

L'intelligence collective, Pierre Lévy

Si le cyberspace peut être sobrement défini comme un « *espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'internet, et par les données qui y sont traitées* »¹, la définition retenue par Pierre Lévy nous plonge dans un parfait « nid d'espions » du XXIème siècle. Il est d'ailleurs entendu que le cyberspace est un concept géopolitique aux nombreux enjeux militaires et sécuritaires qui font nécessairement intervenir les services de renseignement².

En droit, l'absence d'une définition précise de ce concept n'empêche pas de l'appréhender juridiquement à travers les différents sujets qu'il sous-tend³ : la protection des données personnelles et du secret des correspondances électroniques, la lutte contre la cybercriminalité ou encore le droit applicable à la cybersécurité. On rappellera que ces sujets sont, à notre sens, au cœur du droit du

¹ Cf. Vocabulaire de la défense, J. O. du 19/09/2017.

² En ce sens, voir notamment F. Douzet, *La géopolitique pour comprendre le cyberspace*, Hérodote, vol. 152-153, no. 1-2, 2014, pp. 3-21.

³ A ce sujet, voir par exemple C. Cronella, *Autopsie juridique du concept de « cyberspace »*, in *Annuaire 2021 du Droit de la sécurité et de la défense*, Editions mare & martin, 2021, p. 217 à 225 ou encore B. Louis-Sidney, *La dimension juridique du cyberspace*, *Revue internationale et Stratégique*, 2012/3 (n° 87), p. 73 à 82.

numérique¹. Ce droit est donc amené à s'appliquer au renseignement en raison de la montée en puissance de ce dernier dans le cyberspace. En effet, on observe, d'une part, des intrications entre le droit du numérique et le droit du renseignement (**Titre I**) et, d'autre part, une conciliation qui s'opère entre la protection juridique du cyberspace et le renseignement (**Titre II**).

¹ Cf. supra. Introduction.

TITRE I

LES INTRICATIONS DU DROIT DU NUMERIQUE ET DU DROIT DU RENSEIGNEMENT

Certaines dispositions du droit du renseignement relatives au numérique ne sont pas nouvelles ou entièrement autonomes. Elles sont directement issues du droit du numérique ou en constituent une transposition. En effet, le droit européen relatif à la vie privée numérique se diffuse nécessairement dans le droit du renseignement autorisant la surveillance technique des individus en raison de sa valeur supralégislative (**Chapitre I**). En outre, les risques d'abus du cyberespionnage d'Etat appréhendés par le droit du renseignement sont également susceptibles de constituer des infractions relevant de la cybercriminalité. Cette double appréhension juridique affirme la place du droit pénal du numérique dans l'encadrement de la numérisation du renseignement (**Chapitre II**).

CHAPITRE I

LA DIFFUSION DU DROIT EUROPEEN RELATIF A LA VIE PRIVEE NUMERIQUE

Bien que la France se soit rapidement dotée d'une législation adaptée à la protection des données personnelles et au secret de correspondances électroniques avec la loi Informatique et libertés de 1978 et la loi relative secret des correspondances électroniques de 1991, il n'en demeure pas moins que la primauté du droit européen s'est imposée pour constituer le socle juridique du droit relatif à la vie privée numérique. En matière de surveillance et de renseignement, les prescriptions juridiques des instruments du Conseil de l'Europe (**Section I**) et les exigences du droit de l'Union européenne (**Section II**) se sont légitimement diffusées dans le droit du renseignement.

SECTION I : Les prescriptions des instruments juridiques du Conseil de l'Europe

Il convient tout d'abord de procéder à l'étude des stipulations conventionnelles des instruments juridiques du Conseil de l'Europe applicables à la surveillance numérique (§1) pour, ensuite, comprendre que leur interprétation ont permis de dégager des prescriptions fondamentales pour l'élaboration du droit du renseignement français (§2). Cependant, nos observations doivent tenir compte du fait que le cadre européen du renseignement numérique est en constante évolution (§3).

§1. Les textes applicables à la surveillance numérique

Saisie à maintes reprises depuis la fin des années 1970 sur les activités de surveillance numérique des Etats, la Cour européenne des droits de l'homme (CEDH) a eu l'occasion d'affirmer l'application de l'article 8 de la Convention européenne des droits de l'homme de 1950 (Conv. EDH) relatif à la vie privée en la matière. Si le texte de 1950 et la jurisprudence de la CEDH constituent les

fondements principaux du cadre juridique européen de la surveillance numérique, il convient également de mentionner une autre convention du Conseil de l'Europe (CdE) dont le contenu est invoqué pour limiter le développement des programmes de surveillance étatiques : la Convention 108 sur la protection des données personnelles.

A - L'article 8 de la Convention européenne des droits de l'homme

Tout en consacrant le droit au respect à la vie privée en y intégrant le secret des correspondances, l'article 8 de la Conv. EDH introduit un régime dérogatoire à l'exercice de ce droit en autorisant l'ingérence de l'autorité publique lorsqu'elle 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 »*.

Dans un arrêt fondateur *Klass et autres c. Allemagne* du 6 septembre 1978, la CEDH s'est ainsi appuyée sur ce régime dérogatoire pour juger qu'un régime légal de surveillance numérique secrète n'emporte pas systématiquement violation de la Conv. EDH, notamment au regard des menaces d'espionnage et de terrorisme auxquelles sont confrontées les sociétés démocratiques. Si la Cour de Strasbourg a pu reconnaître une marge nationale d'appréciation quant aux moyens numériques de surveillance utilisés, elle n'a pas manqué de rappeler que :

« les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée »¹.

¹ CEDH, 6 septembre 1978, *Klass et autres c. Allemagne*, §49.

Ainsi, il a été jugé que l'ingérence dans la vie privée par le renseignement numérique doit être conforme à trois exigences issues de l'article 8§2 de la convention¹ :

- elle doit être prévue par une loi suffisamment précise et prévisible sur les modalités d'exercice du pouvoir d'appréciation des autorités². En outre, la loi se doit d'énoncer avec clarté les modalités d'exercice d'un tel pouvoir³. En d'autres termes, les individus doivent être en mesure d'accéder à la loi, d'adapter leur comportement en fonction de celle-ci et d'en prévoir les conséquences pour eux ;
- l'ingérence doit être fondée sur les objectifs énoncés à l'article 8§2 : « *la sécurité nationale* », « *la sûreté publique* », « *le bien-être économique du pays* », « *la défense de l'ordre et la prévention des infractions pénales* », « *la protection de la santé ou de la morale* », ou « *la protection des droits et libertés d'autrui* » ;
- elle doit être légitime dans une société démocratique et respecter le principe de proportionnalité.

Reprenant directement les stipulations de l'article 8, cette jurisprudence constitue un « premier étage » de l'édifice jurisprudentiel de la CEDH en matière de renseignement numérique. En effet, un « deuxième étage » a été bâti par les juges de Strasbourg qui ont dégagé des « garanties minimales » de référence censées guider les législations nationales⁴. Ces « garanties minimales » ont été formulée par la Cour dans son arrêt de principe *Weber et Saravia c. Allemagne* du 29 juin 2006 après avoir notamment souligné le fait que les moyens techniques de surveillance ne cessent de se perfectionner (§92 à 95). Au nombre de six, les garanties que la loi doit prévoir sont : « *la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée de l'exécution*

¹ Voir à ce sujet G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 140 à 142.

² CEDH, 2 août 1984, *Malone c. Royaume-Uni*.

³ CEDH, 24 avril 1990, *Kruslin et Huvig c. France*.

⁴ Sur ce point, voir F. Lafouasse, *Le droit du renseignement : un droit conforme aux traités internationaux*, in *Le droit du renseignement*, op. cit., p. 187 à 199.

de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »¹.

Constamment invoquées par la CEDH dans les affaires portant sur des mesures de surveillance secrète, ces six « garanties minimales » ont été complétées par deux autres garanties prises en compte par la Cour depuis son arrêt *Roman Zakharov c. Russie* du 4 décembre 2015 : d'une part, les modalités de contrôle des mesures de surveillance et, d'autre part, l'existence de recours en droit interne et d'un mécanisme de notification. S'agissant plus particulièrement du contrôle, la CEDH considère que ce dernier doit pouvoir intervenir « *lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé* »².

Plus récemment, la Cour de Strasbourg a été amenée à se positionner sur la conformité de la surveillance numérique de masse et du partage international des données de renseignement à l'article 8 de la Conv. EDH dans deux arrêts rendus en Grande Chambre *Big Brother Watch et autres c. Royaume-Uni* et *Centrum För Rättvisa c. Suède* du 25 mai 2021. Fidèle à sa conception large de la marge nationale d'appréciation en matière de surveillance numérique, la CEDH a admis le recours à la surveillance numérique de masse pour les besoins de la sécurité nationale dans un contexte de nouvelles menaces de nature numérique qui ne peuvent être appréhendées que par des moyens techniques³. On précisera que, comme la justement remarqué le spécialiste du droit du numérique Eric A. Caprioli, la Cour admet davantage l'interception de masse des communications ou la collecte de masse des données plutôt qu'une surveillance de masse des individus sans limite dans le temps⁴. Pour parvenir à cette conclusion, les juges de Strasbourg ont eu à dégager des nouvelles « garanties de bout en bout » plus adaptées :

¹ CEDH, 29 juin 2006, *Weber et Saravia c. Allemagne*.

² CEDH, 4 décembre 2015, *Roman Zakharov c. Russie*, §233.

³ Voir sur ce point M. -C. de Montecler, *La CEDH admet le principe de la surveillance électronique de masse*, op. cit. ; A. Danis-Fatôme, *Surveillance de masse – Sécurité nationale et protection des données : quelle articulation ?*, Communication Commerce électronique n° 9, Septembre 2021, comm. 66.

⁴ Cf. E. A. Caprioli, *La CEDH invalide partiellement l'ancien système britannique de surveillance électronique*, Communication Commerce électronique n° 1, Janvier 2019, comm. 5.

« la Cour considère qu'afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, le processus doit être encadré par des « garanties de bout en bout », c'est-à-dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré ri. Ces facteurs sont, de l'avis de la Cour, des garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8 »¹.

En pratique, pour déterminer la conformité aux exigences de l'article 8, la Cour prend *« en compte un groupe plus large de critère que les six garanties Weber »* en jugeant qu'une législation nationale en matière d'interception de masse devrait définir :

- « 1. Les motifs pour lesquels l'interception en masse peut être autorisée ;*
- 2. Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;*
- 3. La procédure d'octroi d'une autorisation ;*
- 4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;*
- 5. Les précautions à prendre pour la communication de ces éléments à d'autres parties ;*
- 6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;*
- 7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;*

¹ CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, §350.

8. *Les procédures de contrôle indépendant ri du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement* »¹.

Alors que pour certains commentateurs la décision de la Cour a pu être considérée comme « *une solution mesurée qui reconnaît aux États membres du Conseil de l'Europe une large marge d'appréciation concernant la mise en place de systèmes d'interception de masse et qui indique à quelles conditions l'existence d'une menace grave pour la sécurité nationale est susceptible de justifier une ingérence dans les droits des requérants* »², pour d'autres, elle constitue en réalité un affaiblissement « *des garanties tirées de la jurisprudence classique relative à la surveillance* » et un accroissement de la marge d'appréciation des Etats ou encore que « *la Cour Européenne des droits de l'homme aura manqué une occasion d'affirmer l'effectivité du droit à la protection de la vie privée face aux pressions des Etats* »³. A notre sens, les juges de Strasbourg ont effectivement renforcé la marge nationale d'appréciation des Etats en admettant clairement les interceptions massives aux fins de sécurité nationale sans toutefois remettre entièrement en question le droit au respect de vie privée ou la protection des données personnelles. Il s'agit là d'une solution de la CEDH visant à concilier, selon un contexte particulier de sécurité nationale, un certain type de surveillance avec les droits garantis par la Convention. Cette logique de « contextualisation » présente depuis l'affaire *Klass et autres c. Allemagne* se retrouve dans le cas du partage international des données de renseignement. Sur ce dernier, la Cour a également entouré les « flux entrants et sortants » d'informations de garanties spécifiques⁴ :

- pour les « flux entrants », la Cour a considéré que « *la protection accordée par la Convention se trouverait vidée de sa substance si les États pouvaient contourner leurs obligations conventionnelles en adressant à des États non contractants des demandes d'interception de communications ou de remise*

¹ CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, §361.

² En ce sens, voir A. Danis-Fatôme, *Sécurité nationale et protection des données : quelle articulation ?*, op. cit..

³ En ce sens, voir F. Dubuisson, *La Cour européenne des droits de l'homme face à la surveillance de masse*, Revue trimestrielle des droits de l'homme, 2022/1 (N° 129), p. 123 à 141 ; O. Tambou, *La condamnation relative des mesures de surveillances massives étatiques : une occasion manquée par la Cour européenne des droits de l'homme*, Blogdroiteuropéen, 2021.

⁴ Cf. CNCTR, 6^{ème} rapport annuel (2021), p. 48 à 52.

de communications interceptées, ou même – bien que cette éventualité ne soit pas directement en cause dans la présente affaire – obtenir ces communications par un accès direct aux bases de données de ces derniers ». La Cour a donc estimé que : « *les demandes d'éléments interceptés adressées aux États non contractants doivent avoir une base en droit interne, être accessibles à la personne concernée et prévisibles quant à leurs effets. L'échange de renseignements doit être encadré par des normes claires et précises indiquant à tous de manière suffisante en quelles circonstances et sous quelles conditions les autorités sont habilitées à formuler de telles demandes et offrant des garanties effectives contre l'utilisation de ce pouvoir à des fins de contournement du droit interne et/ou des obligations conventionnelles des États* » ; « *dès la réception des éléments interceptés, l'État destinataire doit avoir mis en place des garanties suffisantes pour leur examen, leur utilisation, leur conservation, leur transmission à des tiers, leur effacement et leur destruction. Les garanties en question, qui ont d'abord été énoncées par la Cour dans sa jurisprudence relative à l'interception de communications par les États contractants, s'appliquent également à la réception, par un État contractant, d'éléments interceptés demandés à un service de renseignement étranger. Dès lors, comme le soutient le Gouvernement, que les États ne sont pas toujours en mesure de savoir si des éléments reçus de services de renseignement étrangers sont le produit d'une interception, la Cour considère que les mêmes règles doivent s'appliquer à l'ensemble des éléments reçus de services de renseignement étrangers qui pourraient être le produit d'une interception* » ; « *tout régime autorisant des services de renseignements à demander à des États non contractants de procéder à une interception ou de leur transmettre des éléments interceptés doit être soumis à une supervision indépendante et doit également prévoir la possibilité d'un contrôle indépendant* »¹ ;

- pour les « flux sortants », « *la Cour considère que la transmission, par un État contractant, d'informations obtenues au moyen d'une interception en masse à des États étrangers ou à des organisations internationales devrait être*

¹ CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, §497 à §499.

limitée aux éléments recueillis et conservés d'une manière conforme à la Convention, et qu'elle devrait être soumise à certaines garanties supplémentaires relatives au transfert lui-même. Premièrement, les circonstances dans lesquelles pareil transfert peut avoir lieu doivent être clairement énoncées dans le droit interne. Deuxièmement, l'État qui transfère les informations en question doit s'assurer que l'État destinataire a mis en place, pour la gestion des données, des garanties de nature à prévenir les abus et les ingérences disproportionnées. L'État destinataire doit, en particulier, garantir la conservation sécurisée des données et restreindre leur divulgation à d'autres parties. Cela ne signifie pas nécessairement qu'il doive garantir une protection comparable à celle de l'État qui transfère les informations, ni qu'une assurance doive être donnée avant chaque transfert. Troisièmement, des garanties renforcées sont nécessaires lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière – par exemple s'il s'agit de communications journalistiques confidentielles. Enfin, la Cour considère que le transfert d'informations à des partenaires de renseignement étrangers doit également être soumis à un contrôle indépendant »¹.

Tout au long de sa jurisprudence, la CEDH a été amenée à se prononcer sur la conformité à l'article 8 de la Convention de différents types de moyens numériques de surveillance qu'ils s'agissent d'interceptions de correspondances électroniques ou plus généralement de toutes les données relatives aux communications numériques, y compris les métadonnées, ou encore de piratage d'un système d'information². Ces affaires ont été l'occasion pour la Cour de Strasbourg non seulement de réaffirmer le droit au secret des correspondances textuellement garanti par l'article 8 mais aussi d'affirmer le rattachement à ce même article de la protection des données personnelles qui fait l'objet d'une Convention spécifique du CdE³, ce qui nous amène à nous intéresser plus particulièrement à l'application de cette protection à la surveillance numérique.

¹ CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, §362.

² CEDH, 7 juillet 2020, *Privacy International et autres c. Royaume-Uni*.

³ Cf. Conseil de l'Europe, *Partie 1. Les opérations de surveillance massive*, Surveillance de masse, 2016, p. 5 à 62.

B - La Convention 108 sur la protection des données personnelles

La protection des données personnelles a été rapidement appréhendée dans les instruments juridiques du Conseil de l'Europe (CdE), notamment avec l'adoption de la Convention STE n° 108 du 28 janvier 1981. Applicable à tout traitement privé ou public de données personnelles et régulièrement modernisée, cette convention a constitué l'un des premiers textes juridiques à poser les principes communs du droit de la protection des données en Europe et dans le monde : collecte licite et loyale des données à des fins légitimes, proportionnalité des traitements (données adéquates, pertinentes, non excessives et exactes), prise en compte des données « sensibles » et des droits des personnes, dérogations aux restrictions en matière de sécurité, encadrement des transferts internationaux des données ou encore obligation de création d'autorités nationales de contrôle¹.

Considérée comme la seule convention internationale juridiquement contraignante pour les Etats signataires dans le domaine de la protection des données, la Convention 108 est reconnue par les instances du CdE, notamment le Commissaire aux droits de l'homme², comme un instrument qui a pleinement vocation à s'appliquer au renseignement numérique³. Plus précisément, la Présidente du Comité de la « Convention 108 » du Conseil de l'Europe sur la protection des données, Alessandra Pierucci, et le Commissaire à la protection des données du Conseil de l'Europe, Jean-Philippe Walter, ont tenu à souligner que l'article 11 de la version amendée de la Convention par le Protocole STCE n° 223 prévoit que *« les droits prévus par la Convention ne peuvent être limités que lorsque cela est prescrit par la loi et que la restriction constitue une mesure nécessaire et proportionnée dans une société démocratique sur la base de motifs précis et limités, y compris la sécurité et la défense nationales »* et que la Convention stipule clairement que les activités de traitement à des fins de sécurité et de défense

¹ Voir à ce sujet Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données*, op. cit., p. 27 à 30.

² Cf. Commissaire aux droits de l'homme du Conseil de l'Europe, *La prééminence du droit sur l'internet et dans le monde numérique en général*, 2014, p. 22.

³ Cf. Conseil de l'Europe, *Partie 1. Les opérations de surveillance massive*, op. cit., p. 5 à 62.

nationales « *doivent faire l'objet d'un examen et d'un contrôle indépendants et efficaces* »¹.

On ne manquera pas de remarquer la proximité des stipulations de la Convention 108 avec celles de l'article 8 de la Conv. EDH. A ce sujet, la Cour de Strasbourg a confirmé que la protection des données personnelles constitue une composante du droit au respect à la vie privée au fil de sa jurisprudence et se réfère à la Convention 108². Du fait que la Cour veille au respect du droit de la protection des données personnelles dans le cadre de son contrôle lorsqu'elle est saisie de questions relatives à la mémorisation de données relative à la vie privée d'un individu par les autorités publiques³, on peut affirmer que la CEDH a ainsi bâti sa jurisprudence en matière de surveillance numérique en cohérence avec le droit de la protection des données personnelles de la Convention 108. Inversement, les juges de Strasbourg n'ont cessé de faire vivre les stipulations européennes relative à la protection des données dans leurs décisions sur la surveillance numérique.

Que ce soient les prescriptions de l'édifice jurisprudentiel de la CEDH en matière de surveillance ou de la protection européenne des données personnelles, ces prescriptions nous apparaissent fondamentales dans l'élaboration du droit du renseignement en droit interne.

§3. Un cadre européen du renseignement numérique en constante évolution

Même si la CEDH juge que le droit français du renseignement présente des garanties suffisantes, il n'en demeure pas moins que sa position présente un caractère nécessairement évolutif en raison du type de contrôle qu'elle exerce sur la surveillance numérique. En outre, il ne serait pas impossible que le Conseil de l'Europe adopte un nouvel instrument juridique dédié au renseignement face à la

¹ Cf. Déclaration conjointe par A. Pierucci, Présidente du Comité de la Convention 108 et J. -P. Walter, Commissaire à la protection des données du Conseil de l'Europe, « *Mieux protéger les personnes dans un contexte de flux international de données : la nécessité d'une supervision démocratique et effective des services de renseignement* », Strasbourg, 7 septembre 2020.

² En ce sens, voir Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données*, op. cit.. et les décisions CEDH, 25 février 1997, *Z c. Finlande* ou encore en matière de surveillance CEDH, 16 février 2000, *Amann c. Suisse*.

³ CEDH, 4 décembre 2008, *S. et Marper c. Royaume-Uni*.

montée en puissance du cyberespionnage dans un contexte de flux international des données.

A - Le caractère évolutif du contrôle de la Cour européenne des droits de l'homme

La position de la Cour de Strasbourg n'est jamais figée quel que soit le thème de son contrôle. En effet, elle a tenu à rappeler que « *la Convention est un instrument vivant à interpréter [...] à la lumière des conditions de vie actuelles* »¹. La prise en compte des évolutions de la société par la Cour s'est particulièrement illustrée en matière de nouvelles technologies numériques. Les juges de Strasbourg ont rapidement appréhendé les enjeux du numérique et adapté leurs raisonnements aux progrès des techniques de traitement des données, notamment pour encourager la numérisation ou encadrer ses dangers². Ce souci d'adaptation aux évolutions du numérique a ainsi accompagné les décisions de la Cour pour déterminer la marge d'appréciation nationale en matière de surveillance numérique. On mentionnera à cet égard qu'en 1978, la Cour n'avait pas remis en question les régimes d'écoutes téléphoniques pour faire face à l'espionnage et au terrorisme dans les démocraties libérales (arrêt *Klass et autres c. Allemagne*) et, qu'en 2021, elle a admis l'interception massive des communications électroniques en raison des nouvelles menaces numériques pour la sécurité nationale (*Big Brother Watch et autres c. Royaume-Uni*). De même, la Cour n'a cessé de développer et de préciser les garanties applicables à la surveillance numérique en fonction des affaires qui lui ont été soumises et des progrès technologiques ainsi que du contexte international de circulation des données³.

Bien qu'il soit possible de voir apparaître un « édifice jurisprudentiel » relatif à la surveillance numérique dans les décisions de la CEDH, il convient d'en relativiser sa portée en raison du large pouvoir d'appréciation dont dispose l'Etat en matière de sécurité et de défense et qu'« *aucun système procédural n'est imposé dès lors que la qualité des garanties données répond aux critères de la*

¹ CEDH, 25 février 1978, *Tyrer c. Royaume-Uni*, §31.

² Voir à ce sujet N. Le Bonniec, *La Cour européenne des droits de l'homme face aux nouvelles technologies de l'information et de communication numériques*, RDLF 2018, chron. n° 5.

³ Voir par exemple les affaires *Uzun c. Allemagne* ou encore *Roman Zakharov c. Russie* et *Big Brother Watch et autres c. Royaume-Uni*.

Convention »¹. Rappelons que la Cour exerce un contrôle avec une « vision globale » sur les législations nationales afin de déterminer *in concreto* une violation de la Conv. EDH pour les requérants, ce qui nous amène à considérer avec prudence la portée de la jurisprudence de la Cour qui peut contraster avec d'autres interprétations telles que celle du droit de l'Union européenne par exemple. Fabien Lafouasse relève notamment que :

« dans *Centrum för Rättvisa et Big Brother Watch et autres*, la Cour européenne adopte une tonalité générale qui contraste avec la jurisprudence de la Cour de justice de l'Union européenne, du Rapporteur spécial des Nations Unies sur le droit à la vie privée et du Comité des droits de l'homme ; le risque de fragmentation dans le corpus des droits de l'homme est latent »².

Dans ces conditions, gardons-nous de prendre l'édifice jurisprudentiel de la CEDH pour acquis dans l'élaboration et le contrôle du droit du renseignement numérique. En tenant compte du caractère évolutif et *in concreto* du contrôle de la CEDH, rien n'exclut que la surveillance de masse à des fins de sécurité nationale admise dans sa jurisprudence *Big Brother Watch c. Royaume-Uni* soit finalement rejetée lorsque ce type de surveillance concerne les autres motifs énoncés à l'article 8 de la Conv. EDH tels que « le bien-être économique du pays ».

Afin d'assurer la conformité du droit du renseignement à la jurisprudence de la CEDH, une veille juridique, préconisée par Eric. A Caprioli³, nous semble nécessaire. De même, il convient de ne pas négliger les réflexions sur l'adoption d'un nouvel instrument conventionnel applicable à la surveillance numérique.

B - L'adoption d'un nouvel instrument juridique du Conseil de l'Europe dédié au renseignement

Dans leur déclaration conjointe précitée, la Présidente du Comité de la « Convention 108 » du Conseil de l'Europe sur la protection des données, Alessandra Pierucci, et le Commissaire à la protection des données du Conseil de l'Europe, Jean-Philippe Walter, ont fait la promotion d'une réflexion sur l'élaboration d'une

¹ Cf. CNCTR, 6^{ème} rapport annuel (2021), p. 54.

² Cf. F. Lafouasse, *Le droit du renseignement : un droit conforme aux traités internationaux*, in *Le droit du renseignement*, op. cit., p. 191.

³ Cf. E. A. Caprioli, *La CEDH invalide partiellement l'ancien système britannique de surveillance électronique*, op. cit..

nouvelle régulation internationale basée sur des principes communs aux Etats en matière de surveillance et d'interception des communications¹. Plus précisément, les auteurs soutiennent qu'il pourrait être envisagé de « *définir ce qui constitue les garanties adéquates et efficaces, une responsabilité effective et un contrôle indépendant des services de renseignement* » dans le cadre d'un « consensus international », par exemple au sein du Conseil de l'Europe. Ce consensus s'appuierait notamment sur la Résolution 68/167 des Nations Unies de 2013 sur la vie privée à l'ère numérique ayant jugé nécessaire que les Etats adoptent une législation nationale conforme au droit international des droits de l'homme en matière de surveillance et de collecte de données personnelles par les services de renseignement et tiendrait compte de la jurisprudence de la CEDH ou encore celle de la Cour suprême des Etats-Unis.

De son côté, la Commission des questions juridiques et des droits de l'homme du Conseil de l'Europe a évoqué dans un rapport de 2015 sur les opérations de surveillance massive l'élaboration d'« *un « code du renseignement » international qui énonce des principes fondamentaux mutuellement admis* »². Selon le rapport, « *ce code définirait précisément ce qui est permis et ce qui est interdit entre alliés et partenaires ; il préciserait ce que les services de renseignement sont autorisés à faire, de quelle manière ils peuvent coopérer et comment des alliés devraient s'abstenir de s'espionner les uns les autres* ». On notera que Hansjörg Geiger, ancien chef du BND allemand et secrétaire d'Etat auprès du ministère de la Justice qui a été auditionné par la Commission, a proposé quatre principes qui pourraient structurer un « code du renseignement » :

- l'interdiction sans exception de l'espionnage politique ou économique mutuel ;
- « *l'activité d'un service de renseignement sur le territoire d'un autre Etat membre peut uniquement être exercée avec le consentement de ce dernier et dans le respect du cadre juridique qui y est applicable* » ;

¹ Cf. Déclaration conjointe par A. Pierucci, Présidente du Comité de la Convention 108 et J. -P. Walter, Commissaire à la protection des données du Conseil de l'Europe, « *Mieux protéger les personnes dans un contexte de flux international de données : la nécessité d'une supervision démocratique et effective des services de renseignement* », op. cit..

² Cf. Rapport de la Commission des questions juridiques et des droits de l'homme sur les opérations de surveillance massive, 18 mars 2015.

- « les données relatives aux ressortissants non soupçonnés d'Etats amis ne sauraient en aucun cas être recherchées, analysées ou conservées massivement. Seules les informations relatives à des personnes légitimement ciblées peuvent être collectées à titre exceptionnel et dans un but précis » ;
- « les sociétés de télécommunications et les fournisseurs de services internet ne peuvent être contraints par les services de renseignement de leur accorder un accès illimité à d'immenses bases de données à caractère personnel ; seule une décision de justice peut ordonner cette mesure ».

Pour les membres de la Commission, cet instrument juridique international permettrait d'encadrer les pratiques de surveillance entre Etats en altérant leur crédibilité en cas de refus d'appliquer le code. En outre, il « offrirait une occasion de combler les vides juridiques et de protéger les citoyens, non seulement de la surveillance de leurs propres gouvernements, mais également de celle des autres Etats contractants »¹.

Si l'initiative est louable, elle demeure très ambitieuse et soulève des questions essentielles comme le contrôle de l'application d'un tel code, ce que n'oublie pas de relever le rapport. Pour notre part, on ajoutera que le renseignement est une fonction stratégique et opérationnelle au cœur des enjeux de souveraineté des Etats. On comprendrait alors aisément qu'un consensus soit difficile à trouver même si les évolutions de la surveillance numérique ne sont pas sans conséquences pour les populations à travers le monde et les intérêts des Etats, notamment dans le domaine du cyberspace².

En revanche, on pourrait s'attendre à un rapprochement plus facile des législations sur le renseignement numérique entre les Etats membres de l'Union européenne depuis que son droit leur enjoint de respecter certaines garanties énoncées par les juges de Luxembourg à la lumière des dispositions de la Charte des droits fondamentaux de l'Union européenne sur la vie privée et la protection des données personnelles.

¹ Cf. Rapport de la Commission des questions juridiques et des droits de l'homme sur les opérations de surveillance massive, 18 mars 2015.

² Cf. Titre II de la Seconde Partie.

§2. Des prescriptions fondamentales pour le droit du renseignement

En France, la jurisprudence de la CEDH a servi de base à l'œuvre du législateur en matière de renseignement. Néanmoins, la question de la conventionnalité du cadre juridique français des techniques de renseignement n'est pas épuisée et reste toujours discutée, ce qui est également le cas pour les fichiers de renseignement.

A – Un droit du renseignement élaboré sur la base de la jurisprudence de la Cour européenne des droits de l'homme

Après les affaires *Klass et autres c. Allemagne* de 1978 et *Malone c. Royaume-Uni* de 1984, la France n'a pas été épargnée par l'œil critique de la CEDH sur les systèmes d'écoutes téléphoniques. Elle a ainsi été condamnée en 1990 dans les affaires *Huvig et Kruslin* pour ne pas avoir indiqué dans son droit interne avec suffisamment de clarté les pouvoirs des autorités dans le domaine des écoutes judiciaires (voire notamment les §32 et §36 dans l'affaire *Huvig*)¹. En effet, si la Cour de Strasbourg a une interprétation large de la notion de « loi » qui englobe les sources tant législatives que jurisprudentielles², elle a néanmoins jugé que la qualité de la loi exigée en matière d'écoutes n'était pas remplie pour deux raisons : d'abord, parce que les écoutes avaient pour socle juridique une jurisprudence judiciaire « fragmentaire », et ensuite, car cette jurisprudence ne définissait pas assez « les catégories de personnes ou d'infractions susceptibles de donner lieu à des écoutes, les limites à la durée de la mesure, les conditions d'établissement des procès-verbaux, leur contrôle, leur destruction après non-lieu ou acquittement »³.

En conséquence, le gouvernement de Michel Rocard a immédiatement réagi en précisant dans la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances électroniques les conditions et modalités des interceptions judiciaires et de sécurité mais aussi leur contrôle avec notamment la création de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) en

¹ Cf. CNCTR, 1^{er} rapport annuel (2015-2015), p. 15 et 16.

² CEDH, 26 avril 1979, *Sunday Times c. Royaume-Uni*, §47.

³ Voir à ce sujet F. Dumas et F. -Nöel Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 52.

matière de renseignement. Alors que la condamnation de la France ne concernait que les écoutes judiciaires, il ne fait désormais aucun doute que la jurisprudence de la CEDH en matière de surveillance a influencé le choix du législateur d'encadrer également les écoutes des services de renseignement alors même que ces derniers relèvent des affaires secrètes de l'Etat¹. Bien plus encore, les affaires *Huvig et Kruslin* ont constitué, à notre sens, une sorte de « précédent » pour la France dans la nécessité de s'appuyer sur la position des juges de Strasbourg pour faire évoluer son droit du renseignement. En effet, la France s'est efforcée, par la suite, de clairement légiférer sur l'attribution de nouveaux outils de surveillance aux services de renseignement en s'alignant sur la jurisprudence de la CEDH. On évoquera le cas de la LPM 2014-2019 du 18 décembre 2013 qui a modifier le régime des accès administratifs aux données de connexion et consacré un dispositif à part entière de géolocalisation en temps réel en tenant compte de la décision *Uzun c. Allemagne* du 2 décembre 2010 dans laquelle la Cour de Strasbourg avait rappelé l'application à cette technique de l'exigence d'une « loi particulièrement précise » conformément à sa jurisprudence *Weber et Saravia c. Allemagne* (arrêt du 2 décembre 2010, §61). Par ailleurs, on retiendra les termes du Professeur Olivier Forcade² affirmant que la loi du 24 juillet 2015 relative au renseignement n'est « *pas une loi de circonstance* » puisqu'elle « *est le fruit d'une maturation et d'une évolution précise de l'encadrement juridique des pratiques de renseignement en France, dans un environnement international attentif* » auxquels nous associeront les mots de l'un des concepteurs de la loi, Jean-Jacques Urvoas, confirmant que le texte a été « *imaginé à partir de la jurisprudence de la Cour européenne des droits de l'homme* »³. On ajoutera que selon ce dernier, la consécration d'un véritable droit du renseignement en France est apparue nécessaire pour offrir aux services des moyens technologiques adaptés à leurs missions⁴, ce qui impliquait pour le législateur d'éviter tout risque de

¹ Voir notamment les rapports « L'arrivé » sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement du 10 juin 2020 (p. 142 et 143) et de J. -J. Urvoas sur le projet de loi relatif au renseignement du 2 avril 2015 (p. 18 et 19) ainsi que l'article de O. Forcade, *Introduction et Retour historique sur les institutions et les pratiques du renseignement français de 1991 à 2015*, Le droit du renseignement, op. cit., p. 19 à 34.

² Cf. O. Forcade, *Introduction*, in Le droit du renseignement, op. cit., p. 20.

³ Cf. Entretien avec Jean-Jacques Urvoas, « *Était-il tolérable que la France soit le seul État européen où les services de renseignement agissaient en dehors de tout cadre juridique ?* », op. cit..

⁴ Cf. supra. Titre I de la Ière Partie.

condamnation par la CEDH en prenant pour base l'analyse de sa jurisprudence notamment parce qu'elle définissait « *en creux mais assez nettement, le contour d'une future loi sur le renseignement* »¹.

Ainsi, le législateur français a profité de la maturation de la jurisprudence de la CEDH pour reprendre directement des principes et garanties dégagées par les juges de Strasbourg dans la loi du 24 juillet 2015, en particulier dans ses dispositions les plus importantes.

Tout d'abord, on relèvera, comme Fabien Lafouasse², que l'article L. 801-1 du code de la sécurité intérieure « présente une structure identique » à l'article 8 de la Conv. EDH en réaffirmant le principe selon lequel le respect de la vie privée constitue la règle générale et l'ingérence de l'autorité publique dans les seuls cas de nécessité d'intérêt public l'exception. Ce même article du code de la sécurité intérieure n'oublie pas de rattacher le secret des correspondances et la protection des données personnelles au droit au respect de la vie privée comme la Cour de Strasbourg a pu le faire dans sa jurisprudence.

Ensuite, la loi de 2015 a institué « en principes opératoires », selon les termes de Floran Vadillo, les principes de proportionnalité et de subsidiarité qui sont régulièrement invoqués par la CEDH pour s'assurer de la conformité des mesures de surveillance à l'article 8§2³ et un ordonnancement des techniques de renseignement inspiré de l'arrêt *Uzun c. Allemagne* du 2 septembre 2010⁴. On peut également citer d'autres garanties essentielles prévues par la loi qui sont directement issues de la jurisprudence *Weber et Saravia c. Allemagne*⁵ : la délimitation des finalités des techniques de renseignement⁶ ou encore la

¹ Dans son rapport d'information de 2013 relatif au cadre juridique applicable aux services de renseignement et dans son rapport législatif de 2015 en tant que rapporteur sur le projet de loi renseignement, Jean-Jacques Urvoas a insisté sur la nécessité d'inscrire la loi sur le renseignement dans le cadre conventionnel de la jurisprudence de la CEDH (cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., 146 et 147).

² Cf. F. Lafouasse, *Le droit du renseignement : un droit conforme aux traités internationaux*, in *Le droit du renseignement*, op. cit., p. 187 à 199.

³ Voir notamment *Affaire Roman Zakharov c. Russie* du 4 septembre 2015, §260.

⁴ Voir en ce sens F. Vadillo, *Quand l'Etat de droit rencontre l'Etat secret : cadre et garanties du recours aux techniques de recueil de renseignement*, in *Le droit du renseignement*, op. cit., p. 91 et 92.

⁵ Cf. supra. Titre II de la Ière Partie.

⁶ Cf. Article L. 811-3 du code de la sécurité intérieure.

limitation dans le temps de la conservation des renseignements collectés¹ et les circonstances impliquant la destruction des transcriptions et extractions réalisées sur ces derniers².

Enfin, on soulignera que dans son étude d'impact³, le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement s'est appuyé non seulement sur les arrêts *Klass et autres c. Allemagne* et *Weber et Saravia c. Allemagne* mais aussi sur des décisions postérieures à la loi de 2015 comme *Roman Zakharov c. Russie* ou plus récemment *Big Brother Watch et autres c. Royaume-Uni* de 2018 pour fonder les modifications et nouvelles mesures sur le renseignement numérique telles que la pérennisation de la technique algorithmique de l'article L. 851-3 ou l'introduction des interceptions satellitaires à l'article L. 852-3. On remarquera en outre que la jurisprudence de la CEDH en matière de protection des données personnelles a été particulièrement invoquée par l'étude d'impact en ce qui concerne les dispositions : sur les transmissions des renseignements qui doivent être prévue par la loi lorsqu'elles sont susceptibles de constituer une ingérence dans la vie privée des individus⁴ ; sur la conservation de données pour la recherche en renseignement qui constituerait un contexte particulier devant être pris en compte par la Cour pour apprécier la conformité d'une durée de conservation plus longue⁵ ; sur la possibilité de conservation des données de connexion par les opérateurs en cas de menace grave pour la sécurité nationale qui a été admise par la Cour de Strasbourg en matière judiciaire⁶.

Toutes les modifications législatives entreprises depuis la condamnation de la France dans les *affaires Huvig et Kruslin* ont été envisagées dans le cadre conventionnel de la jurisprudence de la CEDH sur le respect du droit à la vie privée. Néanmoins, cette prise en compte ne présume pas pour autant de la conventionnalité du droit du renseignement numérique.

¹ Cf. Article L. 822-2 du code de la sécurité intérieure.

² Cf. Article L. 822-3 du code de la sécurité intérieure.

³ Cf. Etude d'impact sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative, 11 mai 2021.

⁴ CEDH, 27 août 1997, *M. S. c. Suède*.

⁵ CEDH, 4 décembre 2008, *S. et Marper c. Royaume-Uni*.

⁶ CEDH, 8 février 2018, *Ben Faiza c. France*.

B - Une conventionnalité discutable du cadre juridique interne du renseignement

Après avoir observé que le législateur français s'était largement inspiré de la jurisprudence des juges de Strasbourg, il reste que la conventionnalité du cadre juridique interne applicable tant aux techniques qu'aux fichiers de renseignement constitue un motif sans cesse invoqué de contestation contre les mesures de surveillance numérique.

1. La conventionnalité des techniques de renseignement

Nous avons eu l'occasion de relever que le Conseil d'Etat, opérant un contrôle de conventionnalité dans le cadre de recours en annulation contre les décrets d'application des lois relatives au renseignement, n'avait soulevé aucune violation de l'article 8 de la Conv. EDH en raison des garanties prévues par les textes¹. Cependant, on rappellera, ici, que les mesures visées à l'article 323-8 du code pénal ayant fait l'objet d'une exception d'inconventionnalité restée sans suite dans l'arrêt *La Quadrature du Net e.a.* de 2018 ne sont entourées d'aucune garantie inspirée de la jurisprudence européenne et pourraient alors être interprétées comme une ingérence disproportionnée dans le droit au respect à la vie privée². Par ailleurs, dans son arrêt de 2018, on notera que le Conseil d'Etat n'avait pas considéré l'absence de notification des mesures de surveillance aux personnes concernées comme un motif d'inconventionnalité en raison des contrôles exercés par la CNCTR et le juge administratif³. Cette analyse rejoint celle de la CNCTR qui avait relevé dans son rapport annuel 2017 que « *la CEDH n'a-t-elle pas jugé, dans ses arrêts les plus récents, qu'une procédure de notification était par elle-même obligatoire* »⁴, une telle procédure ayant été jugée indispensable que si elle constitue un préalable nécessaire à un recours contre les mesures de surveillance⁵.

Si le juge administratif n'a rien trouvé à redire, plusieurs requêtes ont été introduites devant la Cour de Strasbourg contre la loi du 24 juillet 2015 qui

¹ Cf. supra. Chapitre I du Titre I de la Ière Partie. Voir notamment les décisions CE, 12 février 2016, *Association French Data Network et autres* et CE, 26 juillet 2018, *La Quadrature du Net e.a.*

² Cf. supra. §3 de la Section II du Chapitre I du Titre I de la Ière Partie.

³ CE, 26 juillet 2018, considérants 12 et 13.

⁴ Cf. CNCTR, 2^{ème} rapport annuel (2017), p. 76.

⁵ CEDH, 4 décembre 2015, *Roman Zakharov c. Russie*.

soutiennent notamment plusieurs manquements au droit au respect de la vie privée garantie par l'article 8 de la Conv. EDH¹ : l'absence d'une définition claire des données de connexion (« informations ou documents ») ; une protection insuffisante des professions de journaliste et d'avocat ; une définition trop large des finalités des techniques de renseignement ; une insuffisance des garanties procédurales et l'absence d'un recours effectif en raison des aménagement des principes du droit à un procès équitable et du contradictoire ainsi que l'absence total de recours en matière de partage international des renseignements². Bien que la loi du 30 juillet 2021 ait renforcé les garanties applicables aux techniques de renseignement, la CNCTR s'est gardée « d'émettre des hypothèses sur l'issue de ces requêtes » tout en relevant que « lorsque la CEDH apprécie la conformité d'un régime de droit interne aux exigences de la Convention, elle adopte une vision globale de son fonctionnement »³.

Pour certains auteurs, la loi du 24 juillet 2015 ferait toutefois preuve de « démesure et imprécisions sur le domaine du renseignement » laissant place à une potentielle « surveillance permanente et générale » contraire à la jurisprudence de la CEDH⁴. Pour notre part, on partagera l'avis du spécialiste du droit international du renseignement, Fabien Lafouasse, selon lequel la loi du 24 juillet 2015 « embrasse et régule » les trois stades des opérations de surveillance (avant/pendant/après) conformément aux standards dégagés par le Professeur Asaf Lubin et qui se retrouvent dans la jurisprudence *Roman Zakharov c. Russie* de la CEDH⁵. Autrement dit, la loi du 24 juillet 2015 et ses modifications pourraient ne pas être fondamentalement remises en cause par une censure des juges de Strasbourg dans une appréciation globale du dispositif, y compris au regard des arrêts *Big Brother Watch et autres c. Royaume-Uni* et *Centrum för rättvisa c. Suède*

¹ CEDH, 26 avril 2017, n° 49526/15 et autres, *Association confraternelle de la presse judiciaire c. France* (décision de recevabilité).

² Cf. CNCTR, 4^{ème} rapport annuel (2019), p. 45 et 46.

³ Cf. CNCTR, 6^{ème} rapport annuel (2021), p. 53 et 54.

⁴ Voir en ce sens C. Lazerges et H. Henrion-Stoffel, *Politique criminelle, renseignement et droits de l'homme*, op. cit..

Pour des critiques dans le même sens, voir aussi : cf. O. Desaulnay et R. Ollard, *Le renseignement français n'est plus hors-la-loi Commentaire de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement*, op. cit..

⁵ Cf. F. Lafouasse, *Le droit du renseignement : un droit conforme aux traités internationaux*, in *Le droit du renseignement*, op. cit., p. 187 à 199.

du 25 mai 2021 qui exigent des « garanties de bout en bout » en matière de surveillance de masse. En revanche, ces derniers arrêts invitent la France à mettre rapidement en cohérence notre droit du renseignement sur le partage international des renseignements comme le soulignent la CNCTR et la DPR¹.

2. La conventionnalité des fichiers de renseignement

Il convient de commencer par rappeler que le cadre juridique des fichiers de renseignement est déterminé par la loi Informatique et libertés en ce qui concerne leur création et leur mise en œuvre et par la loi relative au renseignement relative au pour ce qui est du contentieux. Ce contexte juridique interne doit non seulement faire face à la jurisprudence de la CEDH mais aussi aux stipulations de la Convention 108. En effet, cette dernière a été ratifiée par la France en 1983 et constitue donc une norme de référence supérieure à la loi en vertu de l'article 55 de la Constitution de 1958, que la CNIL prend en compte dans son contrôle², même si sa portée demeure relative puisque la loi informatique et libertés adoptée en 1978 consacre des principes identiques³.

En matière de surveillance, la Convention 108 a d'ailleurs pu être directement invoquée, en parallèle des stipulations de l'article 8 de la Conv. EDH, devant le Conseil d'Etat dans l'arrêt *CGT* du 28 juillet 1995 (requête n° 132453) portant sur le décret relatif au fichier des Renseignements généraux (RG). Dans cette affaire, le juge administratif avait cependant jugé compatible le régime dérogatoire des fichiers de souveraineté. Et comme en matière de techniques de renseignement, la jurisprudence du Conseil d'Etat n'a pour le moment pas remis en question la conventionnalité des fichiers de renseignement au regard de la CEDH⁴. Par exemple, le cadre juridique du fichier CRISTINA de la DGSI a été jugé

¹ Voir notamment CNCTR, *6^{ème} rapport annuel (2021)*, p. 52 et F. Dumas et F. -Nöel Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit., p. 58 ainsi que nos développements et propositions sur le partage international des renseignements dans le §4 de la Section I du Chapitre II du Titre I de la Ière Partie.

² CNIL, *6^{ème} rapport annuel (1985)*, p. 215.

³ En ce sens, voir L'ouvrage Le Lamy droit du numérique, *Partie 2 Numérique et libertés, Division 1 Le traitement des données à caractère personnel, Chapitre 1 Historique du dispositif de protection des données personnelles, Section 2 Les travaux du Conseil de l'Europe, §1 La Convention 108 du Conseil de l'Europe*.

⁴ Voir en ce sens, S. Gottot, *Renseignement : premières décisions de la formation spécialisée du Conseil d'Etat*, AJDA 2017. 581.

conforme aux stipulations de la Convention¹. La formation spécialisée du Conseil d'Etat n'a, quant à elle, relevé aucune inconstitutionnalité en ce qui concerne le FPR². Enfin, s'agissant des traitements EASP, PASP et GIPASP, le juge administratif a considéré que :

« il n'apparaît pas que la collecte de ces données dans les traitements litigieux entraînerait une atteinte grave et manifestement illégale au droit au respect de la vie privée ou à la liberté d'opinion. Et il ne saurait, dès lors, être utilement soutenu que la France aurait dû saisir le Conseil de l'Europe d'une demande de dérogation aux obligations prévues par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales avant de prendre les mesures contestées »³.

Pour une partie de la doctrine, le juge administratif a pu être considérée comme « guère exigeant » dans son contrôle de conventionnalité du cadre dérogatoire des fichiers de souveraineté, notamment en ce qui concerne l'absence de publication de leur base légale⁴. Dans un contexte de montée en puissance de la protection européenne des données personnelles, on suivra alors la recommandation du Professeur Xavier Latour selon laquelle les autorités publiques et les juges français devraient faire preuve de vigilance en matière de fichiers de sécurité et de défense⁵. D'autant plus que le cadre européen du renseignement numérique est en constante évolution.

¹ CE, 16 avril 2010, *Association AIDES et autres*, décision n° 320196.

² CE, formation spécialisée, 6 novembre 2017, n° 409075.

³ CE, 4 janvier 2021, *Association VIA La Voie du Peuple et autres et CGT et autres*, requêtes n° 447868 ; 447970 ; 447972 ; 447974.

⁴ Voir en ce sens V. Gautron, « Une mémoire policière hypertrophiée : la fin du droit à l'oubli ? », *Les Cahiers de la Justice*, vol. 4, no. 4, 2016, pp. 607-617.

⁵ Cf. X. Latour, *Sécurité intérieure : un droit « augmenté »*, op. cit..

SECTION II : Les exigences du droit de l'Union européenne

Consciente de la révolution numérique et de son caractère transnational, l'Union européenne a fait de la vie privée et de la protection des données personnelles une préoccupation majeure de son droit, notamment en condamnant la surveillance numérique de masse et en enjoignant aux Etats membres d'adopter une position restrictive dans leur législation relative au renseignement.

La vie privée numérique, un droit fondamental de l'Union européenne. Rappelons que le respect de la vie privée numérique comme la protection des données personnelles a été consacrée d'abord en droit dérivé¹ par une directive européenne 95/46/CE relative à la protection des données personnelles du 24 octobre 1995 puis ensuite dans le droit primaire² comme un droit fondamental de l'Union européenne depuis la signature du traité de Lisbonne le 13 décembre 2007 qui a reconnu la même valeur que les traités à la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000³ qui dispose que :

- « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* »⁴ ;
- « *1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la*

¹ Le droit dérivé est l'ensemble des normes adoptées par le législateur de l'UE sur le fondement des traités constitutifs de l'Union. En vertu des règles relatives à la hiérarchie des normes du droit de l'UE, une directive est un acte juridique qui nécessite d'être transposée en droit interne dans le but d'harmoniser les législations vers des objectifs communs en laissant aux Etats membres le choix de la forme et des moyens. La directive européenne doit être distinguée du règlement européen qui est un acte contraignant de portée générale directement applicable dans les Etats membres ayant vocation à uniformiser l'application du droit de l'UE (article 288 TFUE).

² Le droit primaire de l'UE désigne les traités constitutifs de l'Union ratifiés par les Etats membres ainsi que les textes ayant même valeur comme la Charte des droits fondamentaux de l'Union européenne.

³ Article 6§1 du Traité sur l'Union européenne.

⁴ Article 7 de la Charte des droits fondamentaux de l'Union européenne.

rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante »¹.

En outre, le traité de Lisbonne n'a pas manqué de confier à l'Union européenne une véritable compétence en matière de protection des données personnelles, y compris dans le domaine de la coopération policière et judiciaire en matière pénale². C'est ce cadre de droit primaire qui a permis d'aboutir à l'adoption en 2016 du règlement général sur la protection des données personnelles (UE) 2016/679 (ou dit « RGPD ») qui constitue aujourd'hui le cadre juridique de référence auquel la loi Informatique et libertés française a dû s'adapter³. Par ailleurs, on soulignera que la protection de la vie privée numérique constitue également un objectif de la réalisation d'un espace de liberté, de sécurité et de justice⁴.

L'Union européenne face à la surveillance numérique de masse. Les « révélations Snowden » de 2013 sur les programmes de surveillance américains de la NSA ont remis en question la réelle protection de la vie privée numérique des citoyens de l'Union européenne, ce qui a conduit le Parlement européen à adopter une résolution pour condamner « *les activités de surveillance de masse aveugle* » et renforcer le « *contrôle démocratique des services de renseignement* »⁵. Cependant, le texte du Parlement ne constitue pas un acte juridiquement contraignant. En revanche, la Cour de justice de l'Union européenne (CJUE), dont les décisions ont force obligatoire⁶, n'a pas hésité à affirmer au fil de sa jurisprudence une interprétation sévère des textes de l'Union européenne relatifs à la vie privée numérique afin d'exiger des Etats de limiter fortement leurs mesures de surveillance numérique.

¹ Article 8 de la Charte des droits fondamentaux de l'Union européenne.

² A ce sujet, voir l'article 16 du Traité sur le fonctionnement de l'Union européenne dit « TFUE » et Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données*, op. cit., p. 32.

³ La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles a réorganisé la loi informatique et libertés afin de l'adapter aux nouvelles dispositions du RGPD.

⁴ Article 3§2 du Traité sur l'Union européenne dit « TUE ».

⁵ Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)).

⁶ Article 280 du Traité sur le fonctionnement de l'Union européenne.

L'analyse de la jurisprudence de la CJUE nous conduit d'abord à discuter de la compétence de l'Union européenne en matière de renseignement numérique qui n'apparaît pas nécessairement évidente (§1). Ensuite, il convient de consacrer un développement minutieux sur les « garanties essentielles européennes » dégagées par la Cour de Luxembourg (§2) avant d'analyser la conformité, que l'on qualifiera d'« augmentée », du droit du renseignement à ces garanties (§3). Pour finir, il ressort de notre étude qu'il nous semble indéniable qu'une européanisation du droit du renseignement s'opère dans sa relation indissociable avec le droit européen de la vie privée numérique (§4).

§1. La compétence de l'Union européenne en matière de renseignement

A priori, ni l'Union européenne ni la CJUE n'ont de compétence en matière de renseignement d'Etat au regard de l'article 4§2 TUE qui stipule que :

« L'Union respecte l'égalité des États membres devant les traités ainsi que leur identité nationale, inhérente à leurs structures fondamentales politiques et constitutionnelles, y compris en ce qui concerne l'autonomie locale et régionale. Elle respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre ».

Ajoutons que le Traité sur le fonctionnement de l'Union européenne consacre également une compétence exclusive des Etats membres dans leurs relations en matière de sécurité nationale en stipulant à l'article 73 que :

« Il est loisible aux États membres d'organiser entre eux et sous leur responsabilité des formes de coopération et de coordination qu'ils jugent appropriées entre les services compétents de leurs administrations chargées d'assurer la sécurité nationale ».

Pour autant, ces stipulations de droit primaire n'ont pas empêché la Cour de justice de mettre en cause les activités de sécurité nationale à l'occasion de son

contrôle sur les règles du droit de l'Union européenne¹, notamment en ce qui concerne le renseignement et la conservation des données personnelles et le transfert de ces données hors de l'Union européenne. Dans ce cadre, les juges de Luxembourg ont considéré que l'encadrement et le contrôle de la coopération entre les services de renseignement et des acteurs économiques qui traitent des données personnelles conformément au droit de l'Union européenne entrent dans le champ d'application de ce dernier. Si cette solution demeure limitée à la surveillance numérique partenariale, elle a pu susciter la controverse pour ses implications en matière de souveraineté.

A - Une compétence limitée à la surveillance numérique partenariale

Il ressort de la jurisprudence de la Cour de Luxembourg que le droit de l'Union européenne applicable aux activités des services de renseignement ne concerne que les accès aux données conservées par les opérateurs du numérique et les acteurs des transports ou les accès aux données transférés hors de l'Union européenne.

1. L'accès aux données conservées par les opérateurs du numérique

Dans le prolongement de la directive 95/46/CE sur la protection des données personnelles, le législateur de l'Union européenne a adopté, le 12 juillet 2002, la directive 2002/58/CE qui vise spécifiquement à protéger la vie privée dans le secteur des communications électroniques. Selon cette dernière, les opérateurs du numérique sont tenus d'assurer la confidentialité des communications ainsi que des données de connexion, c'est-à-dire relatives au trafic et à la géolocalisation. Cependant, elle a admis en son article 15 que les Etats membres puissent prendre des mesures législatives afin d'obliger les opérateurs à conserver pour une durée limitée les données des utilisateurs pour les besoins de la sûreté de l'Etat, la défense et la sécurité publique ainsi que les enquêtes pénales. Par la suite, la directive 2006/24/CE est ainsi venue modifier celle de 2002 afin d'harmoniser les législations nationales sur l'application de l'article 15 en imposant aux opérateurs une conservation pour une durée minimale de six mois et maximale de deux ans de l'ensemble des données de connexion des

¹ Sur la compétence de la CJUE en matière de sécurité nationale, voir notamment B. Warusfel, *Conservation des données et sécurité nationale au regard du droit de l'Union européenne*, in *Annuaire 2022 du droit de la sécurité et de la défense*, mare et martin, 2022, pp. 161-173.

utilisateurs (articles 5 et 6). S'agissant des accès à ces données par les autorités, la directive de 2006 renvoyait au droit interne des Etats membres (article 4). On notera qu'une autre directive 2009/136/CE du 25 novembre 2009 a également modifié les dispositions de l'article 15 de la directive de 2002 pour imposer aux opérateurs de prévoir des procédures conformément au droit national pour répondre aux demandes d'accès aux données.

Alors que ce cadre juridique laissait une large place à la réglementation nationale en matière d'accès aux données de connexion par les services de renseignement, la CJUE en a jugé autrement dès lors que le droit primaire de l'Union européenne a consacré le droit fondamental à la vie privée numérique et dans un contexte marqué par les révélations Snowden. En effet, la Cour a été amenée à préciser son interprétation des dispositions de l'article 15 de la directive 2002/58/CE après avoir entièrement invalidé la directive 2006/24/CE dans son arrêt *Digital Rights Ireland et Seltlinger ea.* du 8 avril 2014 (affaires jointes C-293/12 et C-594/12) dans lequel les juges de Luxembourg ont considéré qu'au regard des articles 7 et 8 de la Charte que « *cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* » (point 65).

Par son arrêt *Tele2 Sverige et Watson e.a.* du 21 décembre 2016 (affaires jointes C-203/15 et C-698/15), la Cour a considéré non seulement que les mesures législatives qui imposent une obligation de conservation des données de connexion aux opérateurs entrent dans le champ d'application de l'article 15 de la directive 2002/58/CE et donc du droit de l'Union européenne mais aussi les mesures législatives relatives à l'accès par les autorités nationales en raison du fait que ces mesures portent nécessairement sur des traitements de données réalisés par les opérateurs, peu importe que l'article 1^{er}§3 de ladite directive exclue de son champ d'application les activités de l'Etat relevant du renseignement ou du droit pénal (points 64 à 81). Les juges de Luxembourg ont confirmé cette interprétation en affirmant également la compétence de la Cour de justice pour répondre aux questions de droit que soulève l'application de la directive litigieuse dans la décision *Ministerio Fiscal* du 2 octobre 2018 (affaire C-207/16, points 28 à 43). A

cet égard, la CJUE a été saisie de questions préjudicielles par les juridictions nationales britannique, belge et française dans le cadre de litiges sur la législation de ces pays relatives aux accès aux données par les services de renseignement¹. Deux questions concernaient particulièrement la compétence de l'Union européenne :

- la question de savoir si, à la lumière de l'article 4§2 TUE, les accès aux données pour des raisons de sécurité nationale n'étaient pas exclus du champ d'application du droit de l'Union européenne ;
- la question moins explicitée par les juridictions nationales de savoir quels sont les types d'accès qui entrent dans le champ d'application du droit de l'Union européenne.

Dans ces deux arrêts du 6 octobre 2020 *Privacy International* (affaire C-623/17) et *La Quadrature du Net e.a.* (affaires jointes C-511/18, C-512/18 et C-520/18), la Cour de Luxembourg a finalement maintenu sa jurisprudence pour les accès aux données en matière de sécurité nationale en précisant toutefois que :

*« lorsque les États membres mettent directement en œuvre des mesures dérogeant à la confidentialité des communications électroniques, sans imposer des obligations de traitement aux fournisseurs de services de telles communications, la protection des données des personnes concernées relève non pas de la directive 2002/58 mais du seul droit national »*².

Ainsi, les techniques suivantes n'entrent pas dans le champ d'application du droit de l'Union européenne :

- les interceptions de sécurité et satellitaires qui concernent le contenu des communications³ mais aussi les interceptions des communications

¹ Dans l'ordre des pays mentionnés : Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête au Royaume-Uni), 30 octobre 2017, affaire *Privacy International* (IPT/15/110/CH) ; Cour constitutionnelle belge, 19 juillet 2018, loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (arrêt n° 96/2018) ; Conseil d'Etat, 26 juillet 2018, *La Quadrature du Net* et autres (requête n° 394922).

² Cf. Arrêts de la CJUE *Privacy International*, point 48 et *La Quadrature du Net e.a.*, point 103.

³ Articles L. 852-1 à L. 852-3 du code de la sécurité intérieure.

internationales¹ et le régime d'exception des communications hertziennes ouvertes² ;

- les accès aux données de connexion et de géolocalisation par des appareils ou dispositifs techniques directement mis en œuvre par les agents des services³ ;
- les sonorisations et captations d'images et de données informatiques⁴.

En revanche, aucune technique de renseignement d'accès aux données de connexion et de géolocalisation en temps différé ou en temps réel via les opérateurs n'échappent à l'application du droit de l'Union européenne, c'est-à-dire en France l'ensemble des mesures prévues aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure. En revanche,

On profitera de cette clarification pour préciser que les fichiers des services de renseignement constituent des mesures directement mises en œuvre par l'Etat qui relèvent donc du seul droit national au regard de l'article 2§2 du RGPD⁵ et de la logique jurisprudentielle de la CJUE.

2. L'accès aux données conservées par les acteurs des transports

De manière indirecte, le droit de l'Union européenne encadre l'accès des services de renseignement aux données détenues par les transporteurs aériens des dossiers de passagers (PNR) de vols extra-européens, voire de vols intra-européens. En effet, la directive européenne 2016/681 du 27 avril 2016 relative à l'utilisation des données PNR pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière régit le traitement des données concernées dans les Etats membres par l'Unité Information Passagers (UIP) et leur communication aux autorités nationales compétentes qui peuvent être les services de

¹ Articles L. 854-1 à L. 854-9 du code de la sécurité intérieure.

² Articles L. 855-1 A à L. 855-1 C du code de la sécurité intérieure.

³ Articles L. 851-5 et L. 851-6 du code de la sécurité intérieure.

⁴ Articles L. 853-1 à L. 853-3 du code de la sécurité intérieure.

⁵ Le point 16 introductif du RGPD précise d'ailleurs que : « *le présent règlement ne s'applique pas à des questions de protection des libertés et droits fondamentaux ou de libre flux des données à caractère personnel concernant des activités qui ne relèvent pas du champ d'application du droit de l'Union, telles que les activités relatives à la sécurité nationale. Le présent règlement ne s'applique pas au traitement des données à caractère personnel par les Etats membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union* ».

renseignement comme en France en vertu de l'article R. 232-15 du code de la sécurité intérieure. Soulignons que la CJUE a eu l'occasion de renforcer l'application de la directive 2016/681 dans sa décision récente *Ligue des droits humains* du 21 juin 2022 (affaire C-817/19) en précisant notamment les garanties exigées par le droit de l'Union européenne dans le traitement et la communication des données PNR aux services de renseignement qui ne sont pas sans rappeler les garanties dégagées par l'arrêt *La Quadrature du Net e.a.* de 2020¹.

3. L'accès aux données transférées hors de l'Union européenne

De façon encore plus éloignée, la jurisprudence de la CJUE relative à la réglementation européenne en matière de transferts de données personnelles hors de l'Union tend à étendre l'application du droit de l'Union européenne relatif à la surveillance numérique aux pays tiers. Cette tendance s'est affirmée dans les relations entre l'Union européenne et les Etats-Unis et le Canada.

Considérant que les accès par les services de renseignement américains aux données personnelles des citoyens de l'Union européenne transférées aux Etats-Unis constitue une ingérence dans les droits fondamentaux de l'Union européenne et que le droit américain ne présente pas des garanties similaires au droit de l'Union européenne dans l'accès à ces données, la Cour de justice de Luxembourg a invalidé à deux reprises des décisions d'adéquation de la Commission européenne de protection des données UE-Etats-Unis dans ses arrêts *Schrems I* du 6 octobre 2015 (affaire C-362/14) et *Schrems II* du 16 juillet 2020 (affaire C-311/18).

S'agissant du Canada, la CJUE s'est également prononcée défavorablement à l'accord PNR UE-Canada dans son *avis 1/15* du 26 juillet 2017 toujours en raison du fait que l'encadrement des données personnelles transférées et leur accès par les autorités canadiennes ne répondait pas aux standards de la Cour de justice en matière de surveillance numérique².

¹ Voir à ce sujet S. Hourson, « *Données passagers* » : le contrôle de la machine, Droit administratif n° 8-9, Août 2022, alerte 105.

² Sur ce point, voir V. Correia, *A propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens*, Communication Commerce électronique n° 6, Juin 2018, étude 10.

Bien que l’empiètement du droit de l’Union européenne dans l’encadrement des accès par les services de renseignement aux données personnelles demeure limité à certaines circonstances liées à l’économie numérique européenne et peut, à ce titre, sembler légitime, il reste que la compétence de l’Union européenne en matière de surveillance numérique s’est affirmée par une jurisprudence extensive de la CJUE au regard de la souveraineté des Etats qui a pu être critiquée.

B - Une compétence discutable en matière de souveraineté

La résolution d’un conflit de normes entre le droit national et le droit de l’Union européenne était inévitable en raison des critiques sur la compétence de l’Union européenne.

1. Une compétence critiquée

Avant de discuter du conflit de normes qu’a engendré la jurisprudence de la CJUE dans le droit interne des Etats membres et notamment la France, on évoquera la position des juges de Luxembourg en matière de transferts de données personnelles qui incite clairement les pays tiers à s’aligner sur le droit de l’Union européenne dans leur législation en matière de renseignement pour qu’une décision d’adéquation soit valable¹. C’est ainsi que les décisions *Schrems 1 et 2* invitent les Etats-Unis à revoir leur législation pour se conformer aux standards européens relatifs à la protection des données personnelles et à la surveillance numérique². Si cette extraterritorialité du droit de l’Union européenne peut sembler salubre pour la défense des droits fondamentaux à l’ère du cyberspace³, elle pourrait être perçue comme une immixtion de la CJUE dans les affaires diplomatiques de l’Union européenne et dans la souveraineté des pays tiers sans néanmoins, selon nous, constituer une intervention ou une ingérence illicite au

¹ A ce sujet, voir F. Mattatia, *Données personnelles : la CJUE invalide le Privacy Shield*, La Semaine Juridique Administrations et Collectivités territoriales n° 36, 7 septembre 2020, act. 491.

² Voir à ce sujet B. Haftel, *Transferts transatlantiques de données personnelles : la Cour de justice invalide le Safe Harbour et consacre un principe de défiance mutuelle*, Recueil Dalloz 2016 p.111 et D. Simon, *Coup de tonnerre dans le monde du numérique. La Cour de justice prononce l’invalidité du « bouclier de protection de la vie privée » à propos des transferts de données personnelles vers les États-Unis*, Europe n° 8-9, Août 2020, étude 8.

³ Voir à ce sujet D. Simon, *Coup de tonnerre dans le monde du numérique. La Cour de justice prononce l’invalidité du « bouclier de protection de la vie privée » à propos des transferts de données personnelles vers les États-Unis*, op. cit..

sens du droit international¹. Au regard de ces considérations, il nous semble également fort probable que l'Union européenne aura des difficultés à élaborer de nouveaux « boucliers » de protection de données personnelles ou d'autres accords portant sur ces données avec les Etats-Unis ou d'autres pays tiers².

Mais la situation la plus délicate concerne la conciliation entre le respect de la souveraineté des Etats membres en matière de sécurité nationale et du principe de primauté du droit de l'Union européenne consacré par la jurisprudence de la Cour de Luxembourg³. L'arrêt *Tele2 Sverige et Watson e.a.* de 2016 a particulièrement suscité de vives réactions. Dès la sortie de la décision, la DPR a dénoncé un arrêt qui « *empiète sur la compétence des États, telle qu'elle résulte de l'application du principe de subsidiarité, et ne tient manifestement aucun compte des impératifs et des finalités qui s'attachent à l'action des services de renseignement* »⁴. De leur côté, les rédacteurs du « rapport Larrivé » de 2020 ont, sans ménagement, qualifié l'arrêt de « véritable *hold-up* jurisprudentiel » tout en considérant que les accès aux données de connexion par les services de renseignement relevaient de la compétence exclusive de l'Etat et que leur contrôle ne pouvait être exercé que par le Conseil constitutionnel, le Conseil d'Etat ou la CEDH mais en aucun cas par la CJUE qui « *n'a, aux yeux des membres de la mission, aucune place dans ce système* »⁵. Si les arrêts *La Quadrature du Net e.a.* de 2020 de la CJUE et *French Data Network e.a.* du 21 avril 2021 du Conseil d'Etat (requête n° 393099) ont finalement donné tort aux membres de la mission d'information, il est vrai que la décision de 2016 représentait une « épée de Damoclès » pour le renseignement français avec un risque de remise en cause des accès aux données de connexion en temps différé

¹ Cf. D. Allard, *Les 100 mots du droit international, points 50. Ingérence (non-ingérence) et 53. Intervention*, Presses Universitaires de France, 2021, p 65 et 66 et p. 69 et 70.

² Voir en ce sens A. Danis-Fatôme, *Arrêt Schrems II : sauvetage de façade des « clauses contractuelles types » mais invalidation du bouclier de protection des données*, Communication Commerce électronique n° 11, Novembre 2020, comm. 83 ; V. Correia, *À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens*, op. cit..

³ Voir notamment les décisions de la Cour *Van Gend en Loos* du 5 février 1963 (affaire 26/62), *Costa/E.N.E.L.* du 15 juillet 1964 (affaire 6/64), *Internationale Handelsgesellschaft mbH* du 17 décembre 1970 (affaire 11/70), *Simmenthal* du 9 mars 1978 (affaire 106/77) et *Marleasing* du 13 novembre 1990 (affaire C-106/89).

⁴ Cf. P. Adam, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, op. cit., p. 80.

⁵ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 138 et 153 à 165.

pouvant mettre en difficulté les services¹. Ainsi, sans surprise de nombreuses juridictions nationales des Etats membres, à l'instar du Conseil d'Etat, ont invité la Cour de Luxembourg à reconsidérer sa position². Néanmoins, comme nous l'avons vu, la CJUE a maintenu sa position sur l'extension du champ d'application de la directive 2002/58/CE au domaine de la sécurité nationale malgré les stipulations de l'article 4§2 TUE et les dispositions de l'article 1^{er}§3 de ladite directive³. On relèvera que l'obstination de la Cour a pu également faire l'objet d'une analyse critique des Professeurs Loïc Azoulai et Dominique Ritleng considérant que : « *Si la Cour de justice consacre pareille extension du champ d'application de ladite directive, c'est sans doute qu'elle voit là le seul moyen à sa disposition pour contrôler les violations de droits élémentaires pouvant découler d'une invocation abusive des motifs de sécurité publique ou de sécurité nationale. Il y a de l'opportunisme dans cette solution, qui peut blesser la rigueur juridique* »⁴.

En saisissant cette opportunité, la Cour a créé les conditions d'un conflit de normes entre le droit de l'Union européenne et le droit interne des Etats membres. En France, le Conseil d'Etat a ainsi été amené à statuer sur l'articulation entre l'ordre juridique l'Union européenne et l'ordre juridique national et à confronter « les exigences constitutionnelles invoquées en défense par l'Etat » à la jurisprudence de la CJUE.

¹ Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 138 et 153 à 165.

² En dehors du Conseil d'Etat, de la Cour constitutionnelle belge et de l'Investigatory Powers Tribunal britannique, les autres juridictions nationales invitant la CJUE à reconsidérer sa position sont : la Cour provincial de Tarragone en Espagne, la Cour suprême d'Estonie, la Cour suprême d'Irlande ou encore la Cour administrative fédérale allemande et la Cour de cassation française (voir notamment CNCTR, *Les réactions des Etats : inviter la CJUE à reconsidérer sa position*, 6^{ème} rapport annuel (2021), p. 34 à 36 et, en particulier pour le Conseil d'Etat, M. -C. de Montecler, *Techniques de renseignement : quand le Conseil d'Etat invite la Cour de justice de l'Union européenne à revoir sa jurisprudence*, AJDA, 2018, p. 1586).

³ Cf. Arrêt *La Quadrature du Net e.a.* de la CJUE de 2020.

⁴ Cf. L. Azoulai et D. Ritleng, « *L'État, c'est moi* ». *Le Conseil d'État, la sécurité et la conservation des données*, RTD Eur., 2021, p.349.

2. La résolution du conflit de normes

Dans sa décision *French Data Network e.a.* du 21 avril 2021 (requête n° 393099), la haute juridiction administrative a tenu à rappeler que :

« Le respect du droit de l'Union constitue une obligation tant en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne qu'en application de l'article 88-1 de la Constitution. Il emporte l'obligation de transposer les directives et d'adapter le droit interne aux règlements européens. En vertu des principes de primauté, d'unité et d'effectivité issus des traités, tels qu'ils ont été interprétés par la Cour de justice de l'Union européenne, le juge national, chargé d'appliquer les dispositions et principes généraux du droit de l'Union, a l'obligation d'en assurer le plein effet en laissant au besoin inappliquée toute disposition contraire, qu'elle résulte d'un engagement international de la France, d'une loi ou d'un acte administratif » (considérant 4).

Dans ces conditions, la Conseil d'Etat a alors jugé que : *« il n'appartient pas au juge administratif de s'assurer du respect, par le droit dérivé de l'Union européenne ou par la Cour de justice elle-même, de la répartition des compétences entre l'Union européenne et les Etats membres »* (considérant 8).

Cependant, le raisonnement des juges du Palais Royal va plus loin en considérant que l'article 88-1 place la Constitution au sommet de l'ordre juridique interne auquel est intégré celui de l'Union européenne, ce qui peut conduire le juge national à devoir écarter l'application d'une norme européenne contraire à des exigences constitutionnelles en l'absence d'une protection équivalente dans les deux ordres juridiques (considérants 5 à 7). En l'espèce, le Conseil d'Etat a jugé que les objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme invoqués en défense par l'Etat ne bénéficiaient pas d'une protection équivalente en droit de l'Union européenne en raison de l'incompétence de l'Union dans ces

domaines (considérants 9 et 10) sans néanmoins avoir écarté *in fine* les injonctions de la CJUE en matière de renseignement¹.

Le Conseil d'Etat a ainsi refusé d'opérer un contrôle *ultra vires* qui est, par exemple, pratiqué par la Cour constitutionnelle fédérale d'Allemagne², c'est-à-dire d'apprécier si le droit de l'Union européenne a outrepassé ou non les compétences attribuées à l'Union. En revanche, il a activé la « clause de sauvegarde Arcelor », pour reprendre les termes employés par le rapporteur public, Alexandre Lallet, dans ses conclusions en référence à la jurisprudence *Société Arcelor Atlantique et Lorraine et autres* du Conseil d'Etat du 8 avril 2007 (requête n° 287110) qui a défini le contrôle de constitutionnalité des actes réglementaires de transposition d'une directive européenne impliquant un contrôle préalable de l'équivalence des protections entre les ordres juridiques. Toutefois, l'arrêt *French Data Network e.a.* innove en appliquant la jurisprudence *Arcelor* comme un moyen de défense dans l'hypothèse d'un acte réglementaire considéré comme contraire au droit de l'Union européenne, ce qui consiste en une sorte de « défense antimissile » (conclusions A. Lallet) contre l'application de ce dernier au droit interne. Ce type de contrôle est proche de celui de « l'identité constitutionnelle » exercé par le Conseil constitutionnel³ et, à ce titre, il n'a pas été jugé étonnant par certains commentateurs que les objectifs de valeur constitutionnelle de sécurité aient été donc retenus par le juge administratif puisqu'il ne s'agit pas toujours de protéger les droits fondamentaux mais aussi de garantir l'intérêt général⁴. Il est vrai que l'utilité contentieuse des objectifs de valeur constitutionnelle est avérée devant le Conseil constitutionnel, notamment pour limiter les pouvoirs du législateur⁵. A notre sens, il n'y aurait donc pas d'obstacle à ce que le Conseil d'Etat mobilise

¹ En ce sens, voir B. Bertrand et J. Sirinelli, *Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle*, Dalloz IP/IT, 2021, p.408.

² Le contrôle *ultra vires* a été consacré par la Cour constitutionnelle fédérale d'Allemagne en 2009 à l'occasion du traité de Lisbonne (BVerfGE, 30 juin 2009, Lisbonne, 2 BvE 2/08) et a été réaffirmé récemment dans l'affaire *Weiss* impliquant la Banque centrale européenne (CJUE, Gde ch., 11 déc. 2018, *Weiss*, C-493/17) dans un arrêt de la juridiction allemande du 5 mai 2020.

³ Voir à ce sujet A. Levade, *Le Conseil constitutionnel et l'Union européenne*, Cahiers du Conseil constitutionnel, hors série – colloque du cinquantenaire, 3 novembre 2009 et CNCTR, *6^{ème} rapport annuel (2021)*, p. 40.

⁴ Voir à ce sujet et C. Malverti et C. Beauflis, *L'instinct de conservation*, AJDA, 2021, p. 1194.

⁵ Voir à ce sujet G. Sutter, *Utilité et limites des objectifs de valeur constitutionnelle sur le plan contentieux*, Titre VII [en ligne], n° 8, Les catégories de normes constitutionnelles, avril 2022. URL complète : <https://www.conseil-constitutionnel.fr/publications/titre-vii/utilite-et-limites-des-objectifs-de-valeur-constitutionnelle-sur-le-plan-contentieux>.

également des objectifs de valeur constitutionnelle invoqués en défense par les pouvoirs publics dans son contrôle de constitutionnalité pour limiter l'application du droit de l'Union européenne¹.

Pour autant, cette protection constitutionnelle de la sécurité, mise en avant par la haute juridiction administrative comme étant spécifique à l'Etat français à l'issue de son contrôle de l'équivalence des protections, n'a pas manqué de surprendre les commentateurs. Certains ont vu dans la décision du 21 avril 2021 une résolution du conflit de normes plus soucieuse des besoins de l'administration profitant à la sécurité plutôt qu'à la protection des libertés individuelles et à la protection des données personnelles². On relèvera toutefois que la sécurité tend à s'affirmer en droit constitutionnel³, notamment à travers les objectifs de valeur constitutionnelle mobilisés par le Conseil d'Etat qui ont été d'ailleurs, soulignons-le, réaffirmés par le Conseil constitutionnel par la suite⁴. Là encore, il nous semble cohérent que les objectifs de valeur constitutionnelle de sécurité puissent alors constituer un fondement juridique pour limiter l'application du droit de l'Union européenne dans le cadre d'un contrôle de constitutionnalité dans le cas de figure de l'arrêt *French Data Network e.a.*. A cet égard, ces considérations tendent à démontrer que le droit du renseignement n'évoluerait plus seulement dans le cadre d'une limitation classique des droits fondamentaux mais aussi dans une articulation horizontale des normes relatives à la vie privée et à la sécurité⁵.

Toutefois, il est vrai que l'affirmation du Conseil d'Etat selon laquelle les « exigences constitutionnelles de sécurité » ne sont pas protégées de manière

¹ Dans le même sens, voir aussi B. Bertrand et J. Sirinelli, *Le Conseil d'Etat et la conservation des données de connexion : la quadrature du cercle*, op. cit..

² Sur la critique du souci prépondérant des besoins de l'administration, voir à ce sujet L. Azoulais et D. Ritleng, *L'Etat, c'est moi. Le Conseil d'Etat, la sécurité et la conservation des données*, op. cit..

Sur les critiques entre libertés et sécurité, voir notamment E. Dubout, *Le Conseil d'Etat, gardien de la sécurité*, RDLF, 2021, chron. n° 18 ; T. Douville et H. Gaudin, *Un arrêt sous le signe de l'exceptionnel*, Recueil Dalloz, 2021, p. 1268 ; et, P. Cassia, *Le Frexit sécuritaire du Conseil d'Etat*, billet de blog, Le Club Mediapart, 23 avril 2021.

³ A ce sujet, voir A. Vidal Naquet, *La sécurité en droit constitutionnel : non-dit ou non-être ?*, *La sécurité en droit public*, Institut Universitaire Varenne, Colloques & Essais, 2018.

⁴ Le Conseil constitutionnel a tenu à rappeler que le législateur doit assurer la conciliation entre les OVC de sécurité et le droit au respect à la vie privée dans ses décisions n° 2021-822 DC du 30 juillet 2021, *Loi relative à la prévention d'actes de terrorisme et au renseignement* et n° 2021-976/977 QPC du 25 février 2022, *M. Habib A et autre*.

⁵ En ce sens, voir également B. Bertrand et J. Sirinelli, *Le Conseil d'Etat et la conservation des données de connexion : la quadrature du cercle*, op. cit..

équivalente en droit de l'Union européenne peut sembler curieuse dès lors que les juges du Palais Royal ont reconnu que les textes de l'Union européenne et la jurisprudence de la Cour de Luxembourg prennent en considération ces exigences (considérant 10 de l'arrêt). Sur ce point, la doctrine s'accorde à dire que cette solution retenue par le juge administratif s'expliquerait par le fait que la sécurité a été définie comme une fonction essentielle des Etats membres que seuls ces derniers sont en mesure de garantir, sauf à réviser les traités constitutifs de l'Union¹. La méfiance à l'égard de l'Union et de sa juridiction trouve son origine dans le droit primaire de l'Union européenne.

Par conséquent, il semblerait que l'application de la « clause de sauvegarde Arcelor » dans les domaines de la sécurité consacre « *le principe d'un contrôle systématique sur les obligations issues du droit dérivé et de la jurisprudence de la Cour de justice en ce domaine* » selon les Professeurs Brunessen Bertrand et Jean Sirinelli, qui y voient alors une certaine limitation des effets du refus du contrôle *ultra vires* puisque la « clause de sauvegarde » réintroduit, en l'espèce, la question de la compétence de l'Union européenne². Tantôt qualifié de « Arcelor inversé »³, de « réserve Arcelor » ayant été étendue ou détournée⁴ ou encore de « clause dérogatoire »⁵, ce contrôle de « constitutionnalité du droit de l'Union européenne » introduit par l'arrêt *French Data Network e.a.* « cultive le flou » comme le remarquent très justement les Professeurs Loïc Azoulai et Dominique Ritleng⁶. Certes, on peut toujours soutenir que le contrôle *ultra vires* aurait été

¹ Voir en ce sens L. Azoulais et D. Ritleng, *L'Etat, c'est moi. Le Conseil d'Etat, la sécurité et la conservation des données*, op. cit. ; A. Iliopoulou-Penot, *La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué*, La Semaine Juridique Edition Générale n° 24, 14 juin 2021, 659 ; T. Douville et H. Gaudin, *Un arrêt sous le signe de l'exceptionnel*, op. cit. ; B. Bertrand et J. Sirinelli, *Le Conseil d'Etat et la conservation des données de connexion : la quadrature du cercle*, op. cit. ; C. Malverti et C. Beaufils, *L'instinct de conservation*, op. cit..

² Cf. B. Bertrand et J. Sirinelli, *Le Conseil d'Etat et la conservation des données de connexion : la quadrature du cercle*, op. cit..

³ Sur ce point, voir C. Malverti et C. Beaufils, *L'instinct de conservation*, op. cit..

⁴ Cf. L. Azoulais et D. Ritleng, *L'Etat, c'est moi. Le Conseil d'Etat, la sécurité et la conservation des données*, op. cit. et A. Iliopoulou-Penot, *La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué*, op. cit..

⁵ Voir en ce sens T. Douville et H. Gaudin, *Un arrêt sous le signe de l'exceptionnel*, op. cit..

⁶ Cf. L. Azoulais et D. Ritleng, *L'Etat, c'est moi. Le Conseil d'Etat, la sécurité et la conservation des données*, op. cit..

préférable pour sa clarté¹. Mais dans le même sens que les Professeurs Loïc Azoulai et Dominique Ritleng, nous nous inclinons devant l'ambiguïté du raisonnement des juges du Palais Royal qui ont fait preuve de « diplomatie judiciaire » et évité une « guerre des juges »² en appliquant *in fine* la jurisprudence de la CJUE.

Il reste que Le Conseil d'Etat a développé un « outil d'exception »³ afin de faire respecter la primauté du droit de l'Union européenne tout en permettant à l'Etat de défendre ses intérêts sans toutefois parvenir à satisfaire pleinement les observateurs sur l'articulation entre l'ordre juridique de l'Union européenne et l'ordre juridique national⁴. Pour notre part, nous pensons que la clé de lecture de la jurisprudence *French Data Network e.a.* réside dans la bienveillance entre les ordres de juridiction. En effet, il semble que le juge administratif ait retenu une application bienveillante de la jurisprudence *La Quadrature du Net e.a.* de la CJUE au cadre juridique national des services de renseignement pour conclure à son applicabilité⁵. A la lumière de ces considérations, on peut raisonnablement comprendre que la haute juridiction administrative n'ait pas souhaité s'engager sur la voie de l'*ultra vires*, qui sanctionne l'abus de compétence, et qu'elle ait admis que l'Etat puisse disposer d'un moyen de défense contre les risques d'abus de cette bienveillance. Pour ce qui concerne les motivations du Conseil d'Etat sur la compétence de l'Union européenne, elles n'ont de sens que pour répondre à la sensibilité des domaines en cause dans l'affaire jugée le 21 avril 2021.

Cette résolution du conflit de normes nous conduit donc à devoir analyser les garanties dégagées par la Cour de Luxembourg en matière de surveillance numérique avant d'étudier leurs conséquences sur le cadre juridique du renseignement français.

¹ En ce sens, voir E. Dubout, *Le Conseil d'Etat, gardien de la sécurité*, op. cit..

² Sur ce point, voir M. -C. de Montecler, *Conservation des données : la guerre des juges n'aura pas lieu*, AJDA 2021, p.828.

³ Sur cette formulation, voir l'audition de M. Bertrand Dacosta, président de la Xe chambre de la section du contentieux du Conseil d'Etat, devant la commission des affaires européennes, le jeudi 10 juin 2021 (Audition « *Pouvoir régalien et droit européen* »).

⁴ Voir en ce sens D. Simon, *Retour des monologues juridictionnels croisés ? À propos de l'arrêt du Conseil d'Etat dans l'affaire « French Data »*, Europe n° 6, Juin 2021, étude 3.

⁵ Sur ce constat, voir CNCTR, *6^{ème} rapport annuel (2021)*, p. 41 et C. Malverti et C. Beauvils, *L'instinct de conservation*, op. cit..

§2. Les « garanties essentielles européennes » dégagées par la Cour de justice de l'Union européenne

A partir du principe d'interdiction de conservation généralisée et indifférenciée des données personnelles par les opérateurs du numérique consacré dans l'arrêt *Digital Rights Ireland et Seitlinger e.a.* du 8 avril 2014, les décisions successives de la Cour de justice ont défini en droit de l'Union européenne les limites de la surveillance numérique que les autorités publiques européennes mais aussi étrangères sont tenues de respecter¹.

On regroupera et analysera ces limites dans les quatre « garanties essentielles européennes » identifiées par le Comité européen de la protection des données (CEPD) dans ses recommandations relatives aux mesures de surveillance² : un encadrement par des règles claires et précises ; le respect des principes de nécessité et de proportionnalité ; un contrôle indépendant ; des voies de recours effectives.

A - Des règles claires et précises

Les articles 8§2 et 52§1 de la Charte exigent textuellement que les ingérences dans la vie privée et le traitement de données personnelles soient prévus par la loi.

« Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi »³.

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui »⁴.

¹ En ce sens, voir B. Bertrand, *Chronique Droit européen du numérique - Les enjeux de la surveillance numérique*, RTD Eur. 2021, p.175.

² Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance adoptées le 10 novembre 2020.

³ Article 8§2 de la Charte des droits fondamentaux de l'Union européenne.

⁴ Article 52§1 de la Charte des droits fondamentaux de l'Union européenne.

En matière de surveillance numérique, la Cour de justice ne manque pas de rappeler constamment cette exigence textuelle dans ses décisions. On relèvera plus particulièrement deux précisions apportées par la Cour sur la définition de la « loi » : d'une part, la CJUE a considéré que la « loi » ne se limite pas aux seuls actes du Parlement au sens du droit de l'Union européenne en utilisant le terme « réglementation » dans l'affaire *La Quadrature du Net e.a.* ; et, d'autre part, la « loi » renvoie, selon la Cour, aux règles contraignantes en droit interne¹, c'est-à-dire par exemple des règles qui consacrent des « droits effectifs et opposables » devant les tribunaux². L'invocabilité devant les tribunaux de la réglementation constitue d'ailleurs un critère d'appréciation de la conformité au droit de l'Union européenne du droit interne des pays tiers pour la Cour. Dans l'affaire *Schrems 2*, les juges de Luxembourg ont ainsi écarté une directive présidentielle, la « PPD-28 », encadrant les programmes de surveillance américains au motif que le texte n'était pas invocable devant les tribunaux et seulement applicable pour les services de renseignement³.

En outre, la CJUE a adopté une approche analogue à la CEDH dans l'affaire *Digital Rights Ireland* (point 54) en considérant que la réglementation de l'Union européenne en matière de surveillance numérique doit « prévoir des règles claires et précises »⁴. Ces considérations ont été étendues aux réglementations nationales des Etats membres depuis l'affaire *Tele2 Sverige* et des pays tiers depuis l'affaire *Schrems 1*. La généralité des termes de l'accord PNR UE-Canada ont ainsi conduit la Cour à conclure sur son invalidité dans son *avis 1/15* du 26 juillet 2017⁵. Plus concrètement, la clarté et la précision des règles impliquent, selon la jurisprudence constante de la CJUE, de définir la portée de l'ingérence dans la vie privée

¹ Voir les affaires *Privacy International*, point 68 et *La Quadrature du Net e.a.*, point 132.

² Voir l'affaire *Schrems 2*, point 181.

³ A ce sujet, voir notamment D. Simon, *Coup de tonnerre dans le monde du numérique. La Cour de justice prononce l'invalidité du « bouclier de protection de la vie privée » à propos des transferts de données personnelles vers les États-Unis*, op. cit..

⁴ Sur le rapport entre CJUE et CEDH, voir notamment A. Danis-Fatôme, *Dispositif de surveillance des personnes versus droit à la protection des données à caractère personnel*, Communication Commerce électronique n° 7-8, juillet 2022, comm. 52.

⁵ Sur ce point, voir N. Le Bonniec, *L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne : une délicate conciliation entre sécurité nationale et sécurité numérique*, RTD Eur. 2018, p.617.

numérique des individus, ce qui doit permettre de guider les personnes concernées dans l'application de la réglementation.

A titre d'exemple, la Cour a considéré que, dans le cadre de la directive PNR, « les États membres doivent prévoir des règles claires et précises de nature à guider et à encadrer l'analyse effectuée par les agents en charge du réexamen individuel, aux fins d'assurer le plein respect des droits fondamentaux consacrés aux articles 7, 8 et 21 de la Charte et, notamment, de garantir une pratique administrative cohérente au sein de l'UIP respectant le principe de non-discrimination »¹.

D'une certaine manière, on retrouve l'exigence de prévisibilité de la loi dégagée par la CEDH². Dans les décisions de la CJUE qui concernent directement les services de renseignement telles que l'arrêt *La Quadrature du Net e.a.*, cette prévisibilité est implicitement affirmée par l'obligation d'édicter dans la réglementation nationale des conditions matérielles et procédurales ainsi que des garanties effectives contre les risques d'abus. En réalité, les juges de Luxembourg confondent cette exigence avec le respect des principes de nécessité et de proportionnalité³, ce qui nous amène à étudier ces derniers.

B - La nécessité et la proportionnalité

En application de l'article 52§1 de la Charte, la CJUE exige, dans un premier temps, que les mesures de surveillance numérique respectent le contenu essentiel du droit à la vie privée et de la protection des données personnelles, la Cour opérant, ici, des distinctions dans la gravité des interceptions des communications et des accès aux données de connexion. Dans un deuxième temps, la Cour de Luxembourg veille à ce que soient démontrées la nécessité et la proportionnalité des mesures de surveillance au regard d'objectifs légitimes. A cet égard, le juge de l'Union a été sensible à l'importance que revêt l'objectif de sécurité nationale pour les Etats membres. En outre, la Cour a été amenée à définir des garanties spécifiques à l'utilisation d'algorithmes de surveillance. Sur la nécessité, la jurisprudence de la CJUE considère que cette condition est remplie lorsque les

¹ Voir l'affaire *Ligue des droits humains*, point 205.

² Cf. supra. §1 de la Section 1 du Chapitre 1 du Titre 1 de la Seconde Partie.

³ Pour illustrer cette confusion entre l'exigence de prévisibilité de la loi et le respect du principe de proportionnalité, voir notamment le point 132 de la décision *La Quadrature du Net e.a.*.

mesures se fondent sur des critères objectifs pour caractériser leur stricte nécessité.

1. Le respect du contenu essentiel du droit à la vie privée numérique et les techniques de renseignement

Particularisme du droit de l'Union européenne, la notion de respect du contenu essentiel du droit signifie que les larges limitations vidant un droit fondamental de son contenu essentiel ne peuvent trouver aucune justification, c'est-à-dire qu'elles seront systématiquement considérées comme illicites par le juge de l'Union européenne, sans qu'il ait besoin d'apprécier leur nécessité et leur proportionnalité¹. Même s'il est possible d'identifier plus précisément les contours de cette notion de contenu essentiel, cette notion reste difficile à cerner et semble être appliquée dans une logique de cas par cas par la Cour de Luxembourg². En matière de surveillance numérique et de vie privée et protection des données personnelles, la Cour de justice a considéré dans ses arrêts *Digital Rights Ireland* *Seitlinger e.a.* et *Schrems 1* qu'une réglementation permettant d'accéder de manière généralisée et indifférenciée au contenu de communications électroniques constitue une atteinte au contenu essentiel des droits concernés à la différence des mesures visant les données de connexion conservées par les opérateurs du numérique. D'une part, les juges de Luxembourg ont retenu le critère d'une mesure trop générale et indifférenciée qui est habituellement retenu par la Cour pour caractériser une violation du contenu essentiel d'un droit ; et, d'autre part, ils ont ajouté une appréciation supplémentaire propre au respect du droit à la vie privée numérique en distinguant les interceptions des communications des accès aux données de connexion³. D'une certaine manière, on retrouve cette solution en droit du renseignement français dans la distinction entre les régimes des interceptions de sécurité et des accès aux données de connexion.

¹ Sur cette notion, voir notamment Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données*, op. cit., p. 49.

² Voir à ce sujet R. Tinière, *Le contenu essentiel des droits fondamentaux dans la jurisprudence de la Cour de justice de l'Union européenne*, Cahiers de droit européen- CDE, Bruxelles : Larcier, 2020, pp.417.

³ Sur le contrôle du contenu essentiel du droit à la vie privée et de la protection des données personnelles, voir notamment R. Tinière, *Le contenu essentiel des droits fondamentaux dans la jurisprudence de la Cour de justice de l'Union européenne*, op. cit., pp.417.

Pour le moment, seules les mesures de surveillance américaines sur les communications électroniques ont été considérées par la Cour comme portant une atteinte au contenu essentiel du droit à la vie privée numérique¹. En ce qui concerne les données de connexion conservées par les opérateurs du numérique et les systèmes PNR², l'absence d'atteinte au contenu essentiel des droits concernés implique tout de même, selon la jurisprudence de la Cour, d'apprécier la gravité des mesures de surveillance pour en déterminer leur proportionnalité et leur nécessité³. Là encore, la Cour de justice opère une autre distinction entre, d'une part, les données relatives à l'identité des abonnés des opérateurs et à leurs numéros téléphoniques et, d'autre part, les données relatives au trafic et à la géolocalisation des abonnés ainsi que les données PNR. Pour les premières, la CJUE considère que leur traitement ne constitue pas une ingérence grave⁴, alors que pour les secondes, elle qualifie leur traitement d'ingérence « particulièrement grave », notamment lorsque ces données sont traitées en temps réel ou font l'objet d'une technique algorithmique⁵. De même que pour la distinction opérée entre les ingérences dans les communications et les données de connexion, les juges de Luxembourg s'accordent à nouveau avec les distinctions opérées entre les différents types d'accès aux données de connexion en droit du renseignement français :

- d'une part, La CJUE adopte la même approche que l'article L. 851-1 du code de la sécurité intérieure relatif aux accès aux données en temps différé et que la doctrine de la CNCTR qui considère que les demandes d'identification d'abonnés ou de recensement de numéros d'abonnement sont des mesures préparatoires faiblement intrusives dont le contrôle est réduit à celui de « l'erreur manifeste d'appréciation », sauf lorsque ces

¹ Cf. Affaire *Schrems 1*.

² Cf. Affaire *Ligue des droits humains*, points 119 et 120.

³ Cf. Affaires *Ministerio Fiscal*, points 55 et suivants et *La Quadrature du Net e.a.*, point 131. Ces considérations n'ont pas manqué d'être rappelées par la CNCTR, « en l'absence d'atteinte au « contenu essentiel » d'un droit, la CJUE poursuit son examen de la limitation apportée à ce droit, en qualifiant son degré de gravité » (cf. CNCTR, 3^{ème} rapport annuel (2018), p. 113 à 117).

⁴ Cf. Affaire *Ministerio Fiscal*, points 59 à 61.

⁵ Cf. Affaires *La Quadrature du Net e.a.*, points 177 et 187 et *Ligue des droits humains*, point 111.

mesures concernant des personnes protégées par la loi en raison de leur activité¹ ;

- d'autre part, la Cour considère également les accès en temps réel comme des mesures plus intrusives que ceux en temps différé à l'instar des régimes prévus aux articles L. 851-1 et L. 851-2 du code de la sécurité intérieure.

Une fois que la gravité de l'ingérence est qualifiée, le droit de l'Union européenne s'attache à déterminer l'objectif d'intérêt général légitime qui correspond à cette qualification pour apprécier la proportionnalité des mesures de surveillance². A ce sujet, la Cour de Luxembourg a nuancé sa jurisprudence en tenant compte de l'objectif de sécurité nationale justifiant les activités des services de renseignement.

2. La proportionnalité et la sécurité nationale

Alors que la CJUE ne s'est pas attardée sur l'objectif de sécurité nationale justifiant les mesures de surveillance numérique des autorités publiques étrangères³, elle a été cependant amenée à clarifier sa position lorsque cet objectif est invoqué par les Etats membres pour justifier leurs techniques de renseignement. En effet, la Cour de Luxembourg avait uniquement pris en compte que les objectifs de lutte contre la criminalité grave et la sécurité publique dans ses arrêts *Digital Rights Ireland* et *Tele2 Sverige* pour conclure à l'interdiction de la conservation généralisée et indifférenciée des données. Finalement, la CJUE s'est efforcée d'adapter sa jurisprudence dans sa décision *La Quadrature du Net e.a.* du 6 octobre 2020 à la suite des questions préjudicielles des juridictions nationales sur la possibilité de justifier les mesures de surveillance sur le fondement du droit à la sûreté garanti par l'article 6 de la Charte et sur les exigences de la sécurité nationale, notamment pour justifier la conservation des données considérée comme présentant « une utilité sans équivalent »⁴.

¹ Cf. CNCTR, 3ème rapport annuel (2018), p. 46 à 49.

² Cf. Affaires *Ministerio Fiscal*, points 55 et suivants et *La Quadrature du Net e.a.*, point 131.

³ Dans l'affaire *Schrems 2*, la Cour a bien relevé que les mesures de surveillance américaines étaient justifiées par des exigences de sécurité nationale reconnues par la Commission européenne dans la décision d'adéquation litigieuse sans pour autant avoir eu besoin de les apprécier en raison des manquements constatés portant sur la clarté et la précision de la réglementation américaine et sur l'absence de voies de recours effectives.

⁴ CE, 26 juillet 2018, requête n° 393099.

Tout d'abord, les juges de Luxembourg ont écarté l'interprétation selon laquelle le droit à la sûreté garanti par la Charte pourrait fonder des mesures de surveillance¹, les dispositions de l'article 6 ne concernant que les mesures de privation de liberté au sens de l'article 5 de la Conv. EDH tel qu'interprété par la jurisprudence de la CEDH. Le juge de l'Union européenne met fin à une ambiguïté sur l'existence d'un droit à la sécurité dans le droit à la sûreté qui avait été relevée dans le point 42 de l'arrêt *Digital Rights Ireland*² :

« Il ressort de la jurisprudence de la Cour que constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales (voir, en ce sens, arrêts Kadi et Al Barakaat International Foundation/Conseil et Commission, C-402/05 P et C-415/05 P, EU:C:2008:461, point 363, ainsi que Al-Aqsa/Conseil, C-539/10 P et C-550/10 P, EU:C:2012:711, point 130). Il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique (voir, en ce sens, arrêt Tsakouridis, C-145/09, EU:C:2010:708, points 46 et 47). Par ailleurs, il convient de relever, à cet égard, que l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté ».

Cette ambiguïté est d'autant plus levée que la Cour de justice a ensuite admis dans sa décision du 6 octobre 2020 que l'objectif de sauvegarde de la sécurité nationale devait être spécifiquement reconnu pour fonder des mesures de surveillance numérique des services de renseignement des Etats membres. A ce titre, la Cour n'a pas manqué de proposer une définition de la sécurité nationale afin de faire ressortir l'importance de cet objectif :

« À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque Etat membre. Cette responsabilité correspond à l'intérêt primordial

¹ Voir l'arrêt du 6 octobre 2020, point 125.

² Sur le rapport entre droit à la sûreté et sécurité, voir notamment L. Azoulai et D. Ritleng, « L'État, c'est moi ». *Le Conseil d'État, la sécurité et la conservation des données*, op. cit. ; C. de Terwangne, *L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt La Quadrature du Net de la Cour de justice de l'Union européenne*, *Revue trimestrielle des droits de l'Homme*, vol. 129, no. 1, 2022, pp. 3-27 ; C. Grossholz, *L'avenir incertain d'un instrument de lutte contre le terrorisme : l'exploitation des données de connexion*, *La Semaine Juridique Administrations et Collectivités territoriales* n° 27, 10 juillet 2017, 2177.

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 »¹.

A partir de cette définition, la CJUE considère alors que l'objectif de sécurité nationale peut justifier des ingérences graves dans les droits fondamentaux en raison de son importance qui dépasse les autres objectifs de lutte contre la criminalité grave ou générale et de sécurité publique, notamment permettre de déroger à l'interdiction de conservation généralisée et indifférenciée des données². Dans le même sens et de manière plus spécifique, la Cour juge que la lutte contre le terrorisme, qui entre dans la définition de l'objectif de sécurité nationale, justifie l'accès en temps réel aux données connexion³ (arrêt du 6 octobre 2020, points 183 à 189) ainsi que l'extension de l'application de la directive PNR par les Etats membres à tous les vols intra-UE en provenance ou à destination de leur territoire (affaire *Ligue des droits humains*, points 170 et 171). Si pour certains, il a pu être regretté un manque de précisions sur les activités susceptibles de présenter une menace pour la sécurité nationale dans les motivations de la Cour⁴, on peut également s'interroger sur la portée juridique de la définition retenue par le juge de l'Union européenne. A notre sens, il n'était pas préférable de préciser davantage ce que recouvre l'objectif de sécurité nationale, l'intérêt de la définition étant de faire ressortir l'importance de cet objectif d'intérêt général par rapport aux autres objectifs pour prendre en considération les activités des services de renseignement et les ingérences qu'elles impliquent. De ce fait, la définition établie par la Cour ne semble pas avoir vocation à se substituer à celles retenues par les Etats membres même si elle peut s'avérer utile comme point de départ à une définition en droit interne.

¹ Cf. Affaire *La Quadrature du Net e.a.*, point 135.

² CJUE, 6 octobre 2020, points 136 et 137.

³ CJUE, 6 octobre 2020, points 183 à 189.

⁴ Sur le manque de précisions sur la sécurité nationale, voir notamment C. de Terwangne, *L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt La Quadrature du Net de la Cour de justice de l'Union européenne*, op. cit..

En conséquence, l'arrêt *La Quadrature du Net e.a.* esquisse un « tableau de concordance » de la surveillance numérique hiérarchiquement organisé entre les différents niveaux de gravité des ingérences dans la vie privée numérique et les différents objectifs d'intérêt général¹. Au sommet, on retrouve l'objectif de sécurité nationale justifiant les mesures les plus graves comme nous l'avons exposé précédemment.

Ensuite, on relèvera que les autres concordances s'inscrivent dans la ligne jurisprudentielle des arrêts *Digital Rights Ireland* et *Tele2 Sverige*². Tout en confirmant à nouveau dans son arrêt *Commissioner of An Garda Síochána* du 5 avril 2022 que les objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique sont hiérarchiquement inférieures à l'objectif de sécurité nationale³, la CJUE estime que ces objectifs ne peuvent justifier que :

« -une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;

-une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;

-une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour

¹ Sur le tableau de concordance, voir notamment CNCTR, *6^{ème} rapport annuel (2021)*, p. 37 à 39 ; P. Bonneville, C. Gänser, S. Markarian et A. Iljic, *Chronique de jurisprudence de la CJUE*, AJDA 2021, p. 387 ; C. Malverti et C. Beauvils, *L'instinct de conservation*, op. cit. ; A. Deroudille, *L'exploitation généralisée et indifférenciée des données de connexion en question*, Revue de l'Union européenne, 2022, p.332.

² En ce sens, voir notamment B. Bertrand, *Chronique Droit européen du numérique - Les enjeux de la surveillance numérique*, op. cit..

³ En ce sens, voir F. Viangalli, *De la conservation des données de communication électronique aux fins de politique pénale ou de sécurité nationale au regard du droit européen*, Revue Lamy Droit de l'Immatériel, N° 192, 1er mai 2022.

une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services ».

S'agissant des simples objectifs de lutte contre la criminalité générale et de sécurité publique, ils ne peuvent, quant à eux, seulement justifier « *une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques* ». En outre, on soulignera que la Cour de justice fait application de l'adage « qui peut le plus, peut le moins ».

En ce qui concerne les accès aux données conservées, les règles précédentes impliquent qu'ils ne peuvent être justifiés que par l'objectif d'intérêt général justifiant la conservation des données concernées par la mesure de surveillance, la Cour précisant toutefois que l'accès à des données conservées pour la lutte contre la criminalité grave peut être justifié par l'objectif de sécurité nationale. Lorsque les données sont conservées conformément aux exigences de la CJUE, la législation nationale est donc libre de prévoir, dans le respect des « garanties essentielles européennes », que les accès aux données de connexion peuvent avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale¹.

Comme nous pouvons l'observer, la prise en compte de la sécurité nationale entraîne un véritable assouplissement de la jurisprudence de la CJUE, ce qui affirmerait alors que la vie privée numérique et l'interdiction de la surveillance de masse dans l'Union ne sont pas absolues contrairement à ce que pouvaient laisser penser les arrêts *Digital Rights Ireland* et *Tele2 Sverige*². Il convient cependant de souligner qu'il ne s'agit pas là d'un revirement jurisprudentiel puisque la Cour a répondu à une question nouvelle qui l'a conduit à ajouter une limitation supplémentaire au droit à la vie privée et à la protection des données correspondant à la prise en compte d'un nouvel objectif d'intérêt général³.

Si la bienveillance de la CJUE à l'égard des services de renseignement peut être ainsi constatée, il reste que la Cour a tenu à ce que ses concessions en matière

¹ CJUE, 6 octobre 2020, points 166 et 167.

² En ce sens, voir également B. Bertrand, *Chronique Droit européen du numérique - Les enjeux de la surveillance numérique*, op. cit. et L. Azoulai et D. Ritleng, « *L'État, c'est moi* ». *Le Conseil d'État, la sécurité et la conservation des données*, op. cit..

³ Dans le même sens, voir par exemple C. Maubernard, *Droits fondamentaux*, in *Annuaire de droit de l'Union européenne*, 2021, p. 403 à 461.

de sécurité nationale n'aboutissent pas à une surveillance de masse aveugle en rappelant la nécessité de respecter certaines garanties. En ce qui concerne la conservation généralisée et indifférenciée des données de connexion, trois garanties cumulatives doivent être assurées en plus de répondre à un objectif de sécurité nationale : la menace doit être caractérisée comme « grave et actuelle ou prévisible » ; l'injonction de conservation doit faire l'objet d'un contrôle indépendant ayant un effet contraignant ; et, l'injonction doit être temporellement limitée au strict nécessaire mais renouvelable en cas de persistance de la menace¹. On retrouve également les mêmes garanties en matière de lutte contre le terrorisme pour autoriser l'extension de l'application de la directive PNR à tous les vols intra-UE en provenance ou à destination des États membres². Toujours en matière de lutte contre le terrorisme, la Cour a procédé à une adaptation desdites garanties au cas particulier du recueil des données en temps réel, jugé « particulièrement intrusif », en exigeant que l'autorisation, en plus d'être limitée au strict nécessaire et de faire l'objet d'un contrôle indépendant et contraignant, se limite seulement à des personnes soupçonnées d'être impliquées d'une manière ou d'une autre dans des activités de terrorisme³. L'ensemble de ces garanties renforcent le travail de qualification juridique de l'appréhension des menaces contre la sécurité nationale, notamment de la menace terroriste, et devraient tendre, plus globalement, à une plus grande ouverture et à une rationalisation des débats dans ce domaine comme à leur réactualisation régulière.

Dans le prolongement de ces considérations, une attention particulière doit être réservée à la reconnaissance par la CJUE de recourir à des algorithmes de surveillance dont l'encadrement constitue un nouvel enjeu du droit du numérique et de la surveillance de masse puisqu'il concerne le Big data avec l'utilisation de l'intelligence artificielle.

¹ Cf. Affaire *La Quadrature du Net e.a.*, points 134 à 139.

² Cf. Affaire *Ligue des droits humains*, points 171 et 172.

³ Cf. Affaire *La Quadrature du Net e.a.*, point 189.

3. Les garanties spécifiques à l'utilisation d'algorithmes de surveillance

Dès 2017, la Cour de justice de l'Union européenne s'est interrogée sur l'encadrement du recours à des systèmes d'analyses automatisées des données PNR en matière de sécurité et de renseignement anti-terroriste et de criminalité grave dans son *avis 1/15* sur l'accord PNR UE-Canada (points 168 à 174 de l'avis)¹. Pour que ces algorithmes de surveillance puissent être utilisés, la Cour a exigé le respect de certaines garanties propres aux enjeux de ces outils numériques, ils doivent donc :

- être fondés sur des « *modèles et des critères préétablis* » qui sont spécifiques et fiables pour identifier une cible pouvant être soupçonnée de participer à une activité terroriste ou de criminalité grave ainsi que non discriminatoires. Il est également exigé que les solutions algorithmiques comme les bases de données utilisées pour leur fonctionnement « *ne présentent pas un caractère discriminatoire et soient limités au strict nécessaire* », ce qui implique notamment de réexaminer régulièrement leur fiabilité et leur actualité ; et,
- ne pas être fondés sur des modèles et critères eux-mêmes fondés exclusivement sur des données personnelles sensibles.

En outre, tenant compte des risques de « faux positifs », la Cour exige que les résultats positifs obtenus par ces algorithmes doivent « *être soumis à réexamen individuel par des moyens non automatisés avant l'adoption d'une mesure individuelle produisant des effets préjudiciables* », c'est-à-dire que ces résultats doivent être appréciés au cas par cas par des personnes humaines.

Dans son arrêt *La Quadrature du Net e.a.* de 2020, la CJUE a repris ces garanties pour en faire application à la technique algorithmique de lutte contre le terrorisme de l'article L. 851-3 du code de la sécurité intérieure (points 172 à 182 de l'arrêt). Précisant que l'utilisation des algorithmes de surveillance sur l'ensemble des données de connexion des utilisateurs des opérateurs du numérique constitue une ingérence particulièrement grave dans le droit à la vie

¹ Sur la prise en compte des algorithmes par la CJUE, voir notamment M. Benlolo-Carabot, *Chronique Droit pénal de l'Union européenne - Protection des données personnelles, lutte contre le terrorisme : la CJUE confrontée à la surveillance de masse*, RTD Eur. 2017, p.884.

privée numérique garanti par la Charte, la Cour a considéré que cette utilisation ne peut avoir lieu que dans les conditions d'une menace grave pour la sécurité nationale. On remarquera que le juge de l'Union européenne semble admettre que la technique algorithmique de l'article L. 851-3 du code de la sécurité intérieure puisse être étendue à d'autres finalités de l'article L. 811-3 du même code. Aussi, on soulignera que la Cour a tenu à soumettre l'autorisation de mise en œuvre des algorithmes à un contrôle indépendant et contraignant.

Les juges de Luxembourg ont poursuivi leur cadrage juridique des algorithmes de surveillance dans la décision *Ligue des droits humains* du 21 juin 2022. Dans cette affaire, il a été précisé que les critères préétablis devant fonder les analyses automatisées s'opposent « à l'utilisation de technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage (*machine learning*), susceptibles de modifier, sans intervention et contrôle humains, le processus de l'évaluation et, en particulier, les critères d'évaluation sur lesquels se fonde le résultat de l'application de ce processus ainsi que la pondération de ces critères », cette solution ayant pour cause l'opacité du fonctionnement de certaines technologies d'IA (arrêt du 21 juin 2022, points 194 et 195)¹. Cependant, l'exclusion des algorithmes autoapprenant en matière de surveillance ne nous semble pas absolue selon les termes de la Cour, un modèle d'IA pouvant rester inchangé après la phase d'apprentissage devrait pouvoir être légalement autorisé². On soulignera que l'intervention humaine dans le traitement des résultats algorithmiques comme la compréhension par les autorités de contrôle ou les requérants des modèles d'IA utilisés ont été réaffirmées par le juge de l'Union européenne tant ces garanties présentent une importance pour « garder la main » sur l'IA et faire face aux risques de « faux positifs » et de discriminations³.

En revanche, selon Christophe Maubernard, ces garanties seraient plus performatives qu'effectives et accorderaient trop de confiance dans la capacité de

¹ Sur l'exclusion des technologies d'IA, voir notamment P. Bonneville, C. Gänser, S. Markarian et A. Iljic, *Chronique de jurisprudence de la CJUE*, op. cit. ; D. Simon, *Protection des données*, Europe n° 8-9, Août 2022, comm. 265.

² Voir en ce sens W. Maxwell, *La CJUE dessine le noyau dur d'une future régulation des algorithmes*, op. cit..

³ En ce sens, voir S. Hourson, « *Données passagers* » : le contrôle de la machine, op. cit..

l'humain pour appréhender les techniques algorithmiques¹. Dans le même sens, il devrait être difficile d'éviter effectivement tout « faux positifs » ou discriminations sans avoir véritablement éprouvé préalablement les algorithmes de surveillance et les capacités des personnes à traiter ou à contrôler ces derniers en toute objectivité². Ces considérations tendent à confirmer notre analyse selon laquelle l'IA en renseignement devrait bénéficier de deux régimes juridiques distincts, l'un en matière de recherche et l'autre en matière de surveillance, mais complémentaires³, notamment pour répondre aux exigences de la CJUE et débattre des niveaux d'erreurs et de biais acceptables pour déployer opérationnellement les algorithmes⁴.

Par ailleurs, l'arrêt du 21 juin 2022 apporte une précision sur les interconnexions utilisant un système d'alerte automatisé entre les fichiers de données PNR et d'autres fichiers : ces derniers doivent concerner des personnes ou des objets recherchés ou signalés ainsi qu'être en rapport avec la lutte contre le terrorisme et la criminalité grave tout en présentant un lien objectif ou indirect avec les transports aériens des passagers⁵. En droit interne, ces exigences européennes nous invitent à considérer que les interconnexions des fichiers de renseignement avec d'autres fichiers que ceux de la sécurité devraient, du moins, seulement concerner des fichiers ayant pour objet le signalement des personnes ou leur recherche susceptibles d'avoir un rapport avec les finalités de l'article L. 811-3 pour répondre aux inquiétudes qu'avaient suscité la mise en relation entre le FSPRT et HOPSYWEB⁶.

Enfin, la question de la portée des garanties spécifiques aux algorithmes dégagées par les arrêts de la CJUE a pu être posée, conduisant par exemple Winston Maxwell à soutenir que « *les principes issus de l'arrêt du 6 octobre 2020 de*

¹ Cf. C. Maubernard, *Données personnelles et sécurité nationale : Big Brother can watch everybody, Les juridictions de l'Union européenne et les droits fondamentaux*, Chronique de jurisprudence (2020), Revue trimestrielle des droits de l'Homme 2021/3 (N° 127), p. 573 à 620.

² En ce sens, voir W. Maxwell, *La CJUE dessine le noyau dur d'une future régulation des algorithmes*, op. cit..

³ Cf. supra. §1 de la Section II du Chapitre II du Titre I de la Ière Partie.

⁴ Sur le débat des niveaux d'erreurs et de biais acceptables, voir notamment W. Maxwell, *La CJUE dessine le noyau dur d'une future régulation des algorithmes*, op. cit..

⁵ Cf. Affaire *Ligue des droits humains*, points 182 à 192.

⁶ Cf. supra. §3 de la Section I du Chapitre II du Titre I de la Ière Partie.

la CJUE représentent selon nous une série de conditions incontournables d'une régulation des algorithmes conforme à la Charte » tout en reconnaissant cependant que « l'intensité d'application de chaque principe sera variable en fonction des risques associés au traitement particulier »¹. Pour notre part, il nous apparaît certain qu'il est désormais nécessaire de tenir compte de l'ensemble des exigences des trois décisions précitées (avis 1/15 et les affaires *La Quadrature du Net e.a.* et *Ligue des droits humains*) pour autoriser légalement tous nouveaux algorithmes de surveillance des personnes en matière de sécurité nationale. En dehors de cet objectif de sécurité, la Cour ne semble autoriser ces algorithmes que pour les besoins de la criminalité grave dans un secteur particulier comme les transports aériens des passagers. Dans les autres domaines que celui de la sécurité ou des enquêtes pénales, il est vraisemblable que les conditions de la CJUE puissent être généralisées lorsqu'il s'agit d'algorithmes opérationnels qui traitent des données personnelles non anonymisées. En revanche, on peut raisonnablement supposer qu'un assouplissement des exigences de la CJUE soit conforme à la Charte lorsque les technologies d'IA sont utilisées à des fins de recherche et de développement sur des données anonymisées ou sur des projets de recherche n'impliquant pas la personne humaine.

4. La stricte nécessité caractérisée par des critères objectifs

Il n'est pas toujours facile de décrypter les exigences du principe de nécessité dans la jurisprudence de la CJUE en matière de vie privée et de protection des données. Selon le CEPD, ce principe doit être généralement considéré comme autonome par rapport au principe de proportionnalité et examiné prioritairement². Alors que le principe de proportionnalité serait entendu, au sens strict, comme la mise en balance des avantages et des inconvénients d'un traitement de données, le principe de nécessité suppose « une évaluation factuelle combinée de l'efficacité de la mesure aux fins de l'objectif poursuivi et de déterminer

¹ Cf. W. Maxwell, *La CJUE dessine le noyau dur d'une future régulation des algorithmes*, op. cit..

² Cf. European Data Protection Supervisor, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017, p. 5 et 6.

si cette mesure est moins intrusive par rapport aux autres moyens de réaliser le même objectif »¹.

S'il est vrai que la Cour de justice a uniquement fait référence à la nécessité pour condamner des mesures de surveillance numérique², le CEPD concède que les deux principes se chevauchent en pratique, le principe de proportionnalité au sens strict pouvant être examiné en priorité par la CJUE comme dans l'affaire *Tele2 Sverige*³. A notre sens, la Cour semble adopter une conception large de la notion de proportionnalité en matière de surveillance dans laquelle serait incluse la nécessité⁴. Toutefois, la notion de nécessité demeure autonome en plus d'être considérée strictement par la CJUE. Cette stricte nécessité doit être démontrée par des critères objectifs⁵. Ces derniers visent à définir les conditions spécifiques auxquelles doit répondre une mesure de surveillance dans le cadre de son évaluation factuelle. Par exemple, il peut s'agir du caractère réel et actuel ou prévisible d'une menace pour la sécurité nationale, la limitation dans le temps des mesures de surveillance ou encore la limitation du recueil en temps réel des données aux seules personnes soupçonnées de présenter un lien avec une activité terroriste. On retrouve ainsi une position similaire à celle adoptée par la CEDH dans le cadre de son contrôle de proportionnalité et de nécessité des mesures de surveillance qui vise à apprécier objectivement lesdites mesures au regard des circonstances de l'affaire⁶. Cependant, l'exigence de stricte nécessité qui implique également un contrôle strict des mesures limite fortement le pouvoir d'appréciation du législateur dans le choix des techniques de surveillance⁷, la jurisprudence de la CJUE apparaissant, ici, plus sévère que celle de la CEDH.

¹ Cf. European Data Protection Supervisor, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017, p. 5 et 6.

² Cf. Affaires *Digital Rights Ireland*, points 56 à 69 et *Schrems 1*, points 92 et 93.

³ Ibid., p. 6.

⁴ Voir affaires *Digital Rights Ireland*, point 46 ; *Tele2 Sverige*, point 96 ; ou encore, *La Quadrature du Net e.a.*, point 132.

⁵ Voir affaires *Tele2 Sverige*, point 110 ; *La Quadrature du Net e.a.*, point 133 et *Privacy International*, point 78. Dans le même sens, voir les recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance du CEPD adoptées le 10 novembre 2020.

⁶ Cf. European Data Protection Supervisor, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, op. cit., p. 8.

⁷ Ibid., p. 7 et 8.

A propos du contrôle, la CEDH et la CJUE exigent toutes deux que les techniques de renseignement fassent l'objet d'un mécanisme de surveillance assuré par un juge ou une autorité indépendante.

C - Un contrôle indépendant

De manière tout à fait logique, la CJUE exige de subordonner les mesures de surveillance numérique à un contrôle indépendant en vertu de l'article 8§3 de la Charte qui consacre explicitement un tel contrôle¹. A la condition d'indépendance, la jurisprudence de la Cour ajoute deux autres conditions : un contrôle préalable à la mise en œuvre de la surveillance et, dans certains cas, un contrôle contraignant.

Également applicable aux pays tiers dans le cadre des transferts de données hors de l'Union européenne², l'exigence d'indépendance du contrôle peut être remplie soit par une juridiction soit par une entité administrative³. Pour ce qui concerne la notion d'indépendance, la Cour a d'abord jugé dans l'affaire *Schrems 2* (points 194 à 197) qu'un médiateur de la protection des données décrit comme indépendant des services de renseignement américains ne l'était pas dès lors que cette autorité est désignée et rattachée au gouvernement⁴. De même, la Cour considère dans son *avis 1/15* (point 230) qu'une autorité « *subordonnée à une autorité de tutelle, dont elle peut recevoir des instructions, et qui n'est donc pas à l'abri de toute influence extérieure susceptible d'orienter ses décisions* » n'est pas indépendante⁵. L'arrêt *Prokuratuur* du 2 mars 2021 (points 52 et 54) a ensuite clairement défini cette notion en matière de renseignement et d'enquêtes pénales en exigeant que l'autorité de contrôle dispose « *de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause* », c'est-à-dire qu'elle ait la qualité de tiers par rapport aux services de renseignement et de sécurité afin d'exercer un contrôle

¹ Voir affaire *Tele2 Sverige*, point 132.

² Cf. Affaire *Schrems 2*, point 188.

³ Cf. Affaire *Tele2 Sverige*, point 120.

⁴ A ce sujet, voir également F. Mattatia, *Données personnelles : la CJUE invalide le Privacy Shield*, op. cit. ; D. Simon, *Coup de tonnerre dans le monde du numérique. La Cour de justice prononce l'invalidité du « bouclier de protection de la vie privée » à propos des transferts de données personnelles vers les États-Unis*, op. cit. ; Y. Padova, *Le Safe Harbor est mort, vive le Privacy Shield ?*, Revue Lamy Droit de l'Immatériel, N° 127, 1er juin 2016.

⁵ Voir également V. Correia, *À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens*, op. cit..

« de manière objective et impartiale à l'abri de toute influence extérieure ». En particulier pour ce qui concerne une entité administrative, l'arrêt *Prokuratuur* juge qu'elle est indépendante lorsque l'entité jouit d'un statut garantissant son objectivité et son impartialité dans l'exercice de ses missions tout en étant à l'abri de toute influence extérieure (point 53), ce qui est le cas de la CNCTR en France qui bénéficie du statut d'autorité administrative indépendante. Ces considérations conduisent alors à sanctionner tout accès aux données conservées par les opérateurs du numérique par un fonctionnaire de police judiciaire sous son seul contrôle¹ et, a fortiori, par un fonctionnaire des services de renseignement dans les mêmes conditions.

En plus d'être indépendante, l'autorité de contrôle doit être en mesure d'exercer un contrôle préalable (ou *a priori*) des mesures de surveillance sur l'autorisation de leur mise en œuvre. Ce contrôle préalable concerne les systèmes PNR² et les accès aux données de connexion en temps différé et en temps réel³. On relèvera que la Cour semble opérer une distinction avec l'injonction de conservation des données qui n'apparaît pas devoir être obligatoirement soumise à un contrôle *a priori*⁴. En outre, on précisera que l'obligation de prévoir un contrôle préalable des accès aux données est entendue strictement par la CJUE qui refuse d'admettre qu'un tel accès puisse être autorisé dans le cadre d'un dispositif qui ne prévoit qu'un contrôle *a posteriori*⁵. En revanche, les juges de Luxembourg se sont montrés compréhensifs face aux réalités des opérations des forces de renseignement et de sécurité en consacrant une dérogation à l'exigence d'un contrôle préalable sous deux conditions : une « urgence dûment justifiée »⁶ et un « contrôle doit intervenir dans de brefs délais »⁷.

¹ Cf. Affaire *Commissioner of An Garda Síochána*, point 111.

² Avis 1/15, point 202 et affaire *Ligue des droits humains*, point 233.

³ Cf. Affaires *Tele2 Sverige*, point 120 ; *La Quadrature du Net e.a.*, point 189 ; *Prokuratuur*, point 51 ; *Commissioner of An Garda Síochána*, point 106.

⁴ Voir affaire *La Quadrature du Net e.a.*, point 139.

⁵ Voir Affaire *Commissioner of An Garda Síochána*, point 112. A ce sujet, voir également A. Danis-Fatôme, *Dispositif de surveillance des personnes versus droit à la protection des données à caractère personnel*, op. cit. et A. Deroudille, *L'exploitation généralisée et indifférenciée des données de connexion en question*, op. cit..

⁶ Cf. Affaire *Tele2 Sverige*, point 120.

⁷ Cf. Affaires *La Quadrature du Net e.a.*, point 189 ; *Prokuratuur*, point 51 et 58 ; *Commissioner of An Garda Síochána*, point 110. Sur la dérogation à un contrôle préalable, voir aussi A. Danis-Fatôme,

Enfin, le contrôle des mesures de surveillance exceptionnellement admises par la CJUE pour la sauvegarde de la sécurité nationale est soumis à une condition supplémentaire d'être doté d'un effet contraignant depuis l'arrêt *La Quadrature du Net e.a.* du 6 octobre 2020. Cette condition s'applique :

- à l'injonction de conservation généralisée et indifférenciée des données de connexion¹. On notera qu'un contrôle contraignant est également requis sur l'extension de l'application de la directive PNR à l'ensemble des vols intra-UE pour la prévention du terrorisme² ;
- aux techniques algorithmiques de surveillance telles que celles prévue à l'article L. 851-3 du code de la sécurité intérieure³ ;
- aux accès en temps réel aux données de connexion dont le contrôle vise notamment à « *s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire* »⁴.

On ne manquera pas de saluer l'application de cette dernière condition aux activités des services de renseignement qui, rappelons-le, concernent la surveillance d'Etat. Un contrôle contraignant dans ce domaine permet assurément de renforcer l'Etat de droit mais aussi le sens de la responsabilité des agents impliqués dans l'utilisation de techniques secrètes de renseignement. D'autant plus que le droit de l'Union européenne accorde une grande importance à l'existence d'une protection juridictionnelle effective en matière traitement de données personnelles.

Dispositif de surveillance des personnes versus droit à la protection des données à caractère personnel, op. cit..

¹ Cf. Arrêt du 6 octobre 2020, point 139 et l'affaire *Commissioner of An Garda Síochána*, point 58.

² Cf. Affaire *Ligue des droits humains*, point 172.

³ CJUE, 6 octobre 2020, point 179.

⁴ CJUE, 6 octobre 2020, point 189.

D - Des voies de recours effectives

Le droit à un recours juridictionnel effectif dans la protection des données personnelles constitue une garantie cruciale en droit de l'Union européenne, a fortiori lorsque ces données font l'objet de mesures de surveillance. En effet, la Cour de justice a considéré dans son arrêt *Schrems 1* du 6 octobre 2015 que :

« une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte. En effet, l'article 47, premier alinéa, de la Charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article. À cet égard, l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit » (point 95).

La nécessité de prévoir un recours juridictionnel effectif contre les mesures de surveillance afin de prévenir et sanctionner les abus des autorités publiques est constamment rappelée dans la jurisprudence de la CJUE. Hormis dans le cas de la réglementation américaine en matière de renseignement¹, l'exigence de voies de recours effectives n'a néanmoins pas suscité de difficultés dans les affaires présentées devant la Cour. En revanche, l'examen du droit à un recours juridictionnel a soulevé la question plus particulière de l'obligation de notification de la surveillance aux personnes concernées, ce qui n'a pas manqué de faire débat dans le cas de la réglementation française.

Dans son arrêt *Tele2 Sverige* du 21 décembre 2016 (point 121), la Cour de justice a estimé qu'il était nécessaire d'informer les personnes concernées par une autorisation d'accès à leurs données pour permettre l'exercice du droit à un recours effectif, sauf lorsque cette information est susceptible de compromettre les investigations des autorités. Cette solution a été réaffirmée dans *l'avis 1/15* de

¹ Cf. Affaire *Schrems 2*, point 197. Sur ce point, voir D. Simon, *Coup de tonnerre dans le monde du numérique, la Cour de justice prononce l'invalidité du « bouclier de protection de la vie privée » à propos des transferts de données personnelles vers les États-Unis*, op. cit..

la CJUE portant sur l'accord PNR UE-Canada (points 218 à 225)¹. On notera que la CNCTR a relevé que le mécanisme de notification avait été introduit dans les motivations de l'arrêt *Tele2 Sverige* et non dans son dispositif, ce qui laisserait entendre que ce mécanisme ne constitue pas pour la CJUE une condition autonome et indispensable de la légalité des mesures de surveillance². A cet égard, on rappellera que pour la CEDH, un mécanisme de notification est exigé que s'il constitue une procédure déterminante dans le droit à un recours effectif contre des mesures de surveillance³. Si certains Etats membres, tels que l'Allemagne, ont adopté ce type de mécanisme, la France a fait le choix de ne prévoir aucune procédure d'information en raison du fait que toute personne peut saisir la CNCTR et la formation spécialisée du Conseil d'Etat afin de vérifier la légalité des techniques de renseignement⁴. Pour autant, l'avocat général Manuel Campos Sanchez-Bordona en charge de l'affaire *La Quadrature du Net e.a.* a sévèrement considéré que l'accès aux données de connexion constitue un traitement de données personnelles qui doit être notifié à la personne concernée, estimant que le droit au recours effectif n'était plus garanti lorsque les personnes font réellement l'objet d'une surveillance, même si l'avocat général a reconnu qu'il n'y avait pas d'atteinte à ce droit, « *en théorie, pour ceux qui décident de vérifier s'ils font l'objet d'une opération de renseignement* »⁵. Finalement, la Cour de justice appliquera ses motivations de l'arrêt du 21 décembre 2016 dans son arrêt du 6 octobre 2020 aux mesures de surveillance litigieuses⁶, le mécanisme de notification ne figurant toujours pas dans le dispositif de cette dernière décision. A notre sens, les préoccupations de l'avocat général portaient davantage sur le souci d'une conformité exemplaire du droit français au droit de l'Union européenne plus que sur le souci de garantir le droit à un recours effectif aux individus. La position inchangée de la CJUE sur cette question nous semble alors

¹ A ce sujet, voir V. Correia, *À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens*, op. cit.

² Cf. CNCTR, 2^{ème} rapport annuel (2017), p. 77.

³ Cf. supra. Section I du Chapitre I du Titre I de la Seconde Partie.

⁴ Cf. CNCTR, 2^{ème} rapport annuel (2017), p. 74 à 86.

⁵ Cf. Conclusions de l'avocat général dans l'affaire *La Quadrature du Net e.a.*, 15 janvier 2020 (points 147 à 154).

⁶ Cf. Affaire *La Quadrature du Net e.a.*, points 190 à 192.

plus raisonnable, d'autant plus que l'obligation d'information n'est pas absolue selon l'article 14§5 du RGPD.

Dans le prolongement de ce droit à la transparence des mesures de surveillance, on remarquera que la Cour de justice s'est montrée soucieuse du risque d'opacité des algorithmes. Dans l'arrêt *La Quadrature du Net e.a.*, les juges de Luxembourg ont ainsi exigé que l'autorité chargée du contrôle d'une technique d'analyse automatisée des données soit « *tenue de publier des renseignements de nature générale relatifs à cette analyse, sans devoir procéder à une information individuelle des personnes concernées* »¹. A ce titre, on peut affirmer que le contrôle juridictionnel effectif des algorithmes de surveillance suppose « la transparence et l'explicabilité du modèle »². En effet, ces considérations sont clairement réaffirmées dans la décision *Ligue des droits humains* du 21 juin 2022 (point 210) dans laquelle la CJUE précise que les requérants comme le juge doivent être en mesure de comprendre le fonctionnement des algorithmes pour l'exercice du droit à un recours juridictionnel³.

Si la jurisprudence de la CJUE en matière de surveillance demeure récente et quantitativement encore limitée par rapport à celle de la CEDH, il n'en demeure pas moins que les juges de Luxembourg ont su rapidement bâtir, à leur tour, un socle de garanties essentielles dans le cadre des compétences de l'Union qui s'est adapté aux préoccupations des Etats membres, ainsi qu'à celles de leurs citoyens sur la circulation de leurs données en dehors de l'Union européenne. En conséquence, le droit du renseignement français a nécessairement dû s'adapter lui aussi aux exigences de l'Union.

¹ CJUE, 6 octobre 2020, point 191.

² Voir en ce sens W. Maxwell, *La CJUE dessine le noyau dur d'une future régulation des algorithmes*, op. cit..

³ A ce sujet, voir également P. Bonneville, C. Gänser et A. Iljic, *Chronique de jurisprudence de la CJUE*, op. cit..

§3. Une conformité « augmentée » du droit du renseignement

Assurant la conformité du droit du renseignement aux garanties essentielles européennes, l'arrêt *French Data Network e.a.* du 21 avril 2021 du Conseil d'Etat ainsi que la loi du 30 juillet 2021 relative au renseignement et au terrorisme et ses décrets d'application ont interprété plus largement la lettre des arrêts de la CJUE. Il en résulte alors un renforcement du droit du renseignement dans quatre domaines : les finalités du renseignement numérique ; la définition des données de connexion ; le contrôle du renseignement numérique ; et enfin, dans la relation que peut entretenir le cadre juridique du renseignement avec les enquêtes sur la criminalité grave et sur les atteintes graves à la sécurité publique.

A - Les finalités du renseignement numérique ou le « bloc de sécurité nationale »

De manière générale, la définition de la sécurité nationale en droit européen apparaît compatible avec la conception française de cette notion définie à l'article L. 1111-1 du code de la défense et les « intérêts fondamentaux de la Nation » mentionnés dans le code pénal¹. Plus particulièrement, le Conseil d'Etat a confirmé dans sa décision du 21 avril 2021 la correspondance entre les finalités du renseignement numérique prévues à l'article L. 811-3 du code de la sécurité intérieure et la sauvegarde de la sécurité nationale telle que définie par la CJUE. En effet, cette correspondance est relevée explicitement en ce qui concerne les techniques de renseignement (considérant 67) et implicitement en matière d'obligation de conservation généralisée et indifférenciée des données (considérant 43). Au regard de la position du juge administratif, les finalités du renseignement numérique constitueraient un « bloc de sécurité nationale » en considérant que la caractérisation d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale doit être « *appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3...* » (considérant 44).

La loi du 30 juillet 2021 semble avoir adopté cette idée d'un « bloc de sécurité nationale » en modifiant l'article L. 34-1 du code des postes et des

¹ A ce sujet, voir B. Warusfel, *Conservation des données et sécurité nationale au regard du droit de l'Union européenne*, op. cit.

communications électroniques de la façon suivante : « *pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic, en complément de celles mentionnées au 3° du II bis, et de données de localisation précisées par décret en Conseil d'Etat* ». Les décrets n° 2021-1363 du 20 octobre 2021 et n° 2022-1327 du 17 octobre 2022 portant injonction, au regard de la menace grave, réelle et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion nous confirment que la sécurité nationale constitue un bloc de finalités qui permettent de caractériser une seule et unique menace grave, réelle et actuelle ou prévisible.

Néanmoins, on relèvera qu'en pratique le Conseil d'Etat a procédé à l'examen du caractère grave, réelle et actuelle ou prévisible de plusieurs menaces correspondantes à différentes finalités en jugeant successivement que la France est confrontée à « *la persistance d'un risque terroriste élevé* », qu'elle est « *particulièrement exposée au risque d'espionnage et d'ingérence étrangère* » et qu'elle est « *également confrontée à des menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes* »¹. Une menace pour la sécurité nationale serait donc caractérisée lorsqu'une ou plusieurs menaces relatives aux finalités de l'article L. 811-3 du code de la sécurité intérieure seraient caractérisées comme grave, réelle et actuelle ou prévisible. On peut toutefois soulever deux questions de méthodes :

- la question de savoir si la caractérisation d'une menace relative à une seule finalité du renseignement peut caractériser une menace pour la sécurité nationale ; et,
- la question de savoir s'il peut être cumulées une menace caractérisée uniquement comme grave et réelle pour l'une des finalités de l'article L. 811-3 avec une menace caractérisée comme seulement actuelle ou prévisible pour une autre finalité afin de caractériser *in fine* une menace pour la sécurité nationale.

¹ CE, 21 avril 2021, considérant 44.

A notre sens, la décision du Conseil d'Etat et les nouveaux textes relatifs au renseignement admettraient les deux méthodes pour justifier l'invocation de l'objectif de sécurité nationale. Par ailleurs, on relèvera que la haute juridiction administrative a assuré la conformité de la technique algorithmique de l'article L. 851-3 du code de la sécurité intérieure de lutte contre le terrorisme à l'exigence de la CJUE de justification d'une menace pour la sécurité nationale en précisant que la CNCTR est chargée, dans le cadre de son contrôle *a priori*, de vérifier que la finalité invoquée pour recourir à cette technique « *repose sur des critères objectifs et non discriminatoire* » ainsi que « *l'existence et l'actualité de la menace grave pour la sécurité nationale susceptible de justifier une telle mesures* »¹. En conséquence, le « bloc de sécurité nationale » pourrait s'interpréter largement comme permettant l'utilisation d'une seule technique algorithmique pour l'ensemble des finalités du renseignement numérique mais aussi à des fins d'enquêtes judiciaires pour la répression des infractions d'atteinte aux intérêts fondamentaux de la Nation et de terrorisme. Dans ce cas, la réception de la jurisprudence de la CJUE en droit interne tendrait à faciliter la surveillance de masse plutôt que de la limiter.

Ces considérations nous invitent à soulever deux remarques sur la limitation en pratique des conséquences du « bloc de sécurité nationale ». D'une part, il serait plus souhaitable que l'examen cumulatif des critères de caractérisation d'une menace pour la sécurité nationale soit réalisé par le gouvernement sur chacune des finalités de l'article L. 811-3 du code de la sécurité intérieure lors du réexamen périodique de la nécessité de maintenir l'obligation de conservation des données de connexion exigée par le Conseil d'Etat² puis la loi du 30 juillet 2021. Il s'agit donc d'appliquer la méthode de caractérisation retenue par le juge administratif dans son arrêt *French Data Network e.a.*. D'autre part, cette même méthode devrait, selon nous, être appliquée par les services de renseignement dans leur demande et par la CNCTR dans son contrôle sur la technique algorithmique si cette dernière est étendue à l'ensemble des finalités de l'article L. 811-3 du code de la sécurité intérieure.

¹ CE, 21 avril 2021, considérant 77.

² CE, 21 avril 2021, considérants 45 et 46.

En outre, on fera remarquer qu'il pourrait être envisagé, selon nous, d'introduire plus largement les critères européens de caractérisation de la menace pour la sécurité nationale dans les demandes de techniques de renseignement afin notamment d'harmoniser et d'améliorer la qualité juridique de ces dernières. Autrement dit, chaque finalité invoquée pour justifier l'utilisation d'une technique de renseignement pourrait, en tenant compte du caractère opérationnel des demandes des services de renseignement, s'accompagner d'un examen du caractère grave et réelle, actuelle ou prévisible de la menace.

A ces remarques, on ajoutera que l'émergence d'un « bloc de sécurité nationale » correspondant aux finalités de l'article L. 811-3 du code de la sécurité intérieure pour justifier le recours à certaines mesures de surveillance a relancé le débat sur la délimitation des activités du renseignement d'Etat, certains commentateurs critiquant une interprétation large de l'objectif de sécurité nationale par le Conseil d'Etat¹ et d'autres relevant que cet objectif peut être facilement manipulé en droit interne pour justifier la surveillance². Pour notre part, on rappellera que la définition de la sécurité nationale retenue par la CJUE s'appuie sur des exemples révélant l'importance de cet objectif d'intérêt général, ce qui implique que les Etats membres sont chargés d'identifier les situations en droit interne qui peuvent correspondre aux exemples cités par la Cour. S'agissant des finalités de l'article L. 811-3 qui « *concourent à la défense des intérêts fondamentaux de la Nation* »³, leur correspondance avec la jurisprudence de la CJUE nous apparaît difficilement critiquable puisque cette dernière mentionne notamment « *l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société* »⁴.

Enfin, on ne manquera pas de relever deux critiques soulevées par les Professeurs Loïc Azoulai et Dominique Ritleng sur les finalités de l'article L. 811-3

¹ En ce sens, voir B. Bertrand et J. Sirinelli, *Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle*, op. cit..

² A ce sujet, voir A. Iliopoulou-Penot, *La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué*, op. cit..

³ CE, 21 avril 2021, considérant 67.

⁴ Cf. Affaire *La Quadrature du Net e.a.*, point 135.

et l'objectif de sécurité nationale¹. Tout d'abord, ils ont relevé que le Conseil d'Etat n'avait pas jugé contraire à l'arrêt *La Quadrature du Net e.a.* de la CJUE le fait de pouvoir recourir à la technique de géolocalisation en temps réel de l'article L. 851-4 du code de la sécurité intérieure pour l'ensemble des finalités de l'article L. 811-3 alors que le juge de l'Union européenne a circonscrit le recueil en temps réel de ces données à la seule finalité de prévention du terrorisme². Toutefois, il convient de préciser que le juge administratif a fondé sa décision sur la rédaction de l'article L. 851-4 qui prévoit, à la différence du recueil en temps réel prévu par l'article L. 851-2 du code de la sécurité intérieure, une sollicitation du réseau des opérateurs du numérique pour collecter les données concernées et que c'est la transmission de ces données qui est effectuée en temps réel. La nuance réside dans l'accès direct ou indirect aux données de géolocalisation sur le réseau des opérateurs du numérique, l'exigence européenne de limitation de la finalité ne visant que l'accès direct selon le Conseil d'Etat.

Ensuite, les Professeurs Loïc Azoulai et Dominique Ritleng considèrent que la solution retenue par le Conseil d'Etat laisse une place prédominante à la caractérisation d'une menace pour la sécurité nationale pour s'assurer de la légalité de l'obligation de conservation généralisée et indifférenciée des données, les Professeurs soulignant l'occultation des garanties posées par la Cour de justice permettant d'éviter les risques d'atteinte à la vie privée et aux données personnelles, autrement dit « *l'exigence de compatibilité des mesures de conservation avec les droits fondamentaux, celle-ci est pratiquement ignorée* ». Il est vrai que la haute juridiction administrative a seulement tenu compte de son évaluation de la menace pour la sécurité nationale pour juger que les dispositions du droit du renseignement pouvaient imposer une conservation des données en 2015 et 2016³. En revanche, la position des Professeurs Azoulais et Ritleng nous apparaît sévère au regard de la sanction prononcée par le Conseil d'Etat sur l'absence de réexamen périodique de l'obligation de conservation et des nouvelles dispositions introduites par l'article 17 de la loi du 30 juillet 2021. En effet, le

¹ Cf. L. Azoulai et D. Ritleng, « *L'État, c'est moi* ». *Le Conseil d'État, la sécurité et la conservation des données*, op. cit..

² Cf. Affaire *French Data Network e.a.*, considérant 81 et 82.

³ CE, 21 avril 2021, considérant 66.

dispositif défini désormais de manière claire et précise que l'injonction faite aux opérateurs du numérique doit respecter les exigences de proportionnalité et de nécessité en évaluant la menace pour la sécurité nationale et en limitant strictement dans le temps l'obligation de conservation à une période d'un an. En outre, l'injonction doit être prévue par un décret du Premier ministre, ce qui implique la possibilité d'exercer un recours pour excès de pouvoir contre le texte devant le Conseil d'Etat conformément aux exigences d'un contrôle indépendant et contraignant ainsi que du droit à un recours effectif. On soulignera également que la redéfinition légale des données connexion induite par les arrêts de la CJUE et du Conseil d'Etat a précisé les données concernées par l'injonction du Premier ministre.

B - Une redéfinition plus rigoureuse des données de connexion utiles au renseignement

L'arrêt *French Data Network e.a.* (considérants 35 à 46) a confirmé la conformité de la définition légale des données conservées par les opérateurs du numérique pour les besoins du renseignement aux catégories de données pouvant faire l'objet d'une obligation de conservation pour la sauvegarde de la sécurité nationale telles que précisées par la CJUE. Le Conseil d'Etat a ainsi jugé que les opérateurs du numérique pouvaient donc, en vertu des décrets attaqués, être contraints de conserver : sans limitation de durée, les données relatives à l'identité civile des utilisateurs et, pour une durée d'un an, les données relatives aux paiements, aux contrats et aux comptes des abonnés ; les données relatives aux adresses IP pour une durée d'un an ; et, les données de trafic et de localisation autres que les adresses IP pour la même durée que ces dernières.

Toutefois, le juge administratif a annulé les décrets litigieux sur la conservation des données au motif que les textes n'avaient pas prévu un réexamen périodique de la menace pour la sécurité nationale justifiant la conservation des données de connexion relevant de la dernière catégorie que nous avons précédemment mentionnée. Sur injonction de la haute juridiction administrative, le législateur et le gouvernement ont procédé à la modification exigée tout en redéfinissant dans la loi et les textes réglementaires les données de connexion traitées par les opérateurs qui sont utiles aux services de renseignement.

La loi du 30 juillet 2021 est venue modifier les articles L. 34-1 du code des postes et des communications électroniques et 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) pour y introduire : les catégories des données identifiées par la CJUE susceptibles de faire l'objet d'une obligation de conservation pour une durée limitée ; et, le mécanisme de réexamen périodique d'évaluation de la menace pour la sécurité nationale sur les données autres que les adresses IP dont l'injonction de conservation est prévue par un décret spécifique. On remarquera que le législateur s'est montré plus protecteur que la Cour de justice et le Conseil d'Etat en délimitant à une période de cinq ans la durée de conservation des données relatives à l'identité civile des utilisateurs après la fin de validité de leur contrat. En revanche, notons que la catégorie de données relatives aux données portant sur les paiements, les contrats et les comptes des abonnés n'a pas fait l'objet d'une interprétation particulière par la CJUE, le Conseil d'Etat et le législateur ont alors considéré que cette catégorie pouvait être maintenue en droit interne.

Rapidement, les décrets d'application de la loi de 2021 sont ensuite venus davantage préciser les données concernées. Pour une lecture plus facile, on présentera le nouveau dispositif dans le tableau suivant :

Tableau des données de connexion utiles au renseignement

Catégorie de données des utilisateurs	Décret n°2021-1361 du 20 octobre 2021 modifiant l'article R10-13 du code des postes et des communications électroniques (données relatives aux communications)	Décret n°2021-1362 du 20 octobre 2021 pour l'application de l'article 6 de la LCEN (données relatives à la création d'un contenu en ligne)
Identité civile	Les 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 ; La ou les adresses postales associées ; La ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant ; Le ou les numéros de téléphone.	Idem que le décret n°2021-1361
Contrats et création d'un compte	L'identifiant utilisé ; Le ou les pseudonymes utilisés ; Les données destinées à permettre à l'utilisateur de vérifier son mot de passe ou de le modifier, le cas échéant par l'intermédiaire d'un double système d'identification de l'utilisateur, dans leur dernière version mise à jour.	Idem que le décret n°2021-1361
Paiements	Le type de paiement utilisé ; La référence du paiement ; Le montant ; La date, l'heure et le lieu en cas de transaction physique.	Idem que le décret n°2021-1361

Adresses IP	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 ; Le numéro de téléphone à l'origine de la communication.	Pour les personnes mentionnées au 1 du I de l'article 6 de la loi du 21 juin 2004 susvisée et pour chaque connexion de leurs abonnés : L'identifiant de la connexion ; L'identifiant attribué par ces personnes à l'abonné ; L'adresse IP attribuée à la source de la connexion et le port associé ; Pour les personnes mentionnées au 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée et pour chaque opération de création d'un contenu telle que définie à l'article 6 : L'identifiant de la connexion à l'origine de la communication ; Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus.
Autres données utiles pour la sécurité nationale	Les caractéristiques techniques ainsi que la date, l'heure 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, mentionnées aux 1° à 4° du IV du présent article ; Pour les opérations effectuées à l'aide de téléphones mobiles, les données permettant d'identifier la localisation de la communication.	Pour les personnes mentionnées au 1 du I de l'article 6 de la loi du 21 juin 2004 susvisée et pour chaque connexion de leurs abonnés : Les dates et heure de début et de fin de la connexion ; Les caractéristiques de la ligne de l'abonné ; Pour les personnes mentionnées au 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée et pour chaque opération de création d'un contenu : L'identifiant attribué par le système d'information au contenu, objet de l'opération ; La nature de l'opération ; Les date et heure de l'opération ; L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni.

S'agissant de la dernière catégorie, il s'agit des données qui sont spécifiquement visées par le décret du Premier ministre portant injonction pendant un an de conservation aux opérateurs du numérique au regard de la menace grave, réelle et actuelle ou prévisible contre la sécurité nationale¹.

Si cette redéfinition légale des données de connexion ne semble pas apporter de changements majeurs pour les services de renseignement dont les capacités demeurent inchangées², il n'en demeure pas moins qu'elle aboutit à une augmentation des données utiles à la surveillance selon la CNIL et l'ARCEP, ce qui a suscité les craintes d'une large collecte de données par les opérateurs ou encore de faire peser une charge disproportionnée sur ces derniers³. Pour autant, l'ARCEP

¹ Décrets n° 2021-1363 du 20 octobre 2021 et n° 2022-1327 du 17 octobre 2022 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion.

² En ce sens, voir F. Dumas et F. -Nöel Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*, op. cit. et C. Malverti et C. Beauflis, *L'instinct de conservation*, op. cit..

³ Sur les craintes de la redéfinition légale des données, voir notamment la délibération de la CNIL n° 2021-114 du 7 octobre 2021 et l'avis de l'ARCEP n° 2021-2080 du 7 octobre 2021 ainsi que M. -

a tenu à rappeler que les données conservées sur injonction du Premier ministre étaient déjà collectées par les opérateurs et que la nouvelle liste de données est plus précise que l'ancienne¹. Paradoxalement, la réception en droit interne des exigences de la CJUE s'est traduite par un encadrement plus rigoureux des données de connexion mais également par un renforcement de la surveillance sur ces données.

Par ailleurs, il convient de rappeler que la redéfinition légale des données de connexion ne devrait pas être définitive et qu'elle est susceptible d'être à nouveau modifiée si l'on s'en réfère à la doctrine de la CNCTR qui adopte une approche au cas par cas pour donner son avis sur les données accessibles aux services de renseignement, expliquant que de nouveaux types de données de connexion peuvent émerger en fonction des évolutions du numérique².

C - L'extension du contrôle du renseignement numérique

En matière de contrôle des mesures de surveillance, la jurisprudence de la CJUE introduit deux innovations importantes dans le droit français : l'affirmation d'un contrôle préalable des techniques de renseignement doté d'un effet contraignant et le contentieux de l'évaluation de la menace pour la sécurité nationale. Ces innovations ont eu pour conséquence une extension du contrôle du renseignement numérique.

1. Le contrôle préalable contraignant des techniques de renseignement

En se contentant seulement de rappeler les exigences de la Cour de justice et les dispositions du code de la sécurité intérieure³, le Conseil d'Etat n'a remis en cause les techniques de renseignement soumises au droit de l'Union européenne que parce que leur contrôle *a priori* exercé par la CNCTR n'était pas doté d'un effet contraignant⁴. Si les constatations du Conseil d'Etat ne nous apparaissent pas

C. de Montecler, *Publication des nouveaux décrets sur la conservation des données*, AJDA 2021, p.2133.

¹ Cf. Avis n° 2021-2080 du 7 octobre 2021.

² Cf. CNCTR, 2^{ème} rapport d'activité (2017), p. 61.

³ Voir à ce sujet D. Simon, *Retour des monologues juridictionnels croisés ? À propos de l'arrêt du Conseil d'Etat dans l'affaire « French Data »*, op. cit..

⁴ Cf. Affaire *French Data Network e.a.*, considérants 68 à 83.

véritablement critiquables, il est toutefois intéressant de relever que la haute juridiction administrative s'est fondée sur les arrêts *Tele2 Sverige*, *La Quadrature du Net e.a.* et *Prokuratuur* pour considérer que ce contrôle contraignant devait être opéré sur l'ensemble des techniques litigieuses¹ alors même que les dispositifs des arrêts de la CJUE n'ont qu'en commun l'exigence d'un contrôle préalable et que le caractère contraignant de ce dernier ne concernait, en réalité, que la conservation généralisée et indifférenciée des données, les algorithmes de surveillance et le recueil en temps réel de données. Relevant qu'aucune technique n'avait été autorisée après un avis défavorable de la CNCTR, le Conseil d'Etat n'a pas manqué de prévoir les dispositions d'un droit transitoire en jugeant « *qu'en cas d'avis défavorable de la Commission nationale de contrôle des techniques de renseignement, le Premier ministre ne pourra légalement autoriser la mise en œuvre des techniques de renseignement mentionnées aux articles L. 851-1, L. 851-2, L. 851-4 et au IV de l'article L. 851-3 avant l'intervention de la décision du Conseil d'Etat, qu'il appartiendra alors à la commission de saisir en application de l'article L. 833-8 du même code* »².

Au regard de ces considérations, on ne peut qu'admettre que la décision du Conseil d'Etat renforce les garanties contre les risques d'abus de la surveillance des citoyens³. Mais plus encore, la loi du 30 juillet 2021 a repris le dispositif d'avis conforme énoncé par le juge administratif pour l'étendre à l'ensemble des techniques de renseignement soumises à autorisation (article 18 de la loi), y compris en matière de surveillance des communications internationales (article 23 de la loi). On saluera cette extension supplémentaire de l'exigence de la CJUE dans le droit du renseignement que l'on peut considérer comme une avancée pour l'Etat de droit.

Toujours concernant le contrôle des techniques de renseignement, on ajoutera que les précisions apportées par le Conseil d'Etat sur le droit à l'information des personnes ayant fait l'objet d'une technique de renseignement sont bienvenues pour le respect du droit à la protection des données personnelles

¹ Cf. Affaire *French Data Network e.a.*, considérant 68.

² CE, 21 avril 2021, considérant 98.

³ Dans le même sens, voir B. Bertrand et J. Sirinelli, *Le Conseil d'Etat et la conservation des données de connexion : la quadrature du cercle*, op. cit..

en matière de surveillance. Le juge administratif consacre l'existence de ce droit sans que les textes n'aient besoin d'être modifiés en appliquant aux techniques de renseignement mentionnées aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure les dispositions de la loi « informatique et libertés » du 6 janvier 1978 qui prévoient que si l'application de l'obligation d'information est exclue afin de respecter la poursuite des finalités des traitements mis en œuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique, cette obligation demeure applicable *« dès lors qu'elle n'est plus susceptible de compromettre le respect des fins poursuivies par ces mêmes traitements »*¹. On peut alors observer, ici, un déplacement du droit du renseignement vers le droit du numérique dans l'articulation entre ces deux droits pour encadrer la numérisation du renseignement.

2. Le contentieux de l'évaluation de la menace contre la sécurité nationale.

En introduisant à l'article L. 34-1 du code des postes et des communications électroniques une injonction de conservation généralisée et indifférenciée des données prévue par un décret du Premier ministre justifiant une menace grave, réelle et actuelle ou prévisible contre la sécurité nationale, le législateur de 2021 a créé un contentieux sur l'évaluation d'une telle menace qui devrait répondre aux exigences de la CJUE sur la nécessité d'un contrôle effectif et contraignant par une juridiction ou une entité administrative indépendante². D'abord envisagé d'être introduit dans l'office de la formation spécialisée du Conseil d'Etat, ce nouveau contentieux du renseignement relève finalement du contrôle du juge administratif de droit commun qui peut adapter, selon l'article L. 5 du code de justice administrative, les exigences du débat contradictoire à celles du secret de la défense nationale³. Plus concrètement, la loi implique la possibilité d'exercer un recours en annulation pour excès de pouvoir (REP) contre le décret du Premier ministre et la décision de refus d'abrogation de ce dernier.

¹ CE, 21 avril 2021, considérant 90.

² Article 17 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement

³ Voir à ce sujet l'étude d'impact de la loi du 30 juillet 2021, p. 212 à 214.

Pour notre part, la solution retenue par le législateur nous semble simpliste et ne nous apparaît pas pleinement satisfaisante au regard du risque de l'obstacle du secret qui caractérise « le contentieux de la sécurité nationale », pouvant potentiellement rendre inopérant le contentieux ouvert par la loi du 30 juillet 2021¹. D'autant plus qu'on relèvera, certes avec compréhension, que les décrets n° 2021-1363 du 20 octobre 2021 et n° 2022-1327 du 17 octobre 2022 portant injonction du Premier ministre aux opérateurs n'apportent pas de précisions sur l'évaluation de la menace contre la sécurité nationale, ce qui peut inciter à des recours aveugles et systématiques voire abusifs à chaque nouvelle injonction.

Selon nous, il aurait peut-être été préférable de soumettre la décision du Premier ministre à une procédure d'avis conforme de la CNIL ou de la CNCTR ou encore du Conseil d'Etat lui-même et à un recours contentieux devant la formation spécialisée du juge administratif en matière de renseignement et de sûreté de l'Etat et de défense. Il nous semble que cette solution est la plus conforme à la lettre de la jurisprudence de la CJUE et la plus adaptée à la mesure de surveillance en question, notamment pour contrôler rigoureusement l'évaluation du gouvernement sur la menace pour la sécurité nationale. On notera également que cette solution permettrait de mieux contrôler la décision de renouvellement, le cas échéant, de l'injonction qui pourrait être facilitée lorsque la menace est caractérisée comme prévisible et si cette prévisibilité outrepassse la durée de validité de l'injonction sauf à considérer qu'une telle hypothèse ne saurait être admise.

Au-delà de la procédure contentieuse choisie, les conséquences d'une annulation éventuelle du décret du Premier ministre ont pu être critiquées. Les Professeurs Brunessen Bertrand et Jean Sirinelli ont relevé « *que le contentieux de l'existence de la menace grave ressemble à une impasse contentieuse alors même que la décision La Quadrature du net exige un « contrôle effectif* » » puisqu'une décision du Conseil d'Etat annulant le décret d'injonction de conservation remettrait en cause le dispositif de l'arrêt *French Data Network e.a.* ainsi que le dispositif réglementaire qui en découle au regard des exigences constitutionnelles de

¹ En ce sens, voir B. Warusfel, *Le contentieux de la sécurité nationale*, in *Annuaire du droit de la sécurité et de la défense* 2018, mare & martin, p. 203 à 218.

sécurité¹. Le problème d'inconstitutionnalité ici soulevé s'explique par le fait que l'arrêt du 21 avril 2021 et la loi du 30 juillet 2021 et ses décrets d'application ont utilisé le cadre juridique du renseignement et de la sécurité nationale pour venir au secours des enquêtes judiciaires et de sécurité publique face à des difficultés pratiques de l'application de la jurisprudence de la CJUE, ce qui fait l'objet de notre développement suivant.

D - Le cadre juridique du renseignement au secours des enquêtes judiciaires et de sécurité publique

En reconnaissant l'importance de l'objectif de sécurité nationale justifiant un cadre juridique dérogatoire applicable aux besoins du renseignement numérique, l'arrêt *La Quadrature du Net e.a.* a permis au Conseil d'Etat d'exploiter ce droit dérogatoire pour les besoins des services d'enquêtes judiciaires et de sécurité publique. Par une réinterprétation nationale des exigences européennes, le juge administratif et le législateur ont ainsi consolidé le volet judiciaire de la sécurité nationale mais aussi entraîné une certaine dépendance des enquêtes judiciaires et de sécurité publique au cadre du renseignement.

1. Le renseignement et les infractions relatives aux atteintes aux intérêts fondamentaux de la Nation

Dans son arrêt *French Data Network e.a.* du 21 avril 2021, le Conseil d'Etat a considéré que la répression des infractions relatives aux atteintes aux intérêts fondamentaux de la Nation et au terrorisme figurant au titre Ier et II du livre IV du code pénal entre dans ce que nous identifions comme le « bloc de sécurité nationale » justifiant la conservation généralisée et indifférenciées des données (considérant 43). Cette précision nous semble conforme à la jurisprudence de la CJUE en matière de surveillance qui reconnaît que la lutte contre les infractions terroristes entre dans le champ de la sécurité nationale².

Ainsi, notre hypothèse d'un « bloc de sécurité nationale », initialement consacré pour répondre aux besoins des services de renseignement, serait confortée par sa composition qui regroupe : le renseignement d'Etat délimité par

¹ Cf. B. Bertrand et J. Sirinelli, *Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle*, op. cit..

² Cf. Affaire *Ligue des droits humains*, point 219 et 220.

les finalités de l'article L. 811-3 du code de la sécurité intérieure et les enquêtes criminelles renvoyant aux infractions du code pénal évoquées précédemment. La loi du 30 juillet 2021 semble confirmer cette composition en affirmant seulement que la conservation généralisée et indifférenciée des données peut être justifiée « *pour des motifs tenant à la sauvegarde de la sécurité nationale* » sans faire de distinction entre les activités du renseignement et de la police judiciaire. De son côté, la Cour de cassation a également rattaché les infractions relatives aux intérêts fondamentaux de la Nation et au terrorisme à la sauvegarde de la sécurité nationale dans plusieurs décisions de juillet 2022¹.

Ces considérations ne sont pas négligeables en matière de contre-espionnage ou de lutte contre le terrorisme sur le territoire national puisqu'elles permettent à la Direction générale de la sécurité intérieure (DGSI) de conserver ses capacités opérationnelles aussi bien pour ses agents de renseignement que pour ceux exerçant des missions de police judiciaire, le service ayant « *une double compétence renseignement et judiciaire à des fins d'entrave* »².

Enfin, l'injonction de conservation des données du Premier ministre devrait donc pouvoir être justifiée pour des enquêtes pénales en cours diligentées par la DGSI, ce qui pourrait avoir pour conséquence une caractérisation systématique de la menace pour la sécurité nationale profitable à l'ensemble des services de renseignement étant donné la longueur des procédures judiciaires. Curieusement, le cadre judiciaire pourrait alors venir, cette fois, au secours du renseignement.

2. Une dépendance des enquêtes judiciaires et de sécurité publique au renseignement

Alors que la Cour de justice de l'Union européenne n'a admis qu'une conservation ciblée des données de connexion en fonction de zones géographiques ou de catégories de personnes ainsi qu'une conservation rapide de ces mêmes données pour les enquêtes de criminalité et de sécurité publique qui sont graves,

¹ Cass. crim., 12 juill. 2022, n° 21-83.710, point 25 et Cass. crim., 12 juill. 2022, n° 21-83.820, 21-84.096 et 20-86.652, points 9, 10 et 23. En ce sens, voir également N. Véron, *Le Conseil constitutionnel et la conservation des données de connexion : entre apaisement et perturbation du dialogue des juges*, Communication Commerce électronique n° 10, Octobre 2022, étude 18 ; J. Buisson, *Données de connexion, conservation et accès : la primauté du droit de l'Union réaffirmée*, Procédures n° 10, Octobre 2022, étude 11.

² Sur la double compétence de la DGSI, voir sur le site en ligne du service [Nos missions | DGSI \(interieur.gouv.fr\)](https://nosmissions.dgsi.interieur.gouv.fr) et l'article 1^{er} du décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure.

le Conseil d'Etat a toutefois signalé que ces limites à la conservation des données étaient techniquement difficiles à mettre en œuvre pour les opérateurs et seraient contraire au principe constitutionnel d'égalité devant la loi. La haute juridiction administrative a conclu que les exigences formulées par la CJUE avaient pour conséquence de remettre en cause les moyens d'enquêtes de criminalité et de sécurité publique du fait de l'importance des données de connexion pour ces dernières et, par là même, les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, ainsi que de recherche des auteurs d'infractions, notamment pénales. En revanche, le risque d'inconstitutionnalité est écarté par le Conseil d'Etat dès lors que la conservation rapide des données, qui est une obligation déjà prévue par la Convention de Budapest de 2001 sur la cybercriminalité, est permise lorsque les données sont conservées dans le cadre de la conservation généralisée et indifférenciée pour la sécurité nationale¹. Le raisonnement technicien du Conseil d'Etat met en lumière le manque de réalisme de la solution de la CJUE², mais tire parti de l'analyse de cette dernière selon laquelle l'accès aux données de connexion peut être autorisée à des fins de lutte contre la criminalité grave sur des données conservées conformément à l'article 15§1 de la directive 2002/58³. Cette solution, qui sera reprise par le législateur de 2021⁴, implique une certaine dépendance opérationnelle des enquêtes judiciaires recourant à la conservation rapide des données à la validité de l'injonction du Premier ministre en matière de renseignement et de sécurité nationale, ce qui a suscité des critiques sur la pérennité juridique du dispositif.

Tout d'abord, on relèvera que cette dépendance, qui permet aux enquêteurs judiciaires luttant contre la criminalité grave d'accéder à des données conservées pour des finalités relevant du renseignement ou de la criminalité de sécurité nationale, entraînerait « *l'occultation du principe de finalité* » affirmé en droit de la protection des données personnelles « *...qui protège les citoyens des glissements et*

¹ Cf. Affaire *French Data Network e.a.*, considérants 47 à 59.

² En ce sens, voir D. Simons, *Retour des monologues juridictionnels croisés ? À propos de l'arrêt du Conseil d'Etat dans l'affaire « French Data »*, op. cit..

³ Sur ce point, voir notamment C. Malverti et C. Beaufiles, *L'instinct de conservation*, op. cit..

⁴ Article L. 34-1-III bis du code des postes et des communications électroniques.

des risques d'usage abusif des bases de données » comme le rappelle le Professeur Azoulai et Ritleng¹. Cependant, on soulignera que cette atteinte au principe de finalité peut être justifiée par l'interprétation extensive faite par la CJUE de l'article 15§1 de la directive 2002/58 si l'on s'accorde avec l'arrêt *French Data Network e.a.* du Conseil d'Etat.

Ensuite, en s'attachant à assurer le respect des exigences constitutionnelles de sécurité par son raisonnement, le Conseil d'Etat placerait le régime de conservation des données en matière de surveillance dans une situation constitutionnelle et conventionnelle précaire. En effet, les Professeurs Brunessen Bertrand et Jean Sirinelli remarquent que les exigences constitutionnelles de sécurité nationale ou de lutte contre la criminalité grave ne peuvent être assurées que si la conservation généralisée et indifférenciée des données est maintenue de façon permanente alors que le droit de l'Union européenne considère cette mesure comme dérogatoire, limitée dans le temps et contestable². On peut comprendre alors l'impasse du contentieux de l'évaluation de la menace pour la sécurité nationale. Une annulation de l'injonction du Premier ministre remettrait en cause non seulement les besoins de la sécurité nationale mais aussi ceux des enquêtes criminelles graves et, par là même, les objectifs de valeur constitutionnelle de sécurité, sauf à considérer que ces derniers sont tout bonnement respectés par la simple mise en place du dispositif législatif de conservation en question. A notre sens, le dispositif finalement retenu par le législateur de 2021 tend à rendre effectives les missions des services de sécurité en accord avec la nature des objectifs de valeur constitutionnelle³ tout en permettant aux individus de s'opposer juridiquement aux risques d'abus de la surveillance de leurs données comme l'exige le droit de l'Union européenne. Autrement dit, l'inconstitutionnalité d'une annulation de l'injonction du Premier ministre au motif du respect des exigences constitutionnelles de sécurité nationale devrait être écartée. Il devrait en être de même pour le respect des exigences relatives à la lutte contre la

¹ Cf. L. Azoulai et D. Ritleng, « *L'État, c'est moi* ». *Le Conseil d'État, la sécurité et la conservation des données*, op. cit..

² Cf. B. Bertrand et J. Sirinelli, *Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle*, op. cit..

³ En ce sens, voir P. de Montalivet, *Les objectifs de valeur constitutionnelle*, Cahiers du Conseil constitutionnel n° 20, juin 2006.

criminalité grave. La rédaction de l'article L. 34-1-III bis du code des postes et des communications électroniques ne lie pas juridiquement la conservation rapide des données à l'injonction du Premier ministre, même si la Cour de cassation a réaffirmé que la légalité de la conservation rapide peut être liée en pratique à celle prévue pour la sauvegarde de la sécurité nationale¹.

Si certains ont pu considérer cette réinterprétation du Conseil d'Etat de l'interprétation de la CJUE comme un dialogue des juges positif pour la construction européenne et le respect des droits fondamentaux dans l'Union², d'autres ont considéré que l'aménagement opéré par le juge français constituait une déformation critiquable du raisonnement du juge de l'Union européenne³. Quoiqu'il en soit, il est certain qu'un désaccord s'est formé entre la Cour de justice et le juge administratif « *sous couvert de conciliation avec la sauvegarde des objectifs de valeur constitutionnelle* », pour reprendre les termes des Professeurs Thibault Douville et Hélène Gaudin⁴.

On soutiendra que les objectifs de valeur constitutionnelle de sécurité incitent juridiquement à adopter des mesures effectives pour assurer la sécurité ou les procédures pénales mais qu'ils ne devraient pas permettre de prendre ou de maintenir des décisions jugées abusives pour les droits et libertés des individus, notamment au regard du droit de l'Union européenne. Le Conseil constitutionnel a d'ailleurs jugé, le 25 février 2022 à l'occasion d'une QPC, que si les dispositions de l'article L. 34-1 du code des postes et des communications électroniques issues de la loi de programmation militaire du 18 décembre 2013 respectaient la poursuite des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions, il reste que la conservation généralisée et indifférenciée prévue pour ces objectifs devait être considérée

¹ Voir notamment J. Buisson, *Données de connexion, conservation et accès : la primauté du droit de l'Union réaffirmée*, op. cit..

² En ce sens, voir notamment C. Malverti et C. Beaufiles, *L'instinct de conservation*, op. cit..

³ En ce sens, voir notamment C. de Terwangne, « *L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt La Quadrature du Net de la Cour de justice de l'Union européenne* », op. cit..

⁴ Cf. T. Douville et H. Gaudin, *Un arrêt sous le signe de l'exceptionnel*, op. cit..

Dans le même sens, voir également A. Iliopoulou-Penot, *La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué*, op. cit..

comme une atteinte disproportionnée au droit au respect de la vie privée¹. Toutefois, cette même décision prévoit que les objectifs de valeur constitutionnelle de sécurité font obstacle à ce que cette inconstitutionnalité puisse remettre en cause les procédures pénales existantes, un second désaccord apparaît avec la jurisprudence de la CJUE qui exige l'effet immédiat d'une décision sanctionnant une législation imposant une conservation disproportionnée des données².

Dans ces conditions, un arbitrage entre les positions divergentes des juges ne serait alors possible qu'au niveau du législateur de l'Union européenne qui devrait affirmer une européanisation du droit du renseignement déjà engagée.

§4. Une européanisation indéniable du droit du renseignement

Le droit de l'Union européenne est devenu une source juridique difficilement contestable du droit de la surveillance numérique et du cadre juridique des services de renseignement. D'abord parce qu'au fil des décisions de la CJUE et des réponses nationales, les juges de Luxembourg ont su construire une interprétation uniforme de la surveillance numérique même si leurs solutions ont connu des limites. Ensuite, l'intervention du législateur de l'Union européenne nécessaire pour pallier l'insécurité juridique des règles jurisprudentielles relatives à la conservation et à l'accès aux données de connexion devrait entériner une harmonisation européenne des garanties applicables à la surveillance partenariale avec les opérateurs du numérique. Enfin, cette européanisation soulève à nouveau un débat théorique sur les fondements du droit du renseignement et la dialectique « sécurité et liberté ».

A - L'uniformisation de l'interprétation par la Cour de justice de l'Union européenne

L'encadrement de la surveillance numérique par le droit de l'Union européenne s'est développé à travers les réponses de la Cour de justice aux questions préjudicielles des juridictions nationales. Dans ce contexte, le contrôle

¹ Décision n° 2021-976/977 QPC du 25 février 2022, M. Habib A et autre.

² Voir affaire *Commissioner of An Garda Síochána* du 5 avril 2022 A ce sujet, voir également F. Peltier et C. Wierre, *L'acharnement thérapeutique de la justice sur les données de connexion des opérateurs de téléphonie*, La Semaine Juridique Edition Générale n° 17, 2 mai 2022, 544 et N. Véron, *Le Conseil constitutionnel et la conservation des données de connexion : entre apaisement et perturbation du dialogue des juges*, op. cit..

exercé par la CJUE a pour objectif de « *garantir une uniformité d'interprétation et d'application du droit communautaire* »¹. A la différence de la CEDH qui veille à la conformité d'une législation particulière à la Conv. EDH, la CJUE cherche à rapprocher les législations des Etats membres².

1. L'autorité respectée de la Cour de justice de l'Union européenne

De manière générale, la Cour de justice s'est efforcée d'uniformiser les garanties applicables à la surveillance numérique dans l'exploitation : des données de connexion traitées par les opérateurs du numérique ; des données PNR ; ainsi que des données transférées hors de l'Union européenne. Dans le domaine du renseignement, l'uniformisation de l'interprétation du droit de l'Union européenne s'est particulièrement illustrée par l'introduction d'une notion européenne de la sécurité nationale qui justifie les mesures les plus graves portant à la fois sur les données de connexion mais aussi sur les données PNR. Désormais, l'ensemble des législations nationales sur le renseignement sont contraintes d'appliquer cette notion lorsqu'elles portent notamment sur la conservation généralisée et indifférenciée des données ou sur les techniques algorithmiques. Sur ces dernières, la jurisprudence de la CJUE semble même avoir dessiné « *le noyau dur d'une future régulation des algorithmes* », pour reprendre les termes de Winston Maxwell³. L'autorité des décisions de la Cour de justice et la primauté du droit de l'Union européenne ont été respectées par les autorités nationales, les juges et le législateur français ayant largement repris les exigences européennes en droit interne. De son côté, la Cour constitutionnelle belge n'a pas hésité à annuler la législation nationale concernée en imposant au législateur « un changement de perspective » plus cohérent avec le droit de l'Union européenne⁴.

¹ A ce sujet, voir notamment J. Dupont-Lassalle, « *La « subsidiarité juridictionnelle », instrument de l'intégration communautaire ?* », Droit et société, vol. 80, no. 1, 2012, pp. 47-71.

² En ce sens, voir R. Mehdi et E. Brosset, *De quoi le droit de l'Union est-il le nom ? À propos du droit de l'Union entendu comme le droit commun des Etats membres*. B. Bonnet. Traité des rapports entre ordres juridiques, LGDJ, pp. 669-695, 2016.

³ Cf. W. Maxwell, *La CJUE dessine le noyau dur d'une future régulation des algorithmes*, op. cit..

⁴ Cour constitutionnelle belge, 22 avril 2021, n° 57/2021. Sur cette décision, voir notamment D. Simon, *Retour des monologues juridictionnels croisés ? À propos de l'arrêt du Conseil d'État dans l'affaire « French Data »*, op. cit. et C. de Terwangne, « *L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt La Quadrature du Net de la Cour de justice de l'Union européenne* », op. cit..

2. Les considérations technologiques, le « bug » jurisprudentiel

Pour autant, l'uniformisation européenne des règles sur la surveillance numérique par le mécanisme du renvoi préjudiciel est fragile. En effet, les mesures de conservation des données et l'accès à ces dernières par les services de sécurité et d'enquête criminelle ont pu être considérées en France comme une exigence constitutionnelle relevant de l'identité constitutionnelle des Etats membres permettant de déroger au principe d'uniformité du droit de l'Union¹. Dans les faits, on rappellera que le Conseil d'Etat et le Conseil constitutionnel ont tous deux exprimé des contradictions avec la jurisprudence de la CJUE pour des raisons techniques pertinentes. On s'étonnera d'ailleurs de la persistance du raisonnement irréaliste des juges de Luxembourg sur le ciblage des données à conserver en fonction de zones géographiques ou de catégories de personnes dans le cadre de la lutte contre la criminalité grave². Aussi, on peut comprendre que l'effet immédiat d'une décision d'invalidité d'une législation nationale imposant une conservation disproportionnée des données peut apparaître trop radicale pour la sécurité juridique des procédures antérieures à la décision au regard de l'importance des données pour les enquêtes. A contrario, le raisonnement des juges français manque de neutralité technologique en considérant que la conservation généralisée et indifférenciée des données demeure le seul moyen de garantir l'efficacité des services de sécurité compte tenu des capacités numériques actuelles, ce qui pourrait laisser penser que le respect des libertés fondamentales devrait s'incliner devant des considérations technologiques³.

Comme l'ont relevé Clément Malverti et Cyrille Beaufiles, le dialogue des juges a fait émerger un modèle de « pluralisme interprétatif » permettant une approche nationale de l'eupéanisation du cadre juridique de la surveillance numérique⁴. Cependant, les autorités nationales devraient rester soumises aux contraintes interprétatives de la Cour de justice puisque la primauté du droit de

¹ En ce sens, voir l'intervention de Jean-Marc Sauvé, *L'autorité du droit de l'Union européenne : le point de vue des juridictions constitutionnelles et suprême*, Congrès du 25ème anniversaire de l'Académie de droit européen (ERA) à Trèves le 19 octobre 2017.

² A ce sujet, voir B. Bertrand, *Chronique Droit européen du numérique, Les précisions sur l'interprétation et l'application du régime de l'e-privacy*, RTD Eur. 2022, p.481.

³ Dans le même sens, voir F. Peltier et C. Wierre, *L'acharnement thérapeutique de la justice sur les données de connexion des opérateurs de téléphonie*, op. cit..

⁴ Cf. C. Malverti et C. Beaufiles, *L'instinct de conservation*, op. cit..

l'Union n'a pas été clairement remise en cause. Les approches réalistes des juges français pourraient alors malheureusement exposer l'Etat à une procédure en manquement puisque les objectifs de valeur constitutionnelle de sécurité fondés sur des considérations technologiques ne semblent pas constituer des justifications suffisamment solides pour s'écarter de l'interprétation de la CJUE au regard de ses récentes décisions. Cette situation d'insécurité juridique pousse nécessairement le législateur de l'Union européenne à intervenir.

B - L'harmonisation par le législateur de l'Union européenne

Projet actuellement limité, le nouveau projet de règlement ePrivacy devrait, selon nous, être perfectible pour bien intégrer la jurisprudence de la CJUE.

1. Le règlement ePrivacy, un projet limité

Dès 2017, une proposition de règlement européen abrogeant la directive 2002/58/CE a été adoptée par le Parlement et le Conseil afin que le texte ne prévoie plus aucune disposition spécifique à la conservation des données pour que les Etats membres puissent prendre les mesures qu'ils estiment nécessaires dans le respect du droit de l'Union européenne et de la jurisprudence de la Cour de justice. Dans le cadre des débats, la France a souhaité que le projet de règlement « ePrivacy » exclue de son champ d'application les traitements relevant de la sécurité nationale et de la défense pour que le droit du renseignement échappe aux injonctions de la CJUE¹. Cette demande a été accueillie par le Conseil dans le nouveau projet de règlement arrêté le 10 février 2021 qui prévoit notamment dans son article 2 l'inapplicabilité du règlement aux traitements relatifs à la sécurité nationale réalisés par des autorités publiques ou des opérateurs privés pour le compte de ces dernières. En outre, les articles 6 et 7 du nouveau projet autorisent le traitement des données de connexion ainsi que leur stockage pour une durée limitée afin d'assurer la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, ainsi que la sauvegarde et la prévention de menaces pour la sécurité publique dans le respect de l'essence des droits et libertés fondamentaux de l'Union et des principes de nécessité et de proportionnalité.

¹ Voir en ce sens Y. Braun-Pivet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018*, op. cit., p. 77 et G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 163 et 164.

Ce nouveau projet semble limiter la portée de la jurisprudence de la CJUE. Il n'est alors pas certain qu'il emporte la conviction du Parlement européen en matière de protection de la vie privée et des données personnelles¹. D'autant plus que le CEPD a considéré que le règlement ePrivacy ne devait en aucun cas abaisser le niveau de protection des données offert par la Charte et la jurisprudence *Privacy International* et *La Quadrature du Net e.a.* de la CJUE ainsi que par la Conv. EDH telle qu'elle est interprétée par la CEDH². Par ailleurs, il est intéressant de noter que certains commentateurs n'ont pas manqué de relever que la remise en cause de la jurisprudence de la CJUE par le nouveau projet de règlement pourrait rendre plus difficile l'application des standards européens en matière de surveillance numérique aux pays tiers dans le cadre des transferts de données hors de l'Union européenne, c'est-à-dire que la portée de la jurisprudence *Schrems* pourrait être fragilisée³.

2. Le règlement ePrivacy, un projet perfectible

Pour notre part, on s'alignera sur la position du CEPD tant pour le respect de la protection des données personnelles que pour les apports de la jurisprudence bienveillante de la CJUE à l'Etat de droit. Certes, les solutions de la Cour de justice n'ont pas fait l'unanimité des juridictions nationales mais les aménagements réalisés par ces dernières pourraient servir à guider le législateur de l'Union européenne dans la production d'un texte équilibré et respectueux des libertés des individus et des exigences de sécurité des Etats membres. Enfin, on comprendrait difficilement une totale remise en cause des solutions de la CJUE alors même que les juridictions nationales se sont montrées également bienveillantes et favorables à introduire les garanties européennes voir même à les amplifier en droit interne et, plus particulièrement, en droit du renseignement.

¹ En ce sens, voir notamment B. Bertrand, *L'audace sans le tact : jusqu'où la Cour de justice peut-elle aller trop loin ?*, Dalloz IP/IT 2021, p.468 et E. Delcher, *La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ?*, RDP, mai 2022, p. 845.

² Cf. EDPB, Statement 03/2021 on the ePrivacy Regulation, 9 March 2021.

³ En ce sens, voir C. Moreno et K. Medjaoui, *Dissension among the Courts: France and EU Personal Data Retention Standards*, Revue Internationale de la Compliance et de l'Éthique des Affaires n° 4, Août 2022, comm. 200.

C – Une européanisation qui réinterroge les fondements du droit du renseignement

A travers sa jurisprudence, la CJUE a rappelé l'importance du droit de la protection des données personnelles dans l'encadrement des mesures de surveillance numérique, ce qui n'est pas sans questionner véritablement la place de ce droit dans la construction du droit du renseignement. On peut également s'interroger sur l'émergence d'un « droit européen du renseignement » fondé sur les garanties dégagées par la Cour de Strasbourg et la Cour de Luxembourg.

1. La place du droit de la protection des données personnelles dans la dialectique « sécurité et liberté » en matière de renseignement

Le droit de l'Union européenne, cadre général commun du droit de la protection des données personnelles depuis le RGPD et, plus largement, de la vie privée numérique, a désormais reconnu et clarifié la notion de sécurité nationale comme intérêt public justifiant les atteintes les plus graves aux droits et libertés. En cela, le droit de l'Union européenne s'est accordé avec la construction du droit du renseignement et ses principes que sont la défense et la promotion des intérêts fondamentaux de la Nation et la protection du secret de la défense nationale. En définitive, le droit du renseignement demeure un droit exorbitant qui déroge au droit au respect de la vie privée selon l'articulation prévue par les textes tant nationaux qu'européen en matière de libertés et de droits fondamentaux. Pour autant, le droit de la protection des données personnelles s'est imposé comme un droit fondamental dont on aurait pu penser qu'il remette en cause le caractère dérogatoire du droit du renseignement en matière de techniques de surveillance.

Ces propos sont à prendre en compte puisqu'il a pu être soutenu par Noémie Véron que l'utilisation des données personnelles par le renseignement fait l'objet d'un régime juridique « singulier », voir « autonome » qui s'est construit sur un assouplissement du droit de la protection des données personnelles pour répondre aux impératifs des services de renseignement lorsque l'on compare les principes applicables à la protection des données personnelles aux règles qui gouvernent les mesures secrètes de surveillance numérique¹. Cependant, cette

¹ Voir N. Véron, *Protection des données personnelles et renseignement : contribution à l'identification d'un régime juridique autonome*, Institut Francophone Justice et Démocratie – Theses N° 217, 20 décembre 2022.

analyse, qui pourrait laisser penser que le droit de la protection des données personnelles occuperait une place hiérarchiquement supérieure au droit du renseignement, nous semble occulter la valeur constitutionnelle des intérêts fondamentaux de la Nation et du secret de la défense nationale dans le droit français¹ et la reconnaissance de l'importance de ces intérêts dans la notion de sécurité nationale définie par la CJUE.

Il convient d'admettre que les techniques de surveillance encadrées par le droit du renseignement sont largement soumises à des garanties relatives à la protection des données personnelles, d'autant plus avec la diffusion de la jurisprudence de la CJUE dans les droits nationaux. Toutefois, il nous apparaît plus évident de dire que l'utilisation des données personnelles en renseignement fait l'objet d'un régime juridique dérogatoire du droit de la protection des données personnelles justifié par les besoins de la sécurité nationale dont les fondements juridiques ont la même valeur constitutionnelle et conventionnelle que le droit au respect de la vie privée. Par conséquent, le droit de la protection des données personnelles ne doit pas être regardé comme assoupli dans ses principes, mais bien comme un instrument existant et efficace de limitation des nouvelles mesures secrètes de surveillance numérique. Cette instrumentalisation du droit de la protection des données personnelles contribue effectivement à l'identification d'un régime juridique particulier qui est, selon nous, le droit du renseignement numérique².

2. L'émergence d'un droit européen du renseignement fondé sur les garanties dégagées par les juges européens

La jurisprudence de la Cour de Strasbourg et de la Cour de Luxembourg nous invite à nous interroger sur « la consécration d'un *jus commune* européen du renseignement », pour reprendre les termes de Béatrice Guillaumin³. A ce sujet, on prolongera l'analyse de cette dernière relative aux obstacles à la consécration d'un droit commun européen du renseignement en ajoutant, aux limites liées aux

¹ Décision n° 2011-192 QPC du 10 novembre 2011, *Mme Ekaterina B., épouse D., et autres*.

² Cf. Première partie

³ Cf. B. Guillaumin, « *Étude comparée des jurisprudences de la CEDH et de la CJUE : vers la consécration d'un jus commune européen du renseignement ?* », *Études françaises de renseignement et de cyber*, vol. 1, no. 1, 2023, pp. 23-37.

singularités des juges européens et à la diffusion pleine et entière de leur jurisprudence dans les droits nationaux, que l'organisation juridique de l'appareil de renseignement d'Etat répond à des enjeux de souveraineté nationale qui rend difficile, mais pas impossible au regard notamment des échanges entre les instances spécialisées de contrôle¹, une appréciation commune de l'organisation et du fonctionnement des activités des services de renseignement et de leur contrôle en Europe². Préalablement à la consécration d'un droit commun européen du renseignement, il devrait être nécessaire de s'entendre sur une harmonisation de la notion de sécurité nationale au niveau européen, ce que la jurisprudence de la CJUE pourrait initier.

On prolongera également l'analyse de Béatrice Guillaumin sur les marqueurs de rapprochement de la jurisprudence de la CEDH et de la CJUE en admettant qu'il existe bien désormais un *jus commune* européen spécial de la surveillance numérique qui ne concerne pas seulement le renseignement d'Etat de sécurité nationale, mais aussi la sécurité publique et les enquêtes judiciaires.

Pour finir, on n'oubliera pas de remarquer que la CJUE a mis en cohérence sa jurisprudence avec la Convention de Budapest sur la cybercriminalité de 2001 en rappelant l'exigence de conservation rapide des données pour les besoins des enquêtes pénales. Cette intrication entre le droit pénal du numérique et l'encadrement des mesures de surveillance n'est pas extraordinaire. Au contraire, elle est au cœur de l'encadrement juridique de la numérisation du renseignement.

¹ Sur ce point, voir Y. Braun-Pivet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018*, op. cit., p. 67 à 81 et O. Brun, « Union européenne », Hugues Moutouh éd., *Dictionnaire du renseignement*, op. cit., pp. 801-804

² A ce sujet, les travaux de Béatrice Guillaumin démontrent bien en France la singularisation de l'appareil de renseignement qui dispose d'attributs extraordinaires (B. Guillaumin, *L'appareil français de renseignement. Une administration ordinaire aux attributs extraordinaires*, Mare et Martin, Bibliothèque des thèses, 25 avril 2024).

CHAPITRE II

L’AFFIRMATION DU DROIT PENAL DU NUMERIQUE

Si le droit du renseignement constitue le socle juridique des techniques de renseignement, il se réfère directement ou indirectement au droit pénal du numérique pour : d’une part, réprimer l’usage abusif du renseignement numérique susceptible de relever de la cybercriminalité (**Section I**) ; d’autre part, déterminer plus précisément les appareils et dispositifs techniques directement utilisés par les services de renseignement (**Section II**).

SECTION I : La répression de l’abus cybercriminel du renseignement numérique

Bien que le droit du renseignement autorise le recours à des moyens d’investigation numérique, il n’empêche pas que les personnes impliquées dans la mise en œuvre de ces moyens puissent être poursuivies pénalement. En effet, le droit commun de la responsabilité pénale trouve à s’appliquer en cas de faute personnelle d’un agent qui aurait abusivement utilisé un moyen numérique de renseignement dans le cadre d’une surveillance ou pour servir ses propres intérêts¹.

A ce sujet, nous avons pu observer que, tant en théorie qu’en pratique, les moyens numériques mis à disposition des agents des services de renseignement sont susceptibles de servir à commettre une ou plusieurs infractions cybercriminelles (§1). On soutiendra que cette appréhension pénale du renseignement numérique entraîne alors une délicate conciliation à opérer entre le droit du renseignement et les mesures dédiées à la lutte contre la cybercriminalité (§2).

¹ Cf. supra. §2 de la Section II du Chapitre I du Titre II de la Ière Partie.

§1. Des moyens numériques susceptibles de servir à commettre des infractions cybercriminelles

Tout d'abord, l'usage frauduleux d'un moyen légalisé de renseignement numérique peut constituer une ou plusieurs infractions réprimées par les législations nationales relatives à la cybercriminalité. Pour les Etats signataires de la Convention sur la cybercriminalité de Budapest de 2001, il s'agit des infractions qui regroupent celles qui constituent : des atteintes à la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ; des falsifications ou fraudes informatiques ; des contenus publiés en ligne illicites, ce qui vise particulièrement la pédopornographie ; des atteintes à la propriété intellectuelle et aux droits connexes par des moyens numériques¹. Dans le cadre de sa politique de lutte contre la cybercriminalité, l'Union européenne distingue trois formes de cybercriminalité évoquant les infractions retenues par la Convention de Budapest : d'une part, la criminalité propre aux réseaux électroniques s'intéressant aux attaques contre les systèmes numériques qui constituent des infractions définies dans une directive de 2013² ; d'autre part, la publication de contenus illicites tels que ceux incitant à la violence, à la haine ou au terrorisme ; enfin, les formes traditionnelles de délinquance utilisant les outils numériques et internet³. On ajoutera que cette « classification tripartite » est également utilisée dans la doctrine pour définir l'étendue de la cybercriminalité⁴. En France, ces différentes formes de cybercriminalité font l'objet d'une multiplicité d'incriminations spéciales dans le code pénal depuis la fin des années 1970 ou sont rattachées à des « infractions de portée générale » telles que l'escroquerie ou l'abus de confiance⁵.

¹ Sur les infractions cybercriminelles retenues par les Etats, voir également E. C. Viano, « *Section II - Droit pénal. Partie spéciale - Société de l'information et droit pénal. Rapport général* », *Revue internationale de droit pénal*, vol. 84, no. 3-4, 2013, pp. 311-334.

² Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

³ Sur ce point, voir Communication de la Commission au Parlement européen, au Conseil et au Comité des Régions, Vers une politique générale en matière de lutte contre la cybercriminalité, 22 mai 2007.

⁴ Voir notamment M. Watin-Augouard, *Cybermenace et sécurité nationale*, Le droit de la sécurité et de la défense en 2013, Presse universitaire d'Aix-Marseille, PUAM, 2014, p. 302 et 303.

⁵ Voir notamment S. Joissains et J. Bigot, *Rapport d'information sur la lutte contre la cybercriminalité*, Sénat, 9 juillet 2020, p. 27 à 31 et B. Pereira, « *La lutte contre la cybercriminalité : de l'abondance de*

Ensuite, certaines cyberopérations des services de renseignement, qui entrent dans le champ d'application de leur mission générale de collecte et d'exploitation de données ou de contribution à l'entrave des risques et menaces susceptibles d'affecter la vie de la Nation, en France ou à l'étranger¹, mais dont les techniques n'ont pas fait l'objet de dispositions spécifiques en droit du renseignement peuvent présenter un risque pénal fondé sur des infractions cybercriminelles. Avant de poursuivre notre démonstration, on rappellera que les infractions pénales retenues sont également des moyens de lutte contre les activités de cyberespionnage d'organisations ou de puissances étrangères qui viseraient la France ou des acteurs privés.

A - Les infractions cybercriminelles applicables aux moyens légalisés de renseignement numérique

Parmi les infractions relatives à la lutte contre la cybercriminalité, on peut établir une liste de cinq types d'infractions cybercriminelles qui peuvent être retenues en matière de renseignement numérique. Etant donné le nombre de moyens numériques de renseignement prévu par le code de la sécurité intérieure et que l'usage abusif de ces moyens constituent régulièrement un concours idéal ou réel d'infractions, la liste des types d'infractions retenues servira donc de plan à notre analyse pour éviter de nombreuses répétitions dans un effort de synthèse.

1. Les atteintes aux systèmes de traitement automatisé de données

De manière générale, ces infractions visent le piratage des systèmes de traitement automatisé de données (STAD) qui, sans être juridiquement définies, correspondent à « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, d'organes d'entrées-sorties, et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* » selon le rapport Thyraud du 2 octobre 1987 rédigé dans le cadre des travaux préparatoires de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite « Godfrain »². Concrètement, il s'agit des équipements informatiques et de

la norme à sa perfectibilité », Revue internationale de droit économique, vol. xxx, no. 3, 2016, pp. 387-409.

¹ Article L. 811-2 du code de la sécurité intérieure.

² Cf. J. Thyraud, *Rapport sur la proposition de loi adoptée par l'Assemblée nationale relative à la fraude informatique*, Sénat, 2 octobre 1987, p. 52.

leurs logiciels et programmes comme les ordinateurs, tablettes et smartphones ou encore les objets connectés ainsi que tous les réseaux tels que le WI-FI par exemple.

Parmi ces infractions codifiées au chapitre III du titre II du livre III du code pénal, les qualifications d'accès ou de maintien frauduleux dans un STAD¹, d'introduction frauduleuse de données dans un STAD ou d'extraction, de reproduction ou de transmission frauduleuses de données contenues dans un STAD² ainsi que de détention, d'offrir, céder ou de mettre à disposition un moyen de piratage informatique³ peuvent être retenues pour réprimer l'utilisation abusive des moyens numériques de renseignement suivant :

- les dispositifs techniques d'interception des données de connexion ou de communications⁴ ;
- les interceptions de communications hertziennes ou satellitaires⁵ ;
- la captation de données informatiques⁶ ;
- les traitements de données encadrés par les dispositions de la loi « Informatique et libertés » et celles du droit du renseignement relatives notamment aux transmissions d'informations⁷ et au recours à l'intelligence artificielle⁸.

En effet, l'intention frauduleuse d'accéder à un STAD ou de s'y maintenir est réprimée par la loi et la jurisprudence pour sanctionner tous les types d'intrusion informatique indépendamment de la valeur des informations concernées et des dommages subis, le texte d'incrimination affirmant ainsi une neutralité technologique qui présente l'avantage de pouvoir s'adapter aux évolutions des

¹ Article 323-1 du code pénal.

² Article 323-3 du code pénal.

³ Article 323-3-2 du code pénal.

⁴ Articles L. 851-6 et L. 852-1-II du code de la sécurité intérieure.

⁵ Articles L. 852-2, L. 852-3 et L. 855-1 A du code de la sécurité intérieure.

⁶ Article L. 853-2 du code de la sécurité intérieure.

⁷ Articles L. 822-3 et L. 863-2 du code de la sécurité intérieure.

⁸ Article L. 822-2 du code de la sécurité intérieure.

techniques de piratage¹. S'agissant du maintien frauduleux, on précisera que la Cour de cassation a confirmé qu'il s'agit d'une infraction autonome en 2015 dans l'affaire *Bluetouff* dans laquelle un pirate informatique a été condamné des chefs de maintien frauduleux et de vol d'informations en ayant eu accès sans fraude au système d'information de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) tout en ayant conscience de l'irrégularité de son maintien dans le système². En l'absence de cas d'espèce impliquant les services de renseignement, on retiendra l'affaire *Greenpeace c/ EDF* dont les faits datant de 2006 constituent une véritable opération de renseignement. Dans cette affaire définitivement jugée par la Cour de cassation en 2016³, un pirate informatique (ou « hacker ») a été condamné pour s'être introduit dans l'ordinateur du responsable de Greenpeace de l'époque pour y dérober des informations confidentielles dans le cadre d'une mission de renseignement privé de « veille stratégique » confiée à une société d'intelligence économique par de hauts responsables de la sécurité d'EDF⁴. Une condamnation similaire devrait être prononcée contre un agent des services de renseignement poursuivi pour avoir eu recours aux techniques prévues par le code de la sécurité intérieure précédemment mentionnées à des fins de surveillance pour le compte d'une entreprise privée. D'autant plus qu'une autorisation du Premier ministre et de la CNCTR sur ce type d'opération semble difficilement envisageable au regard des finalités légales des techniques de renseignement.

Depuis l'adoption de l'article 16 de la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme modifiant l'article 323-3 du code pénal, les faits d'espionnage et de vol d'informations stratégiques font l'objet des incriminations d'extraction, de détention, de reproduction et de transmission frauduleuses de données contenues dans un

¹ En ce sens, voir notamment O. de Maison Rouge, *Le droit du renseignement*, LexisNexis, 2016, p. 117 et 118 ; M. Quémener, *Les données personnelles à l'ère du numérique, Quelle protection sur le plan pénal ?*, op. cit..

² A ce sujet, voir E. A. Caprioli, *Condamnation pour maintien dans le STAD et vol de fichiers informatiques*, Communication Commerce électronique n° 9, Septembre 2015, comm. 74.

³ Cour de cassation, criminelle, Chambre criminelle, 26 janvier 2016, 13-83.127.

⁴ Sur cette affaire, voir notamment E. A. Caprioli, *Sécurité des systèmes d'information et espionnage informatique*, Communication Commerce électronique n° 5, Mai 2012, comm. 58 et J. Francillon, *Fraudes informatiques. Introductions frauduleuses de données et intrusions illégales dans un système informatique (piratage de Greenpeace)*, RSC 2013 p.559.

STAD. Cette modification législative a mis fin aux incertitudes jurisprudentielles et doctrinales sur le vol de données. En effet, l'infraction de vol prévue à l'article 311-1 avait été d'abord écartée pour le vol de données informatiques avant d'être retenue par la Cour de cassation¹, notamment dans l'affaire *Rose* sur le téléchargement de données confidentielles d'entreprise² et l'affaire *Bluetouff* précitée sur le piratage de l'ANSES³. L'extension de l'infraction de « soustraction frauduleuse de la chose d'autrui » aux données informatiques téléchargées à l'insu de leur propriétaire avait divisé la doctrine au regard des principes de légalité criminelle et d'interprétation stricte de la loi pénale⁴. On soulignera que l'intervention du législateur en 2014 avait été saluée par la DPR pour répondre aux opérations d'espionnage économique⁵. Ajoutons que les incriminations de l'article 323-3 pourraient renvoyer aux extractions ou transcriptions irrégulières déjà constatées par la CNCTR à l'occasion de son contrôle qui ne concernent pas la cible d'une autorisation de l'une des techniques de renseignement précédemment mentionnées. Toujours en ce qui concerne l'article 323-3, on relèvera que le tribunal de grande instance de Paris a retenu l'infraction d'introduction frauduleuse de données pour l'utilisation d'un programme « sniffer »⁶, c'est-à-dire un « *outil matériel ou logiciel dont l'objet est de capturer les trames transitant sur le réseau* » et qui permet de récupérer des informations sur les systèmes connectés voir des informations confidentielles si les données ne sont pas chiffrées⁷. Néanmoins, l'incrimination de l'article 323-3 ne semble pas être la plus adaptée à ce type de programme informatique de surveillance qui n'a pas pour vocation

¹ A ce sujet, voir notamment O. de Maison Rouge, *Le droit du renseignement*, op. cit., p. 120 à 123.

² Tribunal de grande instance de Clermont-Ferrand, 26 septembre 2011, *Stés X. et Y. c/ Mme Rose*.

³ Cass. crim., 20 mai 2015, n° 14-81.336, *Bluetouff*.

⁴ Sur la controverse doctrinale, voir notamment O. de Maison Rouge, *Le droit du renseignement*, op. cit., p. 120 à 123 ; J. Francillon, « *Infractions relevant du droit de l'information et de la communication* », *Revue de science criminelle et de droit pénal comparé*, vol. 4, no. 4, 2015, pp. 877-888 ; E. A. Caprioli, *Condamnation pour maintien dans le STAD et vol de fichiers informatiques*, *Communication Commerce électronique* n° 9, Septembre 2015, comm. 74.

⁵ Cf. J. -J. Urvoas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, op. cit., p. 43.

⁶ Tribunal de grande instance de Paris, 16 décembre 1997, n° 9733070015, *Ministère public c/ Golovanivsky*.

⁷ Voir à ce sujet Glossaire de l'ANSSI, *Renifleur (Sniffer)*, <https://www.ssi.gouv.fr/particulier/glossaire/r/>.

principale d'introduire frauduleusement des données¹, l'intrusion informatique incriminée à l'article 323-1 pouvant être la qualification la plus pertinente selon nous.

Incriminant de manière suffisamment large la détention et le trafic de moyens de piratage informatique, on rappellera que l'article 323-3-1 du code pénal consacre une infraction obstacle ayant pour objectif la prévention des cyberattaques et de la prolifération des logiciels malveillants². L'infraction pourrait être envisagée dans le cas d'une détention ou d'une mise à disposition sans motif légitime d'un dispositif technique de renseignement par un agent des services de renseignement. A l'appui de notre hypothèse, citons une affaire jugée par la Cour de cassation en 2018 impliquant la détention et l'usage d'un « *Keylogger* » (ou « capteur clavier, enregistreur de frappes » selon le glossaire de l'ANSSI qui considère ce type de logiciel malveillant comme un logiciel espion) par un médecin contractuel au CHU de Nice pour accéder, par vol de mots de passe, aux messageries électroniques de deux collègues afin de pouvoir préparer sa défense sur un litige futur avec un professeur de l'hôpital³. La Cour de cassation a retenu l'infraction de détention sans motif légitime d'un logiciel d'espionnage conformément à l'objectif de cette infraction obstacle pour condamner le prévenu qui n'avait pas encore utilisé l'ensemble des logiciels malveillants à sa disposition⁴. La haute juridiction judiciaire a également condamné le médecin espion pour intrusion informatique réprimée à l'article 323-1 puisque l'utilisation d'un « *Keylogger* » a permis de démontrer l'accès frauduleux à la messagerie électronique de ses collègues par le vol de leurs mots de passe mais aussi une surveillance disproportionnée au regard des règles de collecte privée de preuves pour les droits de la défense⁵. Sur ce dernier point, on ne peut qu'admettre la solution de la Cour de cassation en l'espèce même s'il peut être soutenu

¹ En ce sens, voir *Introduction d'un programme « sniffer »*, Revue Lamy droit des affaires, N° 4, 1er avril 1998.

² En ce sens, voir M. Daury-Fauveau, *Fasc. 20 : ATTEINTES AUX SYSTÈMES DE TRAITEMENT AUTOMATISÉ DE DONNÉES – C. pén., art. 323-1 à 323-8*, JurisClasseur Pénal Code, 22 octobre 2019.

³ Cass. crim., 16 janvier 2018, n° 16-87.168.

⁴ Sur ce point, voir E. Dreyer, *Accès frauduleux, indirect, mais certain, dans un STAD et détention du matériel le permettant*, RSC 2018, p.701.

⁵ Cf. Ibid. et E. A. Caprioli, *Usage frauduleux d'un logiciel keylogger*, Communication Commerce électronique n° 4, Avril 2018, comm. 30.

théoriquement que la détention et l'utilisation d'un logiciel espion pourraient se justifier selon la rédaction de l'article 323-3-1 et la jurisprudence de la Cour de cassation sur la collecte privée de preuve pour assurer les droits de la défense¹. En revanche, cette solution nous semble ne pas pouvoir être admise pour un agent qui détiendrait et utiliserait un logiciel espion d'un service de renseignement pour la défense de ses droits en justice.

En ce qui concerne les peines, les infractions contre les STAD ont été considérés comme un outil répressif très utile pour lutter contre le cyberespionnage visant la France par le législateur. Ainsi, la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité a consacré une circonstance aggravante pour chacune des infractions prévues aux articles 323-1 à 323-3 lorsque le STAD visé par les cybercriminels est un traitement automatisé de données personnelles mis en œuvre par l'Etat. On peut comprendre que la loi de 2012 visait la protection de l'identité des personnes physiques, mais un élargissement de la circonstance aggravante à l'ensemble des traitements automatisés de données mis en œuvre par l'Etat pourrait s'avérer tout aussi utile pour protéger des informations stratégiques détenues par les administrations françaises, notamment lorsque l'ANSSI ne cesse d'alerter sur la croissance de la cybercriminalité et sur la persistance et la complexification des campagnes de cyberespionnage². Plus encore, la loi relative au renseignement du 24 juillet 2015 a multiplié par deux les sanctions pécuniaires suite aux recommandations des membres de la DPR³. Cette initiative du législateur de 2015 a pu sembler constitutionnellement critiquable au regard du respect du principe de proportionnalité des délits et des peines ou du risque de cavalier législatif mais aucune censure n'a été prononcée par les Sages lors de l'examen du texte⁴. Le rehaussement des peines pécuniaires ne manque pas, à notre sens, de légitimité face à l'augmentation des cyberattaques.

¹ Cass. Ass. Plén., 22 décembre 2023, n° 20-20.648.

² Cf. ANSSI, *Rapports d'activité 2019, 2020 et 2021* et ANSSI, *Panorama de la menace informatique 2021*, 9 mars 2022, p. 9 et suivantes.

³ Cf. Proposition n°2 du rapport de la DPR pour l'année 2014.

⁴ En ce sens, voir E. Chauvin et F. Vadillo, *La loi n° 2015-912 du 24 juillet 2015 « relative au renseignement » au secours de la protection pénale des systèmes de données*, Revue Lamy Droit de l'Immatériel, 1^{er} janvier 2016, 122.

Notons enfin que la commission des délits d'atteintes aux STAD en matière de renseignement peuvent impliquer d'autres infractions moins spécifiques à la cybercriminalité. Tout d'abord, on mentionnera les infractions d'espionnage ou de trahison¹ qui concernent la livraison à une puissance étrangère ou une organisation étrangère de données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la Nation ainsi que la collecte de ces données ou fichiers en vue de les livrer à une puissance étrangère². En revanche, l'espionnage entre entreprises concurrentes ne relèverait pas de l'espionnage au sens strict du Code pénal selon l'affaire *Michelin* de 2010³, ce qui suscite des critiques. Certains spécialistes du renseignement et de l'intelligence économique considèrent que la notion classique de l'espionnage ne correspond plus à la réalité du cyberespionnage désormais largement pratiqué dans le domaine économique, revêtant alors une dimension sécuritaire non négligeable pour l'Etat⁴. La DPR elle-même avait également souligné l'intérêt pour le renseignement d'Etat de la montée en puissance de l'espionnage des entreprises dans son rapport d'activité pour l'année 2014⁵. D'ailleurs, on rappellera que les techniques de renseignement peuvent être autorisées pour la finalité relative à la défense et à la promotion des intérêts économiques, industriels et scientifiques majeurs de la France et la « contre-ingérence étrangère » sous le contrôle vigilant de la CNCTR⁶. A ce sujet, on ajoutera que le recours aux techniques de renseignement dans le domaine économique présente un risque particulier de détournement abusif des moyens

¹ Selon l'article 411-1 du Code pénal, les infractions d'espionnage sont qualifiées de trahison lorsqu'elles sont commises par un français ou un militaire au service de la France.

² Articles 411-6 à 411-8 du code pénal.

³ Dans cette affaire, un salarié de Michelin a été condamné le 21 juin 2010 par le Tribunal Correctionnel de Clermont-Ferrand pour avoir tenté de vendre des informations confidentielles de l'entreprise à sa société concurrente Bridgestone. Les juges ont retenu la qualification d'abus de confiance mais pas celle de livraison à une entreprise étrangère de renseignements dont l'exploitation et la divulgation sont de nature à porter atteinte aux intérêts fondamentaux de la Nation en raison de l'intérêt purement économique du cas d'espionnage.

⁴ Voir sur ce point J. Mafart, *Espionnage*, Hugues Moutouh éd., Dictionnaire du renseignement. op. cit., pp. 348-359 et C. Harbulot, « *Étude de cas - L'affaire Michelin* », Manuel d'intelligence économique. Presses Universitaires de France, 2012, pp. 319-326.

⁵ Cf. J. -J. Urvoas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, op. cit., p. 37.

⁶ Cf. CNCTR, 7^{ème} rapport annuel (2022), p. 35.

de sécurité nationale et donc d'atteintes illégitimes à des systèmes numériques d'entreprises et à leurs données confidentielles.

Participant également à la sauvegarde des intérêts fondamentaux de la Nation selon le Conseil constitutionnel¹, la protection pénale du secret de la défense nationale², qui s'étend notamment aux « *réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès* »³, peut être invoquée dans la commission d'une infraction aux STAD ayant pour conséquence la compromission d'un élément classifié par un agent du renseignement⁴ ou par un espion tiers⁵. Cette infraction pourrait être caractérisée notamment dans le cas d'une compromission d'une autorisation de technique de renseignement par un agent ou dans le cas d'un trafic portant sur un appareil ou un dispositif technique de renseignement. Notons que le dispositif pénal mis en place est très dissuasif et indispensable au contre-espionnage, même s'il offre une large protection au secret de la défense nationale pouvant constituer un obstacle à des procédures judiciaires telles qu'une saisie-contrefaçon en matière de création de logiciels⁶, au travail journalistique sur les activités du renseignement⁷ ou à l'ouverture des données en matière de sécurité et de défense⁸.

Ensuite, il pourrait être envisagé de retenir le délit d'abus de confiance de l'article 314-1 du code pénal qui a été plusieurs fois invoqué en matière d'espionnage économique dans des cas de détournement de données confidentielles d'entreprises⁹. Cependant, on soutiendra que ce délit ne trouve pas

¹ Décisions n° 2011-192 QPC du 10 novembre 2011, *Mme Ekaterina B., épouse D., et autres* et n° 2015-713 DC du 23 juillet 2015, *Loi relative au renseignement*.

² Notons qu'au sens du code de la défense, le secret de la défense nationale concerne, plus largement, les éléments intéressant la sécurité nationale.

³ Article 413-9 du code pénal.

⁴ Article 413-10 du code pénal.

⁵ Article 413-11 du code pénal.

⁶ C. cass., civ. 1^{ère}, 21 mars 2006, n° 05-13.302.

⁷ En ce sens, voir B. Michalon et B. Puybureau, « *Secret d'État et secret des sources : comment des journalistes enquêtent-ils sur le renseignement en France ? Entretiens avec Jean Guisnel et Jacques Follorou* », *Cultures & Conflits*, vol. 114-115, no. 2-3, 2019, pp. 227-262.

⁸ En ce sens, voir B. Warusfel, « *Enjeux et limites de l'ouverture des données en matière de sécurité et de défense* », *Revue française d'administration publique*, vol. 167, no. 3, 2018, pp. 551-564.

⁹ Sur le délit d'abus de confiance et l'espionnage, voir O. de Maison Rouge, *Le droit du renseignement*, op. cit., p. 118 à 120 ; A. Mendoza-Caminade, *La protection pénale des biens*

à s'appliquer au renseignement d'Etat puisque que le détournement d'un dispositif technique ou de données de renseignement est appréhendé par les atteintes aux STAD et les infractions relatives à l'espionnage et au secret de la défense nationale.

En revanche, l'incrimination prévue à l'article 226-13 du code pénal qui réprime la révélation d'une information non classifiée à caractère secret par une personne qui en est dépositaire (secret professionnel) pourrait être retenue contre un agent du renseignement portant abusivement atteinte à un STAD. Le Conseil constitutionnel a d'ailleurs confirmé implicitement l'application de l'article 226-13 aux agents de renseignement qui révéleraient les renseignements ou données collectés par les techniques de renseignement¹. Il devrait en être de même concernant les secrets d'affaires en cas de pénalisation de leur compromission, ce qui soulève des débats². Depuis la loi n° 2018-670 du 30 juillet 2018 de transposition de la directive européenne 2016/943/UE du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulguées contre l'obtention, l'utilisation et la divulgation illicites, le secret des affaires fait l'objet d'une protection juridique civile, le législateur ayant refusé d'introduire une protection pénale³ en se fondant sur les interventions du Conseil d'Etat qui a considéré que la définition retenue du secret des affaires « se prêtait mal au domaine pénal »⁴. Néanmoins, il a pu être soutenu qu'une telle protection est non seulement nécessaire pour répondre au droit pénal français qui est insuffisant mais pour faire face à la montée en puissance de l'espionnage économique, notamment dans une société de l'information⁵. Inversement, certains

incorporels de l'entreprise : vers l'achèvement de la dématérialisation du délit ?, Recueil Dalloz 2015 p.415 ; G. Beaussonie, *La dématérialisation de l'abus de confiance*, AJ Pénal 2017 p.215 ; S. Detraz, *Application de l'abus de confiance à des informations*, La Semaine Juridique Edition Générale n° 11-12, 12 mars 2012, act. 322 ; E. A. Caprioli, *Condamnation pour abus de confiance d'un salarié ayant détourné des données professionnelles à des fins personnelles*, Communication Commerce électronique n° 2, Février 2015, comm. 17.

¹ Décision n° 2015-713 DC du 23 juillet 2015, *Loi relative au renseignement* (considérant 35).

² En ce sens, voir C. Harbulot, *L'intelligence juridique et le droit des secrets d'affaires*, Manuel d'intelligence économique, op. cit., pp. 305-318.

³ Cf. R. Gauvain, *Rapport sur la proposition de loi portant transposition de la directive du Parlement et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués contre l'obtention, l'utilisation et la divulgation illicites*, Assemblée nationale, 21 mars 2018, p. 8, 11 et 12.

⁴ Voir les avis du Conseil d'Etat du 31 mars 2011, n° 384892, et du 15 mars 2018, n° 394422.

⁵ En ce sens, voir C. Harbulot, *L'intelligence juridique et le droit des secrets d'affaires*, Manuel d'intelligence économique, op. cit., pp. 305-318 et E. Daoud, E. Mercinier et J. Neiman, *Loi du 30 juillet 2018 relative à la protection du secret des affaires : un apport utile mais insuffisant*, Revue Lamy droit des affaires, N° 147, 1er avril 2019.

auteurs s'accordent avec les arguments du législateur et du Conseil d'Etat pour soutenir qu'une infraction spécifique n'est pas nécessaire¹, notamment en ce qui concerne les infractions déjà existantes sur les atteintes aux secrets, les appropriations frauduleuses d'informations (vol de données, escroquerie, abus de confiance) ou encore les infractions contre les STAD qui peuvent s'appliquer. Le débat, plus politique que juridique, reste ouvert puisque la directive européenne de 2016 autorise les Etats membres à prendre des mesures pénales. Pour notre part, il est vrai que l'instauration d'un délit spécifique de violation du secret des affaires permettrait de disposer d'un outil juridique dissuasif contre les ambitions d'espionnage économique et, surtout, contre les intentions de divulgation des secrets postérieurement à leur appropriation frauduleuse. En effet, la majorité des infractions qui peuvent être invoquées concernent davantage les procédés frauduleux permettant d'accéder au secret que la divulgation du secret lui-même.

Une autre violation du secret sanctionnée par le code pénal qui peut accompagner une atteinte à un STAD doit être invoquée, l'atteinte au secret des correspondances électroniques. Cette dernière constitue le second type d'infraction cybercriminelle particulièrement applicable à l'usage des moyens numériques légalisés de renseignement.

2. L'atteinte au secret des correspondances électroniques

Parmi les dispositions du code de la sécurité intérieure relatives aux techniques de renseignement, celles portant sur les interceptions de sécurité² ne font aucun doute sur le risque de requalification pénale en atteinte au secret des correspondances électroniques en cas d'abus. A titre d'exemple, cette qualification cybercriminelle pourrait, là encore, trouver à s'appliquer à l'irrégularité déjà constatée par la CNCTR concernant les extractions ou transcriptions réalisées qui ne concernent pas la cible d'une autorisation d'une interception de sécurité.

De manière expresse, l'article L. 851-7 du code de la sécurité intérieure rappelle que la mise en œuvre des accès aux données de connexion doit être réalisée dans le respect de l'article 226-15 du code pénal qui sanctionne spécifiquement

¹ En ce sens, voir E. Raschel, *Réflexion sur la pénalisation de la violation du secret des affaires*, Dalloz IP/IT 2018 p.675 et O. de Maison Rouge, *Le secret des affaires : la reconnaissance juridique d'un droit de l'information protégée*, Dalloz IP/IT 2018 p.659.

² Articles L. 852-1 à L. 852-3 du code de la sécurité intérieure.

l'atteinte au secret des correspondances électroniques et donc l'accès à des données de contenu par ce type de techniques.

Afin de démontrer l'application de l'infraction d'atteinte au secret des correspondances électroniques aux interceptions de sécurité et aux accès aux données de connexion, on s'appuiera sur des éléments de précisions sur les évolutions de la notion de correspondance électronique et sur sa protection juridique auxquelles la loi du 10 juillet 1991 encadrant les premières techniques de renseignement a pu contribuer.

Communication entre des personnes, une correspondance est facilement identifiable dans le système postal qui concerne les échanges de lettres écrites. En revanche, face aux évolutions des technologies de l'information et de la communication, il s'est avéré plus difficile d'identifier juridiquement une correspondance parmi la diversité des communications électroniques (téléphone, télévision, internet et réseaux sociaux par exemple). D'autant plus qu'il n'existe pas de définition du terme « correspondance » en droit. Néanmoins, la doctrine a pu préciser quelles sont les communications électroniques qui peuvent être entendues comme des correspondances électroniques. Ainsi, pour la CNCIS, chargée du contrôle de l'application de la loi du 10 juillet 1991 relative au secret des correspondances électroniques, cette notion concernait des communications électroniques individualisables, peu importe les moyens techniques utilisés en référence aux communications mobiles hertziennes¹. Dans le même sens, on retiendra également l'analyse du Professeur Didier Truchet qui démontre que :

« Il y a correspondance (ou correspondance privée) dès lors qu'un message est adressé à un (ou des) destinataire(s) désigné(s) nommément par celui qui l'émet et à lui (ou eux) seul(s). Le législateur ne l'a pas définie, mais il l'a systématiquement distinguée de la communication, comme on l'a vu avec les citations de la loi audiovisuelle de 1986 et de la LCEN »².

De manière négative, une correspondance électronique n'est pas : une communication audiovisuelle au sens de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle ; une communication électronique mise à

¹ Cf. CNCIS, 20^{ème} rapport d'activité 2011-2012, p. 40 et suivantes.

² Cf. D. Truchet, *Correspondance et communication*, Recueil Dalloz 2014 p.2353.

disposition du public au sens de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication ; une communication au public en ligne au sens de la loi n° 2004-575 du 21 juin 2004 pour la confiance pour l'économie numérique (LCEN). De manière positive, une correspondance électronique est un message entre personnes nommément désignées. Dès lors, on pourrait penser que les correspondances électroniques concernent des communications privées qui bénéficieraient de la protection du droit au respect de la vie privée. En réalité, il a été fait le choix de transposer le type de protection du système postal au domaine numérique¹, c'est-à-dire de considérer les correspondances échangées entre les individus comme relevant d'un droit au secret². Ce type de protection a été reconnu par différents textes internationaux et européens ainsi qu'étendu aux correspondances électroniques, notamment dans des textes spécifiques comme la Constitution de l'UIT du 22 décembre 1992 ou encore la directive européenne n° 2002/58/CE « vie privée et communications électroniques »³.

En droit français, les correspondances font également l'objet d'une protection autonome par le droit au secret. Ainsi, la loi précitée du 10 juillet 1991 a consacré positivement ce droit au secret dans le domaine des télécommunications. Et, le code pénal consacre une infraction autonome d'atteinte au secret de toutes les correspondances, y compris électroniques, indépendamment du caractère privé ou non de ces dernières, ce qui implique que l'infraction peut être caractérisée même en l'absence d'atteinte à la vie privée de la victime⁴. En effet, selon l'article 226-15 du code pénal, qui punit d'un an d'emprisonnement et de 45 000 euros d'amende la violation du secret des correspondances, l'atteinte est matériellement constituée en cas d'interception, de détournement, d'utilisation ou de divulgation des correspondances électroniques

¹ En ce sens, voir notamment L. Castex, *Le secret de la correspondance en ligne : dans le sillon des lettres missives*, Revue Lamy Droit de l'Immatériel, N° 137, 1er mai 2017.

² En ce sens, la doctrine cite généralement l'ouvrage F. Gény, *Des droits sur les lettres missives*, Sirey, 1911. Voir également L. Marino, *Le secret des correspondances, tel un satellite...*, La Semaine Juridique Edition Générale n° 6, 4 février 2009, II 10022.

³ Cf. S. Laurent et M. Kheloufi, *Les normes juridiques internationales applicables aux communications individuelles : les enjeux du « secret des correspondances » et des « données personnelles »*, Programme « UTIC France-Europe », IRM, Université de Bordeaux, Livrable n° 7 v. 10, 28 février 2018.

⁴ En ce sens, voir D. Truchet, *Correspondance et communication*, Recueil Dalloz 2014 p.2353 et L. Castex, *Le secret de la correspondance en ligne : dans le sillon des lettres missives*, op. cit..

ou encore lorsqu'il est procédé à l'installation d'un appareil d'interception. Sur l'élément moral de l'infraction, l'intéressé doit avoir commis de mauvaise fois la violation du secret. En revanche, lorsque la violation est commise par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ou encore par un agent des opérateurs de télécommunications, elle doit être commise en violation des cas prévus par la loi selon l'article 432-9 du même code qui augmente la peine encourue à trois ans d'emprisonnement.

Par ailleurs, il nous apparaît opportun de souligner que si le secret des correspondances électroniques fait l'objet d'une protection pénale distincte du droit au respect de la vie privée, il n'en demeure pas moins que cette atteinte constitue une intrusion dans l'intimité des personnes au sens de l'article 9 du code civil¹. Lorsque les interceptions constituent une mesure de surveillance individuelle, l'atteinte au secret des correspondances aboutira donc à une atteinte à la vie privée. Cette remarque peut également s'appliquer aux infractions contre les données personnelles qui font l'objet d'incriminations spécifiques mais qui doivent être rapprochées avec le droit au respect de la vie privée au regard de l'impact des traitements des données personnelles pour les personnes concernées, voir même avec la lutte contre les discriminations en ce qui concerne le principe d'interdiction du traitement des données dites « sensibles »².

3. Les atteintes aux données personnelles

Dès l'adoption de la « loi Informatique et libertés » de 1978, le législateur a prévu deux types de sanctions des atteintes aux données personnelles et aux droits de personnes concernées : les sanctions relevant du contrôle de la CNIL et les sanctions pénales relevant du contrôle du juge judiciaire. Ces dernières ont été introduites dans le code pénal dans une section autonome relevant des infractions contre les personnes et renforcée depuis la loi n° 2004-801 du 6 août relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment par une extension des incriminations des articles

¹ En ce sens voir, S. Canas, L'influence de la fondamentalisation du droit au respect de la vie privée sur la mise en œuvre de l'article 9 du code civil, Nouveaux Cahiers du Conseil constitutionnel n°48, Dossier : Vie privée, Juin 2015, p. 47 à 58.

² En ce sens, voir notamment J. Le Clainche et D. Le Métayer, *Données personnelles, vie privée et non-discrimination : des protections complémentaires, une convergence nécessaire*, Revue Lamy Droit de l'Immatériel, N° 90, 1er février 2013.

226-16 à 226-24 du code pénal et un rehaussement uniforme des peines à cinq ans d'emprisonnement et 300 000 euros d'amende¹.

Bien qu'il apparaissait nécessaire de protéger pénalement les personnes et les libertés individuelles contre les dangers de la numérisation, l'effectivité du droit pénal en matière de protection des données personnelles a été largement critiqué par la doctrine qui a régulièrement dénoncé les faiblesses du contentieux pénal par rapport à la montée en puissance du contrôle exercé par la CNIL, allant jusqu'à soulever la question de la dépénalisation des atteintes aux données personnelles sans pour autant que la doctrine se prononce en ce sens².

Malgré une situation qui semble inchangée depuis la réforme de 2004, la pénalisation des atteintes aux données personnelles conserve toute sa pertinence en ce qu'elle a vocation particulière à sanctionner des comportements délictuels alors que les sanctions de la CNIL concernent davantage des mauvaises pratiques dans les administrations et les entreprises, même s'il convient de souligner que le contrôle exercé par l'autorité administrative indépendante permet de détecter des délits. Pour notre part, on soutiendra que le dispositif pénal est même indispensable à la lutte contre la cybercriminalité ainsi que pour protéger les internautes contre leur fichage et leur profilage clandestin³. A ce titre, il constitue l'un des outils répressifs les plus importants contre les abus du renseignement numérique, il suffit de se référer à certaines incriminations et à la jurisprudence pour s'en convaincre.

Tout d'abord, en matière de collecte, l'article 226-18 code pénal condamne ainsi « *le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite* ». Non seulement cette infraction peut théoriquement

¹ A ce sujet, voir J. -F. Seuvic, *Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, article 226-16 à 226-24 du Code pénal*, RSC 2004 p.916.

² Sur les critiques relatives aux infractions contre les données personnelles, voir notamment J. Francillon, *Infractions relevant du droit de l'informatique. La loi Informatique, fichiers et libertés du 6 janvier 1978 à l'épreuve de la jurisprudence pénale*, RSC 1996 p.676 ; A. Lepage, *Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel*, Droit pénal n° 3, mars 2005, étude 5 ; J. Frayssinet, *La loi relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ?*, Revue Le Lamy Droit de l'immatériel, N° 9, 1er octobre 2005 ; J. Frayssinet, « *La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois* », LEGICOM, vol. 42, no. 1, 2009, pp. 23-33.

³ En ce sens, voir E. Derieux, *Internet et protection des données personnelles*, Revue Le Lamy Droit de l'immatériel, N° 38, 1er mai 2008 ou encore M. Quémener, *Les données personnelles à l'ère numérique Quelle protection sur le plan pénal ?*, op. cit..

être retenue pour l'ensemble des moyens numériques de renseignement légalisés et utilisés dans la surveillance des personnes, mais plus encore elle a pu servir de fondement dans l'affaire des « *fadettes du Monde* » de 2010 pour condamner l'ancien directeur de la DCRI, Bernard Squarcini, à 8 000 euros d'amende¹ pour l'utilisation abusive des dispositions relatives à la surveillance hertzienne de la loi du 10 juillet 1991 pour obtenir des relevés téléphoniques d'un journaliste afin d'identifier ses sources dans l'affaire Bettencourt². Cette affaire nous démontre la réalité du risque pénal du recours à des techniques de renseignement légalisées.

On ajoutera que l'infraction de l'article 226-18 peut se combiner avec des infractions contre les STAD qui viseraient les traitements de données personnelles notamment mis en œuvre par l'Etat, confirmant alors l'utilité du droit pénal des données personnelles en matière de lutte contre la cybercriminalité et l'espionnage. En effet, on ne peut que souscrire à l'affirmation de la Professeure Agathe Lepage selon laquelle « *ces deux catégories d'incriminations permettent le cas échéant d'assurer, en cas de fraude informatique, la protection de l'être et de l'avoir* »³.

Ensuite, en ce qui concerne l'exploitation des données personnelles, plusieurs infractions nous apparaissent intéresser l'usage des techniques de renseignement. On mentionnera particulièrement les infractions sanctionnant le fait de conserver des données personnelles au-delà du délai légal autorisé⁴ et le fait de détourner des données personnelles pour une finalité autre que celle qui a justifié leur collecte et leur traitement⁵ car ces deux infractions ont notamment été invoquées contre des agents de renseignement. Dans le cadre des exploitations de données et des fichiers de police et de renseignement, plusieurs condamnations pour atteintes aux données personnelles ont été prononcées contre des fonctionnaires du renseignement, notamment dans la pratique de la « tricoche » qui consiste à consulter abusivement des fichiers et, dans les cas les plus graves, à

¹ TGI de Paris, 8 avril 2014, n° 12339000279.

² Cf. Le Monde, *Fadettes du « Monde » : Squarcini condamné à 8000 euros d'amende*, 8 avril 2014.

³ Cf. A. Lepage, *Un an de droit pénal du numérique (oct. 2016 – sept. 2017)*, Droit pénal n° 12, décembre 2017, chron. 11.

⁴ Article 226-20 du code pénal.

⁵ Article 226-21 du code pénal.

vendre des informations à des tiers¹. Par exemple, un gardien de la paix en poste aux RG du Var a été jugé coupable du délit de détournement du fichier des infractions constatées (STIC) et du fichier national automobile (FNA) à des fins personnelles et pour avoir communiquées des données confidentielles à un tiers². Dans l'affaire plus médiatique *Haurus* de 2021, le juge pénal a écroué un agent de la DGSi ayant vendu sur le « darknet » des données issues des fichiers de police auxquels il avait accès et donc pour détournement des finalités des fichiers concernés³. A ces cas d'espèce, on ajoutera que parmi les catégories d'irrégularités exposées par la CNCTR dans ses rapports annuels d'activités, on retiendra notamment qu'en matière d'atteinte aux données personnelles, les dépassements de la durée légale de conservation des transcriptions et extractions semblent constituer en pratique les faits incriminés par l'article 226-20 du code pénal et le détournement de finalité des transcriptions et extractions pourrait être, quant à lui, qualifié de détournement de finalité au sens de l'article 226-21 du même code.

Il pourrait également être retenu la création de traitements clandestins de données personnelles normalement soumis à des formalités préalables⁴ et les traitements illégaux de données personnelles sensibles ou concernant des infractions, condamnations ou des mesures de sûreté⁵. Sur l'application de ces deux infractions, on retiendra pour notre étude qu'elles condamnent la constitution, à l'insu des personnes concernées et de la CNIL, de « *ce qu'il est possible d'appeler une sorte de casier judiciaire privé* », pour reprendre les termes du commissaire du gouvernement, Francis Donnat, à propos de l'affaire *M. Mechri* jugée en 2004 par le Conseil d'Etat⁶ sur la compétence de la CNIL pour se prononcer sur un traitement de données concernant des condamnations civiles ou pénales par une entreprise privée⁷. Mais plus encore, relevons que les juges de la

¹ A ce sujet, voir D. Batho et J. A. Bénisti, *Rapport d'information sur les fichiers de police*, Assemblée nationale, 24 mars 2009, p. 143 à 147 et V. Gautron, *Usages et mésusages des fichiers de police : la sécurité contre la sûreté ?*, op. cit..

² Cass. crim., 5 février 2013, n° 12-80.573.

³ Cour d'appel de Versailles, 26 novembre 2021, n° 21/03302.

⁴ Article 226-16 du code pénal.

⁵ Article 226-19 du code pénal.

⁶ Conseil d'Etat, 28 juillet 2004, n° 262851.

⁷ Cf. F. Donnat, *Contrôle des fichiers contenant des informations pénales ou civiles individuelles*, AJDA 2004 p.2228.

cour d'appel de Bourges ont étendu la qualification de l'article 226-19 sur les « fichiers d'infractions » à une « liste noire de notaires », un traitement de données personnelles dénonçant certains professionnels ayant commis des abus, publiée sur internet par une association de défense des victimes de notaires sans avoir été déclarée à la CNIL¹. Si cette solution témoigne de la volonté d'encadrer le fichage privé de particuliers ou professionnels soupçonnées ou jugées malveillants, il est vrai qu'elle entre en contradiction avec le principe d'interprétation stricte de la loi pénale². Néanmoins, on supposera que la solution retenue par les juges du fond s'appuyait sur des considérations tenant au cas d'espèce, une condamnation pénale d'une « liste noire » devant, selon nous, être principalement fondée, en droit, sur l'article 226-16 relatif au fichage clandestin et l'article 226-22 qui réprime la divulgation de données personnelles portant atteinte à la réputation ou à la vie privée des personnes concernées.

Pour aller plus loin, les divulgations illicites de données et de fichiers de sécurité peuvent donner lieu à des condamnations d'agents du renseignement pour violation du secret professionnel. La Cour de cassation a clairement affirmé que le contenu des fichiers de police est secret et que leur utilisation par les fonctionnaires de police est soumise au secret professionnel, ce qui impliquait qu'un fonctionnaire des RG ayant révélé à un tiers des informations contenues dans le FPR pouvait faire l'objet d'une poursuite pour violation du secret professionnel³.

¹ CA Bourges, 2e ch., 11 janv. 2007, *Gisèle N., Ligue européenne de défense des victimes de notaires c/ Ministère public*.

² En ce sens, voir J. Le Clainche, *Liste noire de notaires : dernier acte ?*, Revue Lamy Droit de l'Immatériel, N° 30, 1er août 2007.

³ Cass. crim., 7 novembre 1996, n° 96-80.655.

4. Les atteintes à la vie privée par captations techniques de paroles, d'images ou de localisation

A l'instar de l'atteinte au secret des correspondances électroniques, l'infraction prévue à l'article 226-1 du code pénal réprime sans ambiguïté l'usage illégal de certaines techniques de renseignement en sanctionnant d'un an d'emprisonnement et de 45 000 euros d'amende :

« le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci ».

D'autant plus que, dans l'affaire de la « cellule antiterroriste de l'Elysée », la chambre criminelle de la Cour de cassation a eu l'occasion d'affirmer expressément l'application de l'article 226-1 mais aussi, notons-le, celui de l'article 226-19 visant les traitements sur des données sensibles au renseignement en condamnant des militaires de la gendarmerie, un commissaire de la DST, le directeur du GIC et le directeur du cabinet du Premier ministre en charge des autorisations d'interceptions de sécurité entre 1984 et 1986 ainsi qu'un ancien membre du GIGN pour avoir notamment intercepté et enregistré des conversations téléphoniques d'un avocat et d'un journaliste de manière manifestement illégale¹. Là encore, ce scandale impliquant la présidence de la République de François Mitterrand illustre le risque réel de l'abus du renseignement numérique et l'application effective du droit pénal du numérique à ce type d'activité régalienn².

¹ Voir Cass. crim., 4 mars 1997, n° 96-84.773 et Cass. crim., 30 septembre 2008, n° 07-82.249.

² Pour en savoir plus sur le scandale des écoutes de l'Elysée, voir par exemple Y. Bonnet et P. Krop, *Les Grandes Oreilles du Président*, Presse de la Cité, octobre 2004.

Soulignons que depuis la loi relative au renseignement de 2015, il convient, selon nous, de retenir particulièrement les qualifications de l'article 226-1 du code pénal pour les techniques de sonorisation ou de captation d'images prévues aux articles L. 853-1 du code de la sécurité intérieure ou pour la géolocalisation par balisage prévue à l'article L. 851-5 du même code.

Notons qu'en ce qui concerne les éléments de l'infraction, la nature clandestine du délit combinée à ses éléments tenant à l'intrusivité a pu entraîner une interprétation souple de l'atteinte à l'intimité de la vie privée par la haute juridiction judiciaire. Ainsi, la Cour de cassation¹ a pu confirmer sur le fondement de l'article 226-1 la culpabilité d'un journaliste ayant pu, tel un véritable agent secret, filmer des jurés lors d'une délibération de cour d'assises grâce à un reflet permettant de voir l'intérieur de la salle dans laquelle le jury était réuni². En matière de sonorisation, la jurisprudence aussi bien pénale que civile de la Cour de cassation semble admettre une certaine présomption d'atteinte à l'intimité de la vie privée, c'est-à-dire qu'il n'est pas nécessaire d'apprécier les propos enregistrés, en fonction de la conception, de l'objet et de la durée du dispositif de captation. Dans le cadre de l'affaire des enregistrements illicites de Mme Liliane Bettencourt réalisés par son majordome, tel cette fois-ci un « agent double », les juges du quai de l'Horloge ont caractérisé l'atteinte à l'intimité de la vie privée en relevant que les enregistrements clandestins ont duré pendant une année au domicile même de la victime³. Cependant, on relèvera que la chambre criminelle de la Cour de cassation a récemment considéré que la clandestinité n'est pas nécessairement inhérente au délit prévu à l'article 226-1. En effet, elle a jugé en 2020⁴ que l'enregistrement de la parole ou de l'image d'une personne placée en garde à vue par une équipe de télévision est susceptible de constituer une atteinte à l'intimité de sa vie privée alors même que la personne concernée sait qu'elle est

¹ Cass. crim., 16 févr. 2010, n° 09-81.492.

² Sur cette affaire, voir notamment A. Lepage, *Interprétation pas tout à fait stricte de l'article 226-1 du Code pénal*, Communication Commerce électronique n° 6, Juin 2010, comm. 66.

³ Sur la présomption d'atteinte à l'intimité de la vie privée en fonction du dispositif de captation mis en place et l'affaire *Bettencourt*, voir notamment A. Lepage, *Affaire Bettencourt c/ Mediapart : suite et fin ?*, Communication Commerce électronique n° 3, Mars 2015, comm. 23.

⁴ Cass. crim., 21 avr. 2020, n° 19-81.507.

filmée mais qu'elle n'est pas en mesure de s'opposer à l'enregistrement litigieux¹. En définitive, la répression du délit nous semble principalement reposer sur l'appréciation de l'intrusivité du dispositif de captation (conception, objet et durée). A priori, les techniques de renseignement de sonorisation, de captation d'images ou de géolocalisation par balisage devraient caractériser aisément une intrusivité suffisamment grave pour les juges.

Il convient de compléter le dispositif répressif de l'article 226-1 avec les articles 226-2 et 226-3 du code pénal qui sanctionnent respectivement ce qui s'apparenterait à « une forme spéciale de recel » de l'espionnage audiovisuelle de la vie privée² et le trafic illicite de moyens techniques d'interception de correspondances et de captation de paroles, d'images et de données.

5. Renseignement numérique et contenus en ligne

En matière pénale, le sujet des contenus en ligne concernent « *les infractions de « contenu » qui répriment la détention, l'échange, le transfert, la diffusion, etc. de messages illicites (pédopornographie, incitation à la haine raciale, diffamation, propagande terroriste, etc.) véhiculés par les technologies de l'information et de la communication* » selon le général Marc Watin-Augouard, qui ajoute que « *de telles infractions peuvent être commises en dehors du cyberspace, mais elles bénéficient avec internet et, en particulier, grâce au développement des réseaux sociaux, d'un exceptionnel vecteur d'amplification* »³. Plus concrètement, deux sous-catégories d'infractions de « contenu » peuvent être distinguées en application de l'article 6 de la LCEN du 21 juin 2004 sur la responsabilité des opérateurs de services de communication au public en ligne : d'une part, les infractions inscrites dans le code pénal qui sont spécifiques à la répression de certains discours jugés problématiques et préjudiciables comme l'incitation à des violences ou à la haine ; d'autre part, les infractions relevant de la loi du 29 juillet 1881 sur la liberté de la presse qui concernent des contenus numériques qui répondent à la notion de publication, c'est-à-dire qu'ils sont publiés sur des sites

¹ A ce sujet, voir P. Conte, *Atteinte à l'intimité de la vie privée. Notion d'intimité*, Droit pénal n° 7-8, Juillet 2020, comm. 130.

² En ce sens, voir J. -C. Saint-Pau, *Vie privée : du lien entre délit principal et délit de conséquence*, La Semaine Juridique Edition Générale n° 23, 6 juin 2016, act. 658.

³ Cf. M. Watin-Augouard, *Cybermenace et sécurité nationale*, Le droit de la sécurité et de la défense en 2013, op. cit., p. 302 et 303.

internet accessibles à des personnes qui ne sont pas seulement liées par une communauté d'intérêts et dont l'accès n'est pas restreint à certains utilisateurs en particulier par le responsable du site¹.

Ce type d'infractions s'intéresse notamment à l'apologie du terrorisme en ligne, ce qui présentent un double intérêt pour le renseignement numérique. D'abord, les agents des services de renseignement sont amenés à collecter et traiter de nombreuses informations à caractère terroriste dans l'usage de leurs moyens numériques légalisés de renseignement dans le cadre de la finalité de prévention du terrorisme prévue à l'article L. 811-3 du code de la sécurité intérieure. Ensuite, des agents peuvent être autorisés à effectuer des « cyber-patrouilles » pour partager en ligne sur demande expresse, sous un pseudonyme, une identité d'emprunt ou une fausse qualité, « *des contenus provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie* »².

D'un point de vue pénal, relevons que, d'une part, la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a transféré dans le code pénal les incriminations de provocation et d'apologie du terrorisme initialement inscrites dans la loi sur la presse³ et que, d'autre part, 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 a ajouté les délits autonomes⁴ de dissimulation de données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes et de consultation habituelle des sites terroristes⁵. Ce dernier délit a cependant été censuré à deux reprises par le Conseil constitutionnel⁶ qui a considéré que l'infraction n'était pas nécessaire au regard des nombreux dispositifs de prévention du terrorisme déjà en vigueur, comme notamment les moyens numériques des services de renseignement, mais également disproportionnée au

¹ Sur ce point, voir notamment N. Mallet-Poujol, *La liberté d'expression sur l'internet : aspects de droit interne*, Recueil Dalloz 2007 p.591.

² Articles L. 861-2 et L. 863-1 du code de la sécurité intérieure.

³ Article 421-2-5 du code pénal.

⁴ Articles 421-2-5-1 et 421-2-5-2 du code pénal.

⁵ Voir à ce sujet M. Quémener, « *Radicalisation : quelles réponses juridiques ?* », Sécurité et stratégie, vol. 24, no. 4, 2016, pp. 41-45.

⁶ Décisions n° 2016-611 QPC du 10 février 2017 et n° 2017-682 QPC du 15 décembre 2017.

regard de la liberté d'expression et de communication¹. Sur des motifs similaires, les Sages ont refusé de reconnaître l'existence d'un délit de recel d'apologie d'actes de terrorisme qui avait été admis par la Cour de cassation², ce qui permettait un certain contournement de la censure de l'article 421-2-5-2³.

Ensuite, on ne manquera pas de relever que le délit d'apologie du terrorisme, impliquant le fait de publiquement présenter de manière favorable un acte terroriste ou son auteur⁴, s'inscrit dans ce que la Professeure Agathe Lepage appelle « la pénalisation des influences », plus précisément dans les infractions sanctionnant « l'influence active »⁵. Ces considérations nous renvoient à une activité connue et ancienne des services de renseignement, les opérations relatives aux manipulations de l'information à des fins de déstabilisation ou de contre-ingérence qui sont aujourd'hui exacerbées dans le cyberspace et pratiquées également par des organisations non étatiques et des entreprises⁶. Véritable défi pour les démocraties libérales, les manipulations de l'information ou la diffusion de fausses nouvelles désinformant le public (« *fake news* » en anglais) font l'objet d'un arsenal pénal qui repose principalement sur les délits de presse de la loi de 1881 et quelques articles du code pénal, notamment l'article 411-10 réprimant la fourniture de fausses informations aux autorités civiles ou militaires de la France à des fins d'ingérence étrangère qui retiendra notre attention pour son application

¹ En ce sens, voir X. Latour, *La lutte contre les sites djihadistes et la liberté de communication*, La Semaine Juridique Administrations et Collectivités territoriales n° 7, 19 Février 2018, 2056 ; A. Lepage, *Déclaration d'inconstitutionnalité de l'article 421-2-5-2 du Code pénal*, Communication Commerce électronique n° 4, Avril 2017, comm. 35 ; M. Quémener, *La consultation de sites à caractère terroriste à l'épreuve de la liberté d'expression*, Dalloz IP/IT 2017 p.289 ; J. Bonnet et A. Roblot-Troizier, « *Chronique de droits fondamentaux et libertés publiques* », Les Nouveaux Cahiers du Conseil constitutionnel, vol. 55-56, no. 2-3, 2017, pp. 117-149 ; Y. Mayaud, *Consultation de site internet : seconde censure*, Recueil Dalloz 2018 p.97.

² Décision n° 2020-845 QPC du 19 juin 2020, *M. Théo S.*

³ Sur ce point, voir A. Lepage, *Fin de partie pour la répression du recel de fichiers provenant d'un site d'apologie d'actes de terrorisme*, Communication Commerce électronique n° 10, Octobre 2020, comm. 73 ; E. Dreyer, « *Infractions relevant du droit de l'information et de la communication* », Revue de science criminelle et de droit pénal comparé, vol. 3, no. 3, 2020, pp. 641-662.

⁴ Sur l'intention apologétique, voir notamment J. Alix, « *Chronique de politique criminelle* », Revue de science criminelle et de droit pénal comparé, vol. 2, no. 2, 2019, pp. 505-521.

⁵ Cf. A. Lepage, *Par-delà le prosélytisme, la pénalisation des influences. Essai d'une typologie des influences*, Société, droit et religion 2017/1 (Numéro 7), p. 15 à 34.

⁶ Cf. J.-B. Jeangène Vilmer, A. Escorcía, M. Guillaume, J. Herrera, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018.

directe au renseignement et à l'espionnage¹. Pour autant, quel que soit le contenu illicite, notons que la voie de la pénalisation n'est pas nécessairement la plus adaptée dans un Etat de droit démocratique pour protéger les internautes et l'Etat.

En effet, les décisions du Conseil constitutionnel relatives à la consultation des sites terroristes ou encore le rapport de 2018 sur les manipulations de l'information présenté par le Centre d'analyse, de prévision et de stratégie (CAPS, ministère des affaires étrangères) et l'Institut de recherche stratégique de l'Ecole militaire (IRSEM, ministère des armées) tendent à s'opposer à une surrégulation, notamment pénale, en matière de contenus diffusés sur internet qui risquerait de remettre excessivement en cause la liberté d'expression et de communication. Comme le remarquait le général Marc Watin-Augouard, qui nous rappelle que l'action sur les contenus ne peut se faire sans le concours des acteurs du web, « *la réponse est sans doute plus philosophique et politique que juridique* »². Dans la continuité de cette réflexion, on mentionnera le rapport de la « commission Bronner » qui recommande de ne pas modifier le dispositif pénal existant de lutte contre la diffusion de fausses nouvelles mais de renforcer l'action civile, le rôle de l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) et la responsabilité des plateformes dans la modération des contenus en ligne³. Pour notre part, on relèvera que si la problématique des contenus illicites et des manipulations de l'information nécessite une réponse pénale, elle constitue pour le renseignement davantage un enjeu lié à la cyberdéfense⁴.

Par ailleurs, en évoquant le cas des « cyber-patrouilles » agissant sous un pseudonyme, une identité d'emprunt ou une fausse qualité, d'autres infractions imputables à la cybercriminalité peuvent être envisagées, sans pour autant convaincre sur leur réelle application au domaine du renseignement. On pourrait ainsi penser que le délit d'usurpation d'identité numérique de l'article L. 226-4-1 du code pénal constitue un outil juridique de répression de l'espionnage dans son

¹ Sur les réponses juridiques aux manipulations de l'information, voir notamment M. Quémener, *Fake news, infox, quelles réponses juridiques ?*, Dalloz IP/IT 2019 p.178.

² Cf. M. Watin-Augouard, *Entre sécurité et liberté, quel équilibre pour la défense et la sécurité de l'espace numérique ?*, Annuaire 2018 du droit de la sécurité et de la défense, mare & martin, 2018, p. 115 à 140.

³ Cf. Rapport de la commission Bronner, *Les Lumières à l'ère numérique*, Présidence de la République, 11 janvier 2022, p. 76 à 87.

⁴ Cf. infra. Chapitre I du Titre II de la Seconde partie.

élément matériel¹. Cependant, soulevons deux remarques sur l'élément matériel : d'une part, si la Cour de cassation a jugé que le texte de l'article 226-4-1 « *définit de manière suffisamment précise les agissements qu'il réprime pour exclure l'arbitraire, compte tenu du pouvoir d'appréciation reconnu aux juridictions pénales, chargées d'apprécier si les situations de fait poursuivies devant elles revêtent ou non un caractère répréhensible* »², il reste que l'interprétation du texte peut s'avérer difficile en l'absence de définition légale des données numériques pouvant être utilisées pour la réalisation du délit, d'autant plus que la jurisprudence demeure faible en la matière. D'autre part, il semblerait que dans le numérique le délit ne concerne que les réseaux de communication au public en ligne, ce qui exclurait le fait d'usurper l'identité d'un tiers pour infiltrer un réseau de communication électronique privé. En outre, l'élément moral consacre un dol spécial qui vise à sanctionner spécifiquement l'atteinte à la tranquillité ou à la réputation d'autrui, ce qui réduit nettement le champ d'application du texte dans le domaine du renseignement. Aussi, on préférera retenir d'autres infractions comme les atteintes aux données personnelles dans le cas de l'abus des « cyber-patrouilles », notamment si ces dernières sont utilisées pour la technique d'hameçonnage (ou « *phishing* » en anglais)³ ou encore pour la création de faux sites internet pour entrer en contact avec des organisations ou des personnes à surveiller⁴. Dans le prolongement de ces considérations, on pourrait également penser à invoquer les

¹ En ce sens voir, M. Griguer, *Le point sur la lutte contre l'usurpation d'identité numérique*, Cahiers de droit de l'entreprise n° 4, Juillet 2011, prat. 20 ; Légipresse, *L'infraction d'usurpation d'identité numérique prévue par l'article 226-4-1 du Code pénal s'applique aux personnes morales*, Légipresse N° 402, 13 avril 2022, p. 209 ; F. Mattatia, « *L'usurpation d'identité sur internet dans tous ses états* », Revue de science criminelle et de droit pénal comparé, vol. 2, no. 2, 2014, pp. 331-337 ; E. A. Caprioli, *Usurpation d'identité par création d'adresses mails et de faux profils Facebook*, Communication Commerce électronique n° 1, Janvier 2015, comm. 9 et J. Francillon, *L'affaire du « faux site officiel » de Rachida Dati : une étape dans la lutte contre la cyberdélinquance*, RSC 2015 p.101.

² Cass. crlm., 20 juin 2018, n° 18-90.012.

³ Selon l'ANSSI, « *l'hameçonnage reste l'un des principaux vecteurs de la cybercriminalité. Ce type d'attaque vise à obtenir du destinataire d'un courriel d'apparence légitime qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent. L'hameçonnage peut également être utilisé dans des attaques plus ciblées pour essayer d'obtenir d'un employé ses identifiants d'accès aux réseaux professionnels auxquels il peut avoir accès* » (<https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/attaque-par-hameconnage-phishing/>).

⁴ En ce sens, voir notamment C. Legris-Dupeux et E. Renaud-Chouraqui, *Quelle réponse juridique face à l'augmentation exponentielle du développement des faux sites administratifs ?*, Revue Lamy Droit de l'Immatériel, N° 158, 1er avril 2019.

délits d'escroquerie¹ et de recel² dans l'abus du dispositif prévu à l'article L. 863-1 du code de la sécurité intérieure, mais de tels abus ne semblent possibles que dans la situation d'un agent agissant pour son propre intérêt en dehors d'une mission de renseignement. Toutefois, on retiendra le délit de faux et d'usage de faux prévu à l'article 441-1 du code pénal en ce qui concerne la conception ou l'usage d'une identité d'emprunt ou d'une fausse qualité pour les besoins des « cyber-patrouilles ».

B – Le risque pénal de moyens numériques n'entrant pas dans le champ du droit du renseignement

On distinguera deux hypothèses d'utilisation abusif de moyens numériques par les services de renseignement qui ne sont pas encadrés par le droit du renseignement et qui peuvent servir à commettre des infractions cybercriminelles : l'usage offensif de moyens de lutte informatique et le recours à des moyens automatisés de renseignement d'origine sources ouvertes en ligne.

1. L'usage offensif de moyens de lutte informatique

Les services de renseignement, français comme étrangers, jouent un rôle de premier plan dans les opérations de cyberdéfense et participent activement à la lutte informatique³, notamment pour entraver des menaces susceptibles d'affecter les systèmes numériques de l'Etat. D'ailleurs, on rappellera que l'article L. 811-2 du code de la sécurité intérieure dispose explicitement que les services de renseignement doivent contribuer à l'entrave de ces menaces. Ainsi, les agents des services spécialisés pourraient se voir poursuivis pénalement pour un usage offensif et abusif de moyens de lutte informatique. Il pourrait en être ainsi en cas des délits de sabotage ou d'atteintes à l'intégrité ou à l'authenticité des systèmes numériques ou des données qu'ils contiennent prévus aux articles 323-2 et 323-3⁴ du code pénal commis en violation de l'excuse pénale introduite à l'article 323-

¹ On notera que le délit d'escroquerie prévu à l'article 313-1 du code pénal répond particulièrement, et de manière plus adaptée que l'usurpation d'identité, à la lutte contre le *phishing* (en ce sens, voir E. A. Caprioli, *Le phishing saisi par le droit*, Communication Commerce électronique n° 2, Février 2006, comm. 37 et D. Père, *L'arsenal répressif du phishing*, Recueil Dalloz 2006 p.2666).

² Article 321-1 du code pénal.

³ Cf. Section I du Chapitre I du Titre II de la Seconde partie.

⁴ A ce sujet, voir J. Françillon, *De diverses variétés de piratages*, RSC 1998, p. 138.

8 du même code pour le renseignement extérieur. Ces délits pourraient aussi être retenus dans le cas d'un usage abusif d'une captation de données informatiques ayant pour conséquence de saboter un système numérique ou de modifier son contenu. Ajoutons que le délit de sabotage peut être requalifiable en crime lorsque sont en cause les intérêts fondamentaux de la Nation¹, cette qualification criminelle étant adaptée au domaine du contre-espionnage d'Etat.

Enfin, on ne manquera pas de relever que la qualification d'entrave à un système de traitement automatisé de données a été notamment retenue par le Parquet de Paris² dans l'affaire de la cyberattaque mondiale *NotPetya* de 2017 qui impliquerait le renseignement militaire russe (GRU) selon l'Union européenne³. De son côté, l'ANSSI a considéré que cette cyberattaque constituait une campagne de sabotage visant à chiffrer et rendre inutilisable les systèmes d'informations (utilisation d'un logiciel malveillant de « crypto-verrouilleur ») en précisant que ces derniers avaient été infectés par un moyen de propagation automatique (ou « vers informatique ») utilisant un code d'exploitation de vulnérabilité informatique (ou « exploit ») « *supposément développé par la NSA et divulgué en source ouverte* »⁴. Cette affaire souligne la proximité ou, du moins, les rapprochements qui peuvent exister entre les services de renseignement russes et la cybercriminalité⁵.

2. Le recours à l'automatisation du renseignement d'origine sources ouvertes en ligne

Si les services de renseignement ont particulièrement vocation à rechercher des informations secrètes, confidentielles et protégées ou dites « fermées », ils ont également recours aux techniques de collecte des informations

¹ Article 411-9 du code pénal.

² Voir l'article *Cyberattaque mondiale : le parquet de Paris ouvre une enquête en France*, Le Parisien, 28 juin 2017, (<https://www.leparisien.fr/high-tech/une-nouvelle-cyberattaque-frappe-l-europe-le-groupe-saint-gobain-touche-27-06-2017-7092270.php>).

³ Décision (PESC) 2020/1127 du Conseil du 30 juillet 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres.

⁴ A ce sujet, voir ANSSI, *Etat de la menace rançongiciel à l'encontre des entreprises et institutions*, 5 février 2020, p. 6 et 7.

⁵ Dans le même sens, voir B. Bertrand, *La souveraineté numérique européenne : une « pensée en acte »* ?, op. cit..

rendues publiquement accessibles ou ouvertes à tous¹. En effet, il ressort des rapports de la DPR que par exemple : la DGSE « *maîtrise la totalité des modes de recueil de renseignements sources humaines, capteurs techniques (interceptions électromagnétiques et imagerie satellitaire principalement), moyens opérationnels et sources ouvertes* »² ; Tracfin travaille principalement en sources ouvertes³ ; le SNRP dispose « *d'agents formés à l'investigation numérique et à la recherche en sources ouvertes* »⁴ ; la DRM utilise des solutions développées par des entreprises pour faire de la veille et de l'investigation en sources ouvertes⁵. Avec le développement du cyberspace, les services de renseignement tendent à s'approprier les technologies du Big data et de l'intelligence artificielle afin de collecter et traiter les informations ouvertes massivement accessibles sur internet et les réseaux sociaux⁶.

La plupart des informations publiées sur internet sont considérées comme librement accessibles même si elles sont payantes. La collecte de ces données relève alors du renseignement d'origine sources ouvertes (ROSO ou OSINT pour « *Open Source Intelligence* » en anglais) qui est une activité qui peut s'exercer librement par les services spécialisés, à la condition qu'elle ne concerne pas des informations protégées techniquement et/ou juridiquement par le droit à la vie privée ou aux secrets⁷. C'est pourquoi le législateur n'a pas soumis cette forme de recueil de renseignements à un régime d'autorisation préalable, ni consacré de dispositions légales spécifiques à cette activité⁸.

¹ Sur les informations ouvertes et renseignement fermé, voir E. Meillan, *Le renseignement intérieur : pour l'efficacité dans la démocratie*, Droit pénal n° 7-8, juillet 2016, étude 15.

² Cf. J. -P. Raffarin, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, op. cit., p. 48.

³ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 74.

⁴ Ibid., p. 114.

⁵ Ibid., p. 275 et 276.

⁶ En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 267 et O. Chopin et B. Oudet, « *Chapitre 6. Sources ouvertes, cyber, data : le renseignement et la révolution de l'information* », *Renseignement et sécurité*, Armand Colin, 2019, pp. 169-194.

⁷ En ce sens, voir J. Poirot, « *ROSO* », Hugues Moutouh éd., *Dictionnaire du renseignement*, op. cit., pp. 677-681.

⁸ A ce sujet, voir F. -N. Buffet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2021-2022*, op. cit., p. 65.

Pour autant, le recours à des outils automatisés et sophistiqués de recherche et de collecte de données d'origine sources ouvertes sur internet peuvent contourner des mécanismes de cyberprotection pour compromettre des données confidentielles stockées sur internet. Cette automatisation de la collecte de données peut alors se révéler être une atteinte à un système de traitement automatisé de données ou encore une collecte clandestine et frauduleuse de données personnelle réprimés par le code pénal. A titre d'exemple, le tribunal de grande instance de Paris a jugé, dans l'affaire *Editions Neressis c/ Arkadia* de 2008, que l'utilisation d'un outil de ligne de commande pour parcourir des sites internet ayant permis de s'introduire dans des bases de données confidentielles et de collecter des données personnelles y figurant constituait un accès frauduleux au sens de l'article 323-1 et une collecte frauduleuse au sens de l'article 226-18¹. Plus sévère, l'arrêt de la cour d'appel de Paris du 15 septembre 2017 rendu dans l'affaire *Weezevent* a considéré que la collecte automatisée et sélective de très nombreuses données personnelles consultables publiquement sur un site internet devait être sanctionnée pour extraction frauduleuse de données dès lors que cette opération ne pouvait se réaliser sans autorisation expresse mais aussi pour collecte déloyale et frauduleuse de données personnelles². On précisera que la Cour de cassation a défini dans son arrêt *Fabrice H. c/ Ministère public* de 2006³, largement commenté⁴, les conditions du délit de collecte déloyale de données personnelles accessibles publiquement sur internet, notamment lorsqu'elle est

¹ Voit à ce sujet E. A. Caprioli, *L'aspiration d'un site sanctionnée sur le fondement de la fraude informatique*, Communication Commerce électronique n° 1, Janvier 2009, comm. 10.

² En ce sens, voir E. A. Caprioli, *Collecte de données personnelles non protégées et extraction frauduleuse*, Communication Commerce électronique n° 2, Février 2018, comm. 16.

³ Cass. crim., 14 mars 2006, n° 05-83.423.

⁴ Sur l'arrêt, voir notamment G. Roussel, *Déloyauté du recueil d'adresses électroniques sur Internet par l'utilisation d'un logiciel*, AJ Pénal 2006 p.260 ; J. Le Clainche, *La Cour de cassation clarifie le régime des pourriels*, Revue Lamy Droit de l'Immatériel, N° 16, 1er mai 2006 ; P. Belloir, *Le délit de collecte déloyale de données à caractère personnel à l'épreuve d'internet*, Revue Lamy Droit de l'Immatériel, N° 17, 1er juin 2006 ; A. Lepage, *Collecte déloyale de données personnelles sur Internet*, Communication Commerce électronique n° 9, Septembre 2006, comm. 131.

réalisée de manière automatique sur des adresses électroniques dans le cadre des pourriels¹ en dehors du champ d'application de la prospection commerciale² :

- d'une part, la collecte est désormais caractérisée sans qu'il n'y ait besoin que les données soient enregistrées dans un fichier conformément à la lettre des dispositions de l'article 226-18 issues de la réforme de 2004 ;
- d'autre part, le caractère déloyal de la collecte des données personnelles sur l'espace public internet résulte de la clandestinité de l'opération faisant obstacle au droit d'opposition des personnes concernées.

Dans ces conditions, les agents des services de renseignement pratiquant le ROSO pourraient ainsi s'exposer à un risque pénal en l'absence de dispositions législatives ou réglementaires protectrices de cette activité. En effet, l'automatisation de cette activité pourrait être requalifiée par la CNCTR ou le juge en captation de données informatiques mise en œuvre sans autorisation préalable et manifestement illégale ou en collecte ou exploitation frauduleuse de données personnelles et se voir appliquer les infractions précédemment retenues.

Dans le silence des textes, il convient alors de déterminer quelle protection juridique peut être accordée aux agents lorsqu'ils agissent de manière légitime pour les besoins de leurs missions. S'agissant d'une éventuelle atteinte à un système de traitement automatisé de données, l'exclusion de la loi pénale française prévue à l'article 323-8 du code pénal devrait permettre aux agents de bénéficier d'une protection pénale suffisante pour les mesures de piratage informatique à l'étranger qui aurait été opérée par des outils automatisés intrusifs de ROSO ciblant des sites web étrangers ou des personnes physiques ou morales étrangères sans liens avec la France.

En revanche, l'exclusion pénale ne tient plus pour une atteinte commise sur internet en France ou contre une personne physique résidant sur le territoire de la République ou une personne morale dont le siège se situe sur le territoire de la

¹ Selon l'ANSSI, le pourriel (spam) est « *tout courrier électronique non sollicité par le destinataire. Remarques : Le courrier est souvent envoyé simultanément à un très grand nombre d'adresses électroniques. Les produits les plus vantés sont les services pornographiques, la spéculation boursière, des médicaments, le crédit financier, etc* » (<https://www.ssi.gouv.fr/entreprise/glossaire/p/#pourriel-pollurriel-spam>).

² Article L. 34-5 du code des postes et des communications électroniques.

République¹. Pour les infractions contre les données personnelles qui seraient caractérisées dans tous leurs éléments, les règles de droit commun de l'application de la loi pénale dans l'espace devraient s'appliquer². Un mécanisme d'auto-régulation des services de renseignement pourrait alors être envisagé en s'appuyant sur le cadre légal des techniques de renseignement, c'est-à-dire en limitant l'utilisation de l'automatisation du ROSO potentiellement intrusif aux finalités de l'article L. 811-3 du code de la sécurité intérieure et en soumettant la collecte et l'exploitation des données au principe de proportionnalité. De manière similaire aux « cyber-patrouilles », un agent chargé de superviser ou de coordonner le recueil des renseignements en sources ouvertes pourrait en assurer le contrôle interne. Une présentation de ce type de technique à la CNCTR, dans la même idée que pour le contrôle de la surveillance des communications hertziennes publiques³, permettrait également un contrôle externe pour prévenir les risques de confusion avec la technique de captation de données informatique et de collecte frauduleuse de données personnelles.

En reprenant l'ensemble de nos développements précédents, il est possible de dresser un tableau récapitulatif des infractions cybercriminelles applicables au renseignement numérique et d'affaires cybercriminelles emblématiques impliquant des agents des services de renseignement.

¹ Article 113-2-1 du code pénal.

² Articles 113-1 à 113-14 du code pénal.

³ Article L. 855-1 C du code de la sécurité intérieure.

Tableau récapitulatif des infractions et affaires cybercriminelles concernant le renseignement numérique

	Atteintes aux STAD	Atteinte au secret des correspondances électroniques	Atteintes aux données personnelles	Atteintes à l'intimité de la vie privée par un quelconque moyen technique	Diffusion de contenus illicites	Affaires
Moyens numériques légalisés de renseignement	Accès ou maintien frauduleux dans un STAD, introduction frauduleuse de données ou extraction, reproduction ou transmission frauduleuses de données et trafic de moyens de piratage informatique pour usage abusif des moyens suivant : • dispositifs techniques d'interception des données de connexion ou de communications ; • Interceptions de communications hertziennes ou satellitaires ; • captation de données informatiques • accès aux données et fichiers intéressant le renseignement et leurs usages encadrés par les dispositions de la loi « Informatique et libertés », du droit du renseignement sur les transmissions d'informations et sur l'intelligence artificielle et des textes réglementaires spécifiques aux fichiers. Ajoutons à ces moyens le non-respect des mesures prévues par l'article 323-8 C. pén. ou des règles de l'article 2371-2 C. défense. encadrant les essais de matériels de renseignement.	Applicable à l'ensemble des moyens d'interception de communications prévus par le code de la sécurité intérieure ainsi qu'en cas de collecte interdite de données de contenu dans le cadre des accès aux données de connexion, notamment par IMSI-catcher ou algorithme, et à la captation de données informatique portant sur des moyens de communications tels qu'une messagerie électronique. Comme pour les STAD, ajoutons le non-respect des mesures prévues par l'article 323-8 C. pén. ou des règles de l'article 2371-2 C. défense. encadrant les essais de matériels de renseignement.	Applicables à l'ensemble des moyens numériques légalisés de renseignement, que ce soit pour la collecte des données ou leurs exploitations.	Applicables à la sonorisation, à la captation d'images et la géolocalisation par balisage.	Application de la répression relative à l'apologie du terrorisme en ligne aux partages de contenus par les « cyber-patrouilles ».	Les écoutes de l'Elysée (de 1983 à 1986) : interceptions de sécurité illégales constituant les infractions d'atteintes à l'intimité de la vie privée et aux données personnelles. Les fadettes du Monde (2010) : atteinte aux données personnelles par l'application détournée du régime de la surveillance hertzienne pour collecter des fadettes d'un journaliste. Haurus (2021) : consultation abusive des fichiers de police par un agent de la DGSI et vente sur le « darknet » des informations consultées portant atteintes aux données personnelles et au secret professionnel.

Usage offensif de moyens de lutte informatique	Sabotage ou atteintes à l'intégrité ou à l'authenticité des systèmes numériques ou des données qu'ils contiennent en cas d'abus de l'excuse pénale de l'article 323-8 C. pén. ou d'une captation de données informatiques entraînant des conséquences offensives.		Application en cas de sabotage ou de manipulation sur des données personnelles.			NotPetya (2017) : implication du renseignement militaire russe dans la cyberattaque mondiale qualifiée d'entrave à un STAD selon le Parquet de Paris.
Automatisation du ROSO en ligne	Risque de requalification en captation de données informatiques portant atteinte à un STAD.		Risque de requalification en collecte ou traitement frauduleux de données personnelles.			

§2. La délicate conciliation entre la lutte contre la cybercriminalité et le renseignement numérique

L'application de la loi pénale au renseignement numérique, à laquelle s'ajoute la croissance simultanée des activités de cyber-renseignement d'Etat et cybercriminelles, constitue un risque juridique pour les services de renseignement sans toutefois être un « angle mort » du droit du renseignement. Ce dernier peut avoir pour effet de s'opposer aux mécanismes de lutte contre la cybercriminalité qui pourraient viser les services. Parallèlement, le législateur a adapté le droit pénal du numérique à l'essor d'activités privées de cyber-renseignement, ce qui nous amène à nous interroger sur les limites de l'encadrement des partenariats entre les services de renseignement et certains acteurs privés exerçant des activités de cyber-renseignement.

A - Les obstacles aux mécanismes de lutte contre la cybercriminalité par le droit du renseignement

L'une des fonctions du droit du renseignement réside dans la protection juridique des activités et des agents des services de renseignement. A ce titre, il peut faire obstacle aux poursuites judiciaires visant des agents des services à deux niveaux : lorsque le procureur de la République est avisé de l'usage illégal d'une technique de renseignement ou lorsqu'une opération de cyber-renseignement d'Etat entraîne le déclenchement de la coopération pénale internationale en matière de cybercriminalité.

1. L'usage illégal d'une technique de renseignement et le secret de la défense nationale

Rappelons que les articles L. 861-3 du code de la sécurité intérieure et L. 773-7 du code de justice administrative disposent tous deux que le procureur de la République peut être saisi par la CNCTR, dans le cadre de la procédure de lanceur d'alerte, ou le Conseil d'Etat, en cas de contentieux, lorsqu'une illégalité constatée dans l'usage d'une technique de renseignement est susceptible de constituer une infraction. Cependant, la protection du secret de la défense nationale qui s'étend à la mise en œuvre des techniques de renseignement pourrait rendre difficiles les investigations judiciaires du ministère public. En effet, les

articles précités précisent que les éléments classifiés dont disposent la CNCTR et le Conseil d'Etat doivent être transmis à la Commission du secret de la défense nationale (CSDN) « *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* ». Dans ces conditions, l'administration conserve, d'une certaine manière, la maîtrise des poursuites judiciaires susceptibles de concerner un directeur ou un agent fautif. On peut souligner la nouveauté pour un juge de pouvoir directement transmettre à la CSDN des éléments classifiés d'un dossier dans le cadre de la procédure de l'article L. 773-7 alinéa 3¹ mais le législateur aurait pu aller plus loin en conférant à la formation spécialisée du Conseil d'Etat, habilitée au secret de la défense nationale, le pouvoir de statuer sur la déclassification des éléments nécessaires à la procédure pénale après avoir entendu les observations du Premier ministre et de la CSDN sur cette question.

2. La protection du droit du renseignement contre la coopération pénale internationale

Du fait du caractère transnational du cyberspace, il est crucial pour les Etats de mettre en place une coopération policière et judiciaire internationale en matière de lutte contre la cybercriminalité, notamment à travers la Convention de Budapest de 2001 du Conseil de l'Europe qui constitue actuellement le seul traité international visant à harmoniser les législations nationales et à favoriser les échanges de preuves numériques entre les pays². En outre, une véritable politique pénale européenne de lutte contre la cybercriminalité tend progressivement à s'affirmer³.

En pratique, la coopération pénale internationale est mise en œuvre par les services répressifs nationaux avec les instances de coordination policières et

¹ A ce sujet, voir également P. Bas, *Rapport sur le projet de loi relatif au renseignement et sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, op. cit., p. 108.

² En ce sens, voir notamment S. Taillat, « *Un mode de guerre hybride dissymétrique ? Le cyberspace* », *Stratégie*, vol. 111, no. 1, 2016, pp. 89-106 et E. C. Viano, « *Section II - Droit pénal. Partie spéciale - Société de l'information et droit pénal. Rapport général* », *Revue internationale de droit pénal*, vol. 84, no. 3-4, 2013, pp. 311-334.

³ A ce sujet, voir l'article Cybercriminalité - « *Les cyberattaques et la cybercriminalité revêtent des formes de plus en plus sophistiquées. Cette tendance devrait se poursuivre* ». - 3 questions à Myriam Quémener, avocat général près la cour d'appel de Paris, docteur en droit, *La Semaine Juridique Édition Générale* n° 19-20, 10 mai 2021, 533 et F. Chopin, *Les politiques publiques de lutte contre la cybercriminalité*, *AJ Pénal*, 2009, p. 101.

judiciaires multilatérales que sont Interpol ou encore Europol et Eurojust au niveau européen¹. On notera que ces dernières ont suivi le mouvement de spécialisation du droit pénal sur la cybercriminalité en créant des services dédiés de coopération comme le Centre européen de la lutte contre la cybercriminalité (EC3) en 2013 ou encore le Complexe mondial d'Interpol pour l'innovation (CMII) en 2015². Cependant, le manque d'échanges automatiques d'informations entre les Etats, la lourdeur des procédures et les difficultés d'accès aux preuves numériques ont été des constats partagés par les praticiens et la doctrine³. Pour répondre à ces difficultés, un renforcement de la coopération internationale a été initiée avec deux nouvelles propositions :

- un nouveau protocole additionnel à la Convention de Budapest de 2001 sur la divulgation des preuves électroniques qui a été ouvert à la signature le 12 mai 2022⁴. Ce protocole assure notamment une coopération plus immédiate en cas d'urgence entre les services répressifs et une coopération plus directe avec les opérateurs du numérique pour l'accès aux informations sur leurs abonnés⁵ ;
- un nouveau règlement européen « E-evidence » du Parlement et du Conseil de l'Union européenne qui permettra aux autorités judiciaires d'émettre des injonctions de production et de conservation de preuves électroniques stockées par les opérateurs du numérique, quelle que soit la localisation des données dans l'Union européenne⁶. Le nouveau règlement est complété par une directive visant à harmoniser les règles de désignation de

¹ Sur ce point, voir J. -M. Nesme, *Rapport sur le projet de loi n° 905 autorisant l'approbation de la convention sur la cybercriminalité*, Assemblée nationale, 8 décembre 2004, p. 9 à 11.

² En ce sens, voir le rapport du Club des juristes, « *Le droit pénal à l'épreuve des cyberattaques* », avril 2021 et G. Beaussonie, *La place du droit pénal dans la lutte contre la cybercriminalité*, La Semaine Juridique Edition Générale n° 21, 25 Mai 2021, 538.

³ Voir en ce sens B. Pereira, « *La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité* », *Revue internationale de droit économique*, vol. xxx, no. 3, 2016, pp. 387-409 ; M. Quémener, *Cyberattaque : le point de vue du magistrat sur les actions en justice*, Dalloz IP/IT 2021 p.389 ; G. Haas et A. Dubary, *Cybercriminalité : mais que fait la justice ?*, *Revue Lamy droit des affaires*, n° 168, 1^{er} mars 2021.

⁴ Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE n° 224).

⁵ Ibid.

⁶ Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale.

représentants légaux chargés de la collecte de preuves au sein des fournisseurs de services numériques¹ ainsi que l'adoption d'un accord avec les Etats-Unis pour garantir un accès transfrontière aux preuves électroniques dans le respect des droits fondamentaux de l'Union européenne².

Les cyberopérations de renseignement menées à l'étranger susceptibles de constituer une infraction n'échappent pas à la coopération pénale internationale et aux risques de poursuites judiciaires puisque les textes internationaux précédemment mentionnés ne distinguent pas les actes cybercriminels des actes clandestins des services de renseignement autorisés en droit interne ou considérés comme légitimes en l'absence d'un cadre légal. En revanche, le droit français du renseignement prévoit un certain nombre de dispositions qui permettent d'opérer une telle distinction en droit interne. D'abord, on rappellera l'exclusion de l'application de la loi pénale aux mesures de piratage menées à l'étranger qui constituent des infractions aux systèmes de traitement automatisé de données³. Ensuite, on relèvera que l'article L. 862-1 du code de la sécurité intérieure instaure une procédure d'avis préalable aux poursuites judiciaires contre un agents des services spécialisés de renseignement :

« Lorsque des faits commis hors du territoire national, à des fins strictement nécessaires à l'accomplissement d'une mission commandée par ses autorités légitimes, par un agent des services mentionnés à l'article L. 811-2, sont portés à sa connaissance et paraissent susceptibles de constituer des infractions pénales, le procureur de la République territorialement compétent en informe le ministre dont relève le service de l'agent concerné aux fins de recueillir son avis préalablement à tout acte de poursuite. Hormis le cas d'urgence, cet avis est donné dans le délai d'un mois. L'avis est demandé par tout moyen dont il est fait mention au dossier de la procédure. L'avis

¹ Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales.

² Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters - 21 May 2019.

³ Article 323-8 du code pénal.

figure au dossier de la procédure, à peine de nullité, sauf s'il n'a pas été formulé dans le délai précité ou en cas d'urgence ».

Ces dispositions nous semblent s'appliquer en cas de coopération pénale internationale si un agent français est impliqué dans des faits cybercriminels relevés à l'étranger et portés à la connaissance du parquet français. Sur la forme, le procureur de la République est donc tenu de procéder à la consultation du ministre de tutelle concerné. Sur le fond, il conserve son opportunité des poursuites, notamment en appréciant la stricte nécessité des faits pouvant être reprochés à l'agent. Si l'article L. 862-1 ne fait pas obstacle aux poursuites judiciaires, il n'en demeure pas moins que le procureur de la République peut se voir opposer le secret de la défense nationale et la protection de l'anonymat des agents¹. Ces considérations tendent à limiter l'effectivité du texte et, plus largement, celle de la coopération pénale.

Ici, le droit du renseignement réaffirme, d'une certaine manière, les limites traditionnelles de la coopération pénale internationale tenant à la souveraineté des Etats. Pour autant, les risques de procédures internationales à l'encontre d'agents des services de renseignement ne sont pas nuls. Il convient alors pour les services de bien évaluer les risques juridiques encourus par leurs agents dans la mise en œuvre de cyberopérations à l'étranger.

B – L'adaptation du droit pénal du numérique aux activités privées de cyber-renseignement

Le renseignement d'Etat et les services de police judiciaire n'ont pas le monopole des technologies d'espionnage et de surveillance. Le secteur privé s'est également approprié ces technologies pour la défense de ses propres intérêts. A cet égard, le dispositif pénal de lutte contre la cybercriminalité a été adapté pour tenir compte des activités privées de surveillance. On mentionnera succinctement trois exemples :

- la cybersurveillance du salarié par l'employeur : selon le code du travail et la jurisprudence de la chambre sociale de la Cour de cassation, le chef d'entreprise est autorisé à mettre en œuvre des moyens techniques de surveillance des activités professionnelles dans le cadre de son pouvoir de

¹ Article L. 861-1 du code de la sécurité intérieure.

direction lorsque ces moyens sont notamment portés à la connaissance du salarié¹ et qu'ils respectent le principe de proportionnalité² ainsi que les principes de la loi informatique et libertés³. Il peut s'agir du contrôle des messageries professionnelles, des fichiers et outils informatiques professionnels et de l'usage d'internet⁴ ou encore de la géolocalisation⁵ et de la vidéosurveillance ou sonorisation des salariés⁶ ;

- l'exercice des droits de la défense : cause d'exonération pénale prétorienne, les droits de la défense peuvent être invoqués devant le juge pour justifier, selon le cas d'espèce, des mesures de surveillance numérique portant atteintes à la vie privée et au secret des correspondances ou aux STAD⁷. Précisons que la Cour de cassation admet cette solution que dans le respect du principe de proportionnalité⁸ ;
- la constitution de fichiers de type « listes noires » : fichier de données personnelles, une « liste noire » est une « *liste de personnes considérées comme étant « à risques » par une société, un organisme ou un*

¹ Article L. 1222-4 du code du travail.

² Article L. 1121-1 du code du travail.

³ Voir à ce sujet H. Bouchet, *La cybersurveillance sur les lieux de travail*, rapport adopté par la CNIL le 5 février 2002 et H. Bouchet, « *La surveillance numérique au travail* », Hermès, La Revue, vol. 53, no. 1, 2009, pp. 85-90.

⁴ Voir sur ces sujets, A. Lepage, *Le faux-jumeau de l'arrêt Nikon*, Communication Commerce électronique n° 7, Juillet 2005, comm. 121 ; L. Casaux-Labrunée, *Vie privée des salariés et vie de l'entreprise*, Droit social n° 4, avril 2012 ; E. A. Caprioli, *Validité du contrôle du contenu de messages envoyés depuis une messagerie personnelle*, Communication Commerce électronique n° 10, Octobre 2013, comm. 110 ; E. A. Caprioli, *La CEDH valide le contrôle des messages professionnels*, Communication Commerce électronique n° 4, Avril 2016, comm. 37 ; O. de Maison Rouge, « *La surveillance et le contrôle au sein de l'entreprise : les limites de l'exercice posées par le Droit* », Sécurité et stratégie, vol. 21, no. 1, 2016, pp. 12-17 ; E. A. Caprioli, *Contrôle par l'employeur des fichiers stockés sur l'ordinateur professionnel d'un salarié en son absence*, Communication Commerce électronique n° 5, Mai 2018, comm. 40.

⁵ Voir à ce sujet, M. Quémener, *La géolocalisation : un outil de protection ou de surveillance ?*, Sécurité et stratégie, vol. 15, no. 4, 2013, pp. 11-17 ; A. Gardin, *Géolocalisation du véhicule du salarié : quand finalité, proportionnalité et fiabilité font loi*, Revue de droit du travail 2015, p. 544.

⁶ Voir à ce sujet, L. Marino, *Protection pénale de la vie privée du salarié espionné par son employeur*, Recueil Dalloz 2003, p. 1533 et O. de Maison Rouge, « *La surveillance et le contrôle au sein de l'entreprise : les limites de l'exercice posées par le Droit* », op. cit..

⁷ En ce sens, voir E. Dreyer, « *Infractions relevant du droit de l'information et de la communication* », Revue de science criminelle et de droit pénal comparé, vol. 3, no. 3, 2018, pp. 701-720 ; P. Mistretta, « *Droit pénal médical* », Revue de science criminelle et de droit pénal comparé, vol. 2, no. 2, 2018, pp. 473-485 ; G. Roujou de Boubée, T. Garé et S. Mirabail, *Droit pénal*, Recueil Dalloz 2007 p.399 ; J. -C. Saint-Pau, *L'enregistrement clandestin d'une conversation*, Droit pénal n° 9, Septembre 2008, étude 17.

⁸ Cass. Ass. Plén., 22 décembre 2023, n° 20-20.648.

commerçant »¹. Ce fichage privé peut être autorisé par la loi ou le règlement² ou en respectant les exigences de la CNIL de formalités préalables, de transparence, de limitation dans l'accès au fichier, de respect des règles de la loi informatique et libertés sur la collecte et la conservation des données, du droit à l'oubli et de confidentialité et de sécurité des données³.

Toutefois, il convient de remarquer que ces exemples de surveillance numérique privée ont pour point commun d'être autorisés que lorsque qu'un droit à la transparence et à l'information pour les personnes concernées est garanti. Si les moyens techniques utilisés sont similaires à ceux du renseignement d'Etat, la surveillance numérique privée doit être clairement distinguée de celle autorisée pour les services de renseignement qui est par nature secrète et protégée, à ce titre, par le droit du secret de la défense nationale.

En revanche, la lutte contre les cyberattaques et la masse de données librement accessibles sur internet ont fait émerger un marché privé du renseignement d'intérêt cyber (RIC) et du renseignement d'origine cyber (ROC) en sources ouvertes qui intéresse directement les services de renseignement en recherche de nouvelles technologies et d'expertises. D'un point de vue juridique, le droit pénal de fond et de forme a été adapté, en cohérence avec l'organisation étatique de la cyberdéfense, pour reconnaître la légitimité du RIC tout en contribuant à un encadrement restrictif des partenariats public-privé de cyber-renseignement.

1. La reconnaissance du renseignement privé d'intérêt cyber

Dès la création de l'article 323-3-1 du code pénal par la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 qui réprime la détention et l'échange de moyens ou de données permettant de commettre les infractions contre les systèmes de traitement automatisé de données, le législateur avait

¹ Voir la définition sur le site internet de la CNIL, "[Liste noire](https://www.cnil.fr/fr/cnil-direct/question/liste-noire-doit-minformer-que-je-suis-fiche)" : doit-on m'informer que je suis fiché ? | [Besoin d'aide | CNIL](https://www.cnil.fr/fr/cnil-direct/question/liste-noire-doit-minformer-que-je-suis-fiche) (<https://www.cnil.fr/fr/cnil-direct/question/liste-noire-doit-minformer-que-je-suis-fiche>).

² A ce sujet, voir par exemple le cas des listes noires des supporters (cf. A. Debet, *Constitutionnalité des listes noires des supporters*, Communication Commerce électronique n° 9, Septembre 2017, comm. 75).

³ Sur les exigences de la CNIL, voir J. Frayssinet, « *Les sites de notation (Note2be...) face au droit* », LEGICOM, vol. 43, no. 2, 2009, pp. 83-87.

prévu dans le texte d'incrimination une exonération pour les personnes justifiant d'un « motif légitime » sans toutefois apporter plus de précisions. A l'occasion d'une affaire de divulgation de failles de sécurité informatique constitutive du délit prévu à l'article 323-3-1, la Cour de cassation¹ a considéré qu'une divulgation au grand public ne permettait pas de caractériser un motif légitime, la Cour rappelant « la nécessaire confidentialité de ce type d'informations » et le « risque d'utilisation à des fins de piratage » des failles de sécurité².

Afin de sécuriser juridiquement les activités de recherche ou de prestation de services de sécurité informatique, le législateur est à nouveau intervenu en 2013 lors de l'adoption de la loi de programmation militaire (LPM) 2014-2019 pour consacrer à l'article 323-3-1 les motifs légitimes « *de recherche ou de sécurité informatique* »³. Ces nouvelles dispositions permettent plus particulièrement d'assurer un cadre légal aux programmes de « Bug Bounty », c'est-à-dire des programmes visant « *à solliciter des chercheurs ou des hackers experts pour rechercher, sur une période donnée, les vulnérabilités sur une application ou un système* » selon l'ANSSI⁴, ou encore à la mise en œuvre de projets d'analyse de logiciels malveillants, notamment à travers des « Cyber Ranges » qui sont des simulateurs virtuels cyberdéfense⁵. On soulignera que parallèlement au renforcement de la sécurité juridique des activités privées de renseignement d'intérêt cyber, la loi de programmation militaire du 18 décembre 2013 a également explicitement autorisé les services de l'Etat en charge de la cyberdéfense dont les services de renseignement à « *détenir des équipements, des*

¹ Cass. crim., 27 octobre 2009, n° 09-82.346.

² Sur cette affaire, voir notamment A. Darsonville, *Le motif légitime dans l'infraction de trafic de moyens destinés à commettre des infractions en matière informatique*, op. cit. et J. Francillon, *Piratage informatique. Révélation de failles de sécurité informatique*, « *Infractions relevant du droit de l'information et de la communication* », Revue de science criminelle et de droit pénal comparé, vol. 1, no. 1, 2010, pp. 170-181.

³ Voir sur ce point J. -L. Carrère, *Rapport sur le projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, Sénat, 8 octobre 2013, p. 191 et 192.

⁴ Sur le « Bug Bounty », voir la plaquette d'informations de l'ANSSI à propos du volet cyber de France Relance : [anssi-france_reliance-bug_bounty.pdf](https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_reliance-bug_bounty.pdf) (https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_reliance-bug_bounty.pdf) et l'article de L. Dubau, *CYBERSECURITE : L'AGILITE DES ORGANISATIONS EN QUESTION*. Congrès Lambda Mu 21, " Maîtrise des risques et transformation numérique : opportunités et menaces ", Oct 2018, Reims, France.

⁵ Sur les « Cyber Ranges », voir par exemple la plaquette d'informations du National Institute of Standards and Technology du Département du commerce américain : [cyber_ranges.pdf \(nist.gov\)](https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf) (https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf).

instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 323-1 à 323-3 du code pénal, en vue d'analyser leur conception et d'observer leur fonctionnement »¹. On remarquera que la reconnaissance juridique du renseignement d'intérêt cyber s'accompagne d'une harmonisation de son cadre légal entre les acteurs publics et privés du secteur au regard des similitudes des dispositions du code de la défense avec celles de l'article 323-3-1 du code pénal.

2. Un encadrement restrictif des partenariats public-privé de cyber-renseignement

Si la reconnaissance juridique du renseignement d'intérêt cyber devrait inciter à des partenariats public-privé de cyber-renseignement, il reste que le droit pénal et le cadre juridique de la cyberdéfense française tendent à limiter ces partenariats pour les services de renseignement. En effet, le mouvement de dépénalisation des « *hackers* blancs » (ou « *white hats* » en anglais) considérés comme des lanceurs d'alertes par certains auteurs² s'est prolongé avec la loi pour une République numérique du 7 octobre 2016 créant l'article L. 2321-4 du code de la défense qui offre une certaine protection pénale en cas de divulgation de failles de sécurité informatique à l'ANSSI. Le dispositif permet aux agents de l'Agence de ne pas être contraints d'appliquer l'article 40 du code de procédure pénale lorsqu'un hacker de bonne foi leur transmet une faille de sécurité informatique et de garantir la confidentialité du « *hacker* » et des conditions d'obtention des informations transmises³. En revanche, le texte prévoit que la seule autorité nationale pouvant être informée est l'ANSSI, ce qui implique que les services de renseignement français ne devraient pas pouvoir recourir à des *hackers* privés pour collecter des failles de sécurité informatique au regard du risque d'une éventuelle saisine du procureur de la République. En effet, les agents des services demeurent soumis à l'article 40 du code de procédure pénale et au

¹ Alinéa 2 de l'article L. 2321-2 du code de la défense.

² En ce sens, voir F. Mattatia, « *Faut-il dépénaliser les hackers blancs ?* », Revue de science criminelle et de droit pénal comparé, vol. 4, no. 4, 2015, pp. 837-846 et E. A. Caprioli, *Le régime des lanceurs d'alertes de sécurité dans la loi pour une République numérique*, Communication Commerce électronique n° 1, Janvier 2017, comm. 9.

³ Voir à ce sujet, C. -A. Frassa, *Rapport sur le projet de loi pour une République numérique*, Tome 1, Sénat, 6 avril 2016, p. 120 à 122 et E. A. Caprioli, *Le régime des lanceurs d'alertes de sécurité dans la loi pour une République numérique*, op. cit..

principe de primauté de l'autorité judiciaire en cas de connaissance d'une infraction. A notre sens, la dépénalisation des « *hackers* blancs » étant fondée sur l'idée d'une protection collective de la sécurité des systèmes d'information et du cyberspace, la solution de n'avoir que l'ANSSI comme interlocuteur légitime nous apparaît juste au regard des risques avérés de détention secrète de vulnérabilités informatiques par des agences de renseignement qui peuvent en perdre le contrôle comme en témoigne l'affaire *WannaCry* de 2017 avec la NSA¹. Toutefois, rien ne semble interdire un échange d'information sur les failles de sécurité informatique entre l'ANSSI et les services de renseignement qui collaborent au sein du centre de coordination des crises cyber (C4)². Placée sous l'égide du Secrétariat général de la défense et de la sécurité nationale (SGDSN), cette instance stratégique et opérationnelle s'assure de la coordination interministérielle des moyens défensifs et offensifs, civils et militaires, de lutte informatique en matière de traitement des cyberattaques³.

Au-delà du renseignement d'intérêt cyber, le besoin de recourir à une externalisation du renseignement numérique semble se confirmer en France sans pour autant aller jusqu'à une privatisation comme observée aux Etats-Unis⁴. Ici, les limites des partenariats avec des entreprises privées du cyber-renseignement pèsent sur ces dernières qui se voient appliquer pleinement le droit pénal du numérique. Autrement dit, ces entreprises ne bénéficient d'aucune protection pénale particulière lorsqu'elles collaborent avec les services de renseignement qui ne peuvent aucunement déléguer leurs prérogatives inhérentes aux missions de souveraineté de l'Etat en vertu de l'article L. 811-1 du code de la sécurité intérieure et de la jurisprudence du Conseil constitutionnel⁵. Tout au plus, elles peuvent se

¹ Voir l'article Le Monde, *Le rançongiciel WannaCry ravive le débat sur les failles de sécurité*, 16 mai 2017, https://www.lemonde.fr/pixels/article/2017/05/16/le-rancongiel-wannacry-ravive-le-debat-sur-les-failles-de-securite_5128242_4408996.html.

² Sur ce point, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 252 à 255.

³ A ce sujet, voir notamment O. Cadic et M. Vallet, *Rapport d'information pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024-2030*, Sénat, p. 24 mai 2023, p. 12 à 15.

⁴ En ce sens, voir J. -C. Cousseran et P. Hayez, *Leçon sur le Renseignement*, op. cit., p. 293 et suivantes ; O. Chopin et B. Oudet, *Renseignement et sécurité*, op. cit., p. 178 à 183 ; C. Lepri, « *Les services de renseignement en quête d'identité : quel rôle dans un monde globalisé ?* », *Géoéconomie*, vol. 45, no. 2, 2008, pp. 33-53 ; G. -H. Bricet, « *Les technologies de renseignement en France : à la recherche d'un modèle de développement* », *Revue Défense Nationale*, vol. 825, no. 10, 2019, pp. 83-89.

⁵ Décision n° 2002-461 du 29 août 2002, *Loi d'orientation et de programmation pour la justice*.

voir appliquer le droit de la protection du secret de la défense nationale lorsqu'elles en sont dépositaires, ce qui constitue une lourde responsabilité. En définitive, les partenariats avec des acteurs privés exerçant des activités de cyber-renseignement seraient limités principalement aux échanges d'informations soit sur le fonctionnement des moyens de piratage informatique, soit sur toutes autres informations stratégiques ouvertes obtenues de manière licite sur internet.

Cette dernière hypothèse nous conduit à évoquer l'acquisition de données commercialement accessibles par les services de renseignement, une pratique reconnue par les Etats-Unis dans un rapport dédié de 2022 du bureau du « *Director of National Intelligence* »¹. Il s'agit pour les services d'acheter de nombreuses données à des courtiers en données (« *data brokers* » en anglais), c'est-à-dire des entreprises qui collectent en sources ouvertes et agrègent des données personnelles ou sur des organisations afin de les revendre. Cette activité est controversée en raison des atteintes susceptibles d'être commises aux données personnelles ou à des informations juridiquement et techniquement protégées, à plus forte raison qu'en les clients sont des services de renseignement. Le rapport américain précité ne manque pas de souligner ces risques tout en rappelant que ce mode de recueil de renseignements est stratégique pour les services spécialisés dans une société de l'information mondialisée. Il convient aussi de prendre en compte l'existence du « marché noir » de données collectées en dehors de tout cadre légal ou illicitement, trafic à l'origine par exemple de l'affaire médiatique *Cambridge Analytica* d'exploitation abusive de données de millions d'utilisateurs Facebook. En France, des opérations d'achat de données par les services de renseignement nécessitent de tenir compte des droits européen et français des données personnelles et du secret professionnel, notamment leur volet pénal. A ce titre, l'achat de données faisant l'objet d'une protection juridique devraient répondre aux missions des services de renseignement², être proportionné et contrôlé. Sur ce dernier point, un contrôle interne pourrait être organisé pour autoriser et superviser les opérations commerciales et un contrôle externe dédié de la CNIL ou de la CNCTR est à prévoir, selon nous, dans le cadre du contrôle plus

¹ Cf. Office of the Director of National Intelligence, Senior Advisory Group, Panel on Commercially Available Information, Report the Director of National Intelligence, 27 January 2022.

² Article L. 811-2 du code de la sécurité intérieure.

large des fichiers des services. Notons que ce type d'opération devrait également faire l'objet d'un contrôle financier au regard de sa nature transactionnelle. Par ailleurs, le droit du renseignement autorise explicitement l'acquisition de données personnelles de personnes susceptibles de porter atteinte aux intérêts fondamentaux de la Nation par des « cyber-patrouilleurs »¹. Cette disposition peut s'avérer utile dans l'élaboration d'un encadrement spécifique de l'achat de données sur le « marché noir » numérique comme sur le *dark web* par exemple.

En plus d'encadrer les activités du cyber-renseignement, le droit pénal du numérique est invoqué pour déterminer les appareils et dispositifs techniques de renseignement mentionnés dans la loi du 24 juillet 2015.

¹ Article L. 863-1-2° du code de la sécurité intérieure.

SECTION II : La détermination des appareils et dispositifs techniques de renseignement

En consacrant de nouvelles techniques de renseignement directement mises en œuvre par les agents des services de renseignement, le législateur de 2015 a souhaité qualifier avec plus de précisions les appareils et dispositifs techniques utilisés en faisant référence au 1° de l'article 226-3 du code pénal (§1). En l'absence d'une autorisation administrative, l'article prohibe « *la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer [les infractions d'atteintes au secret des correspondances électroniques ou à l'intimité de la vie privée] ou ayant pour objet la captation de données informatiques* ». Cette référence au régime d'autorisation de l'article 226-3 n'est pas sans conséquences dans l'encadrement juridique de la numérisation du renseignement (§2).

§1. La référence aux appareils ou dispositifs techniques mentionnés au 1° de l'article 226-3 du code pénal

D'une part, les dispositions de la loi du 24 juillet 2015 relative au renseignement et du 1° de l'article 226-3 du code pénal précisent les techniques de renseignement concernées par l'usage d'appareils ou dispositifs techniques d'espionnage. D'autre part, une liste de ces derniers est fixée par arrêté du Premier ministre¹, ce qui permet de déterminer les appareils ou dispositifs techniques entrant dans le champ d'application des techniques de renseignement concernées.

A - Les techniques de renseignement concernées

Les techniques concernées sont visées par le code de la sécurité intérieure et par le code pénal.

1. Les techniques visées par le code de la sécurité intérieure

Parmi les techniques de renseignement mentionnées au code de la sécurité intérieure, l'utilisation d'appareils ou dispositifs techniques mentionnés au 1° de l'article 226-3 a été circonscrite :

¹ Article R. 226-1 du code pénal.

- aux recueils directs à distance de données de connexion d'un équipement terminal autorisés à l'article L. 851-6 du code de la sécurité intérieure ;
- aux interceptions de sécurité à distance d'un équipement terminal autorisées au II de l'article L. 852-1 du code de la sécurité intérieure ;
- aux interceptions de sécurité à distance des communications par voie satellitaire autorisées à l'article L. 852-3 du code de la sécurité intérieure depuis la loi n° 2021-998 du 30 juillet 2021.

Initialement qualifiées de techniques de renseignement « *au moyen d'un « dispositif technique de proximité* » » au regard du système de collecte de données à distance pour surveiller une cible en temps réel située dans une zone proche de l'agent utilisateur, le législateur de 2015 a finalement préféré renvoyer le dispositif juridique au régime de l'article 226-3 du code pénal afin de proposer « un dispositif plus complet »¹. Contrairement à l'avis de la Commission nationale consultative des droits de l'homme (CNCDH) selon lequel la référence à l'article 226-3 manquait en qualité et réduisait la prévisibilité de la loi², il nous semble que cette référence permet d'être plus précis dans la détermination des outils numériques intrusifs pour la vie privée utilisés par les services de renseignement.

2. Les techniques visées par le code pénal

Au-delà des techniques mentionnées précédemment, les dispositions du 1° de l'article 226-3 affirment que les appareils ou dispositifs techniques soumis à autorisation sont également ceux qui doivent être utilisés dans le cadre des techniques de sonorisation et de captation de données informatiques³. Effectivement, le texte du code pénal fait lui-même référence aux techniques permettant la réalisation de l'infraction d'atteinte à l'intimité de la vie privée⁴ et directement à l'article L. 853-2 du code de la sécurité intérieure pour la captation de données informatiques. On soulignera que cette solution confirme notre analyse sur les similitudes entre les infractions pénales du numérique et les

¹ Sur le choix de la référence à l'article 226-3, voir J. -J. Urvoas, *Rapport sur le projet de loi relatif au renseignement*, op. cit., p. 198 à 200.

² Cf. CNCDH, Avis sur le projet de loi relatif au renseignement dans sa version enregistrée le 1er avril 2015 à la présidence de l'Assemblée nationale.

³ Articles L. 853-1 à L. 853-3 du code de la sécurité intérieure.

⁴ Article 226-1 du code pénal.

techniques de renseignement. Par ailleurs, on notera que l'absence de référence à l'article 226-3 dans les dispositions de l'article L. 853-2 a pu être remarquée par Floran Vadillo qui proposait alors une modification de l'article du code de la sécurité intérieure¹. Pour notre part, on rappellera qu'en matière de captation judiciaire, l'article 706-102-1 du code de procédure pénale, également cité par l'article 226-3, ne procède pas non plus à un renvoi. En outre, le texte du code pénal comme la liste fixée par arrêté du Premier ministre nous semblent suffisamment clairs et intelligibles pour être articulés avec les dispositions du code de la sécurité intérieure.

B - La liste des appareils ou dispositifs techniques

Conformément à l'article R. 226-1 du code pénal, la liste des appareils et dispositifs techniques prévue par l'article 226-3 du même code est établie par arrêté du Premier ministre dont l'exécution a été confiée au secrétaire général de la défense et de la sécurité nationale (SGDSN) puis au directeur général de l'ANSSI depuis l'arrêté du 4 juillet 2012². Régulièrement modifié pour s'adapter aux nouvelles technologies, cet arrêté constitue le socle réglementaire de la liste des appareils et dispositifs techniques qui figure en ses annexes I et II. A partir de la dernière modification réalisée par un arrêté du 11 août 2016³, il est possible de dresser un tableau relationnel entre les techniques de renseignement concernées et la liste prévue pour l'application de l'article 226-3.

¹ Cf. F. Vadillo, *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, op. cit. (Préconisation n° 14).

² Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal.

³ Arrêté du 11 août 2016 modifiant l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal.

**Tableau relationnel des techniques de renseignement et des appareils
et dispositifs techniques**

Techniques de renseignement	Appareils et dispositifs techniques
• Accès aux données de connexion autorisés par l'article L. 851-6 • Interceptions de sécurité autorisées par les articles L. 852-1-II et L. 852-3	Appareils, à savoir tous dispositifs matériels et logiciels, conçus pour réaliser l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances émises, transmises ou reçues sur des réseaux de communications électroniques, opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 du code pénal. Entrent notamment dans cette catégorie : • les appareils qui permettent aux opérateurs de communications électroniques de connecter les équipements de leurs clients au cœur de leur réseau radioélectrique mobile ouvert au public, dès lors que ces appareils disposent de fonctionnalités, pouvant être configurées et activées à distance, permettant de dupliquer les correspondances des clients, à l'exclusion des appareils installés chez ceux-ci ; • les appareils dont les fonctionnalités qui participent à l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances ne sont pas activées, quel que soit le moyen d'activation ; • les appareils permettant, par des techniques non intrusives d'induction électromagnétique ou de couplage optique, d'intercepter ou d'écouter les correspondances transitant sur les câbles filaires ou les câbles optiques des réseaux de communications électroniques.
Sonorisation autorisée par l'article L. 853-1	Appareils qui, spécifiquement conçus pour détecter à distance les conversations afin de réaliser à l'insu du locuteur l'interception, l'écoute ou la retransmission de la parole, directement ou indirectement, par des moyens acoustiques, électromagnétiques ou optiques, permettent de réaliser l'infraction prévue par l'article 226-1 du code pénal. Entrent dans cette catégorie : • les dispositifs microémetteurs permettant la retransmission de la voix par moyens hertziens, optiques ou filaires, à l'insu du locuteur ; • les appareils d'interception du son à distance de type microcanon ou équipés de dispositifs d'amplification acoustique ; • les systèmes d'écoute à distance par faisceaux laser.
Captation de données informatiques autorisée par l'article L. 853-2	Dispositifs techniques, à savoir tous matériels ou logiciels, spécifiquement conçus pour, sans le consentement des intéressés, accéder aux données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères, opérations ayant pour objet la captation de données informatiques prévue par l'article 706-102-1 du code de procédure pénale.

Deux remarques peuvent être faites sur l'articulation de la liste des appareils et dispositifs techniques et des techniques de renseignement. D'une part, il convient de préciser que les techniques de recueil et d'interception des articles L. 851-6 et L. 852-1-II du code de la sécurité intérieure devraient pouvoir s'adapter aux évolutions de la technologie 5G avec l'entrée en vigueur le 1^{er} octobre 2021 des dispositions de l'arrêté du 11 août 2016 sur les antennes relais des réseaux de téléphonie mobile, ce qui va dans le sens d'un renforcement des moyens numériques du renseignement et de la coopération des services avec les opérateurs de télécommunications¹.

D'autre part, on relèvera que la liste des appareils entrant dans la catégorie des accès aux données de connexion et des interceptions de sécurité susceptibles de constituer l'infraction prévue à l'article 226-15 du code pénal n'est pas exhaustive. Pour l'Autorité de régulation des communications électroniques et des postes (ARCEP), *« une telle liste non exhaustive est source d'incertitude car elle ne permet pas aux équipementiers et aux opérateurs de savoir précisément si d'autres appareils que ceux qui apparaissent dans la liste doivent être soumis à autorisation »* et préconise de la rendre exhaustive². La même incertitude peut être relevée pour les services de renseignement dans la fabrication ou l'acquisition de nouveaux outils de surveillance car ils subissent les conséquences de la référence au régime d'autorisation de l'article 226-3 du code pénal.

¹ En ce sens, voir E. A. Caprioli, *Interception légale de sécurité*, Communication Commerce électronique n° 10, Octobre 2016, comm. 87.

² Cf. ARCEP, Avis n° 2016-0449 du 29 mars 2016 sur le projet d'arrêté modifiant l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du Code pénal.

§2. Les conséquences de la référence au régime d'autorisation de l'article 226-3 du code pénal

Non seulement le régime du code pénal que l'on qualifiera de « régime d'autorisation 226-3 » s'applique aux services de renseignement, mais il implique également un contrôle sur les appareils et dispositifs techniques utilisés par les agents des services.

A - L'application du « régime d'autorisation 226-3 »

En procédant au renvoi à l'article 226-3, le dispositif retenu par le législateur de 2015 oblige les services de renseignement à obtenir une autorisation de détention des appareils ou dispositifs techniques préalablement à leur autorisation de mise en œuvre pour la surveillance d'une cible¹. La procédure d'autorisation est prévue par décrets dont les dispositions réglementaires sont codifiées aux articles R. 226-1 à R. 226-12 du code pénal. Sur demande déposée auprès du directeur de l'ANSSI, deux types d'autorisation peuvent être accordées :

- pour « *la fabrication, l'importation, l'exposition, l'offre, la location ou la vente de tout appareil ou dispositif technique* »² ;
- pour « *l'acquisition ou la détention de tout appareil ou dispositif technique* »³.

Toutes les demandes d'autorisation sont soumises à un avis préalable d'une commission consultative composée du directeur de l'ANSSI et de représentants ministériels et d'autorités administratives indépendantes, notamment la CNCTR, ainsi que de deux personnalités compétentes désignées par le Premier ministre⁴. On notera que cette commission est également saisie pour avis des projets d'arrêtés fixant la liste des appareils et dispositifs techniques. Les autorisations sont limitées dans le temps – maximum six ans pour le cas de l'article R. 226-3 et trois ans pour celui de l'article R. 226-7 – et peuvent conditionner l'usage et le déploiement des appareils ou dispositifs techniques. Toutefois, la procédure

¹ Sur l'affirmation de l'application de la procédure d'autorisation, voir J. -J. Urvoas, *Rapport sur le projet de loi relatif au renseignement*, op. cit., p. 198 à 200

² Article R. 226-3 du code pénal.

³ Article R. 226-7 du code pénal.

⁴ Article R. 226-2 du code pénal.

d'autorisation a été aménagée pour les services de renseignement à la suite de l'adoption de la loi du 24 juillet 2015.

1. Une autorisation de plein droit

Le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement a consacré une autorisation de plein droit limitée à la fabrication, à l'acquisition et à la détention des appareils ou dispositifs techniques¹.

Selon une instruction du SGDSN du 5 septembre 2006 dont les modalités qui étaient applicables aux interceptions de sécurité antérieures à la loi de 2015 pourraient être encore en vigueur², l'autorisation de plein droit ne devrait pas exclure les services de faire une demande d'autorisation soumise à l'avis de la commission consultative afin de s'assurer de l'habilitation des agents destinataires des appareils et dispositifs techniques.

2. La nécessité d'un registre spécifique

En contrepartie de l'autorisation de plein droit, la CNCTR a recommandé que le registre retraçant l'ensemble des opérations relatives aux appareils et dispositifs techniques prévu à l'article R. 226-10 et défini par arrêté du 16 août 2006 puisse retracer « *non seulement les opérations de commercialisation portant sur les appareils et dispositifs techniques contrôlés mais également celles de fabrication* » et « *attester, même succinctement, les fonctionnalités des appareils et dispositifs techniques fabriqués ainsi que leur adéquation aux missions confiées aux services bénéficiaires de l'autorisation de plein droit* »³. Il convient de distinguer ce registre du « registre spécial » de mise en œuvre de la technique prévue à l'article L. 851-6 du code de la sécurité intérieure et qui devrait être également prévu pour les techniques des articles L. 852-1-II et L. 852-3 du même code selon la CNCTR⁴. Ces deux types de registre nous apparaissent nécessaires afin de garantir, pour reprendre les termes de la Commission, « *un contrôle efficace des atteintes portées*

¹ Articles R. 226-5 et R. 226-9 du code pénal.

² Instruction relative à la commercialisation et à l'acquisition ou détention des matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances.

³ CNCTR, Délibération n° 1/2016 du 14 janvier 2016.

⁴ Cf. CNCTR, 6^{ème} rapport annuel (2021), p. 161 et 162.

à la vie privée » via les appareils et dispositifs techniques d'espionnage soumis à autorisation.

B - Le contrôle des appareils et dispositifs techniques

L'application du « régime d'autorisation 226-3 » incite les services de renseignement à organiser un contrôle interne des demandes et de suivi des autorisations pour se prémunir contre le risque d'un retrait d'autorisation à la suite d'un contrôle externe ou de poursuites pénales fondées sur l'absence d'autorisation valable.

1. L'organisation d'un contrôle interne

Les autorisations de plein droit accordées aux services de renseignement de fabrication, d'acquisition et de détention des appareils et dispositifs techniques d'espionnage sont, a priori, contrôlées par les services dans le cadre du contrôle des techniques de renseignement. Toutefois, un contrôle plus spécifique peut être organisé au sein des directions techniques des services de renseignement à l'instar du dispositif mis en place au sein de la DGSI pour les captations de données informatiques en matière judiciaire. Centralisées au sein du Service technique national de captation judiciaire (STNCJ) rattaché à la direction technique de la DGSI, les opérations de conception et d'acquisition des outils de surveillance sont placées sous le contrôle de deux personnalités qualifiées habilitées au secret de la défense nationale qui disposent d'un accès permanent au STNCJ et à ses moyens techniques ainsi que d'un droit à toute information nécessaire à l'exercice de leur mission de contrôle¹.

2. L'affirmation d'un contrôle externe

Les services de renseignement et leurs agents habilités à recourir à des appareils ou dispositifs techniques mentionnés au 1° de l'article 226-3 s'engagent à se soumettre à un contrôle externe exercé par l'ANSSI et la commission consultative sur le respect des indications fournies lors de la demande d'autorisation². Comme en matière de techniques de renseignement, le contrôle

¹ Arrêté du 9 mai 2018 portant création du service à compétence nationale dénommé « service technique national de captation judiciaire » et voir aussi M. Audibert, « *La pénétration du droit pénal dans l'espace privé. La captation de données informatiques* », Archives de politique criminelle, vol. 43, no. 1, 2021, pp. 91-103.

² Articles R. 226-4 et R. 226-8 du code pénal.

s'exerce *a priori* lors de la demande d'autorisation et *a posteriori*, de manière inopinée, durant la durée de mise en œuvre de l'autorisation¹. Dans le premier cas, il s'agit notamment de vérifier que les agents titulaires de l'autorisation répondent aux conditions techniques et de moralité. Dans le second cas, les contrôles portent sur le registre qui retrace les opérations relatives aux matériels autorisés et sur le fonctionnement de ces derniers.

3. La sanction, le retrait d'autorisation

Le contrôle des appareils et dispositifs techniques s'accompagne d'une sanction de retrait d'autorisation dans des cas spécialement prévus par le code pénal qui peuvent être classés en deux catégories : le retrait administratif et le retrait en cas de condamnation pénale². Selon l'article R. 226-11 du code pénal, l'autorisation peut être retirée par le Premier ministre après instruction du dossier par l'ANSSI lorsque l'autorisation est modifiée (circonstances nouvelles ou cessation d'activité du titulaire de l'autorisation) ou en cas de manquement aux obligations du « régime d'autorisation 226-3 » (fausse déclaration ou faux renseignement ou non-respect de la procédure ou des conditions d'application de l'autorisation). Dans le cadre de cette procédure de retrait, il est prévu que le titulaire de l'autorisation puisse faire valoir ses observations, sauf urgence. En revanche, l'article R. 226-11 met fin à l'autorisation de plein droit en cas de condamnation du titulaire pour les infractions d'atteintes à l'intimité de la vie privée ou au secret des correspondances électroniques. A notre sens, il aurait pu être ajouté à ces dernières, les infractions d'atteintes à un système de traitement automatisé de données ou aux données personnelles qui peuvent être réalisées par la technique de captation de données informatiques dont les moyens matériels entrent dans le champ du « régime d'autorisation 226-3 » mais aussi l'infraction d'atteinte au secret de la défense nationale lorsqu'elle concerne un matériel classifié. On comprendrait difficilement que les dispositions de l'article R. 226-11 ne s'appliquent pas à un agent titulaire d'une autorisation condamné pour compromission du secret de la défense nationale concernant les capacités des

¹ Instruction relative à la commercialisation et à l'acquisition ou détention des matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances.

² Instruction relative à la commercialisation et à l'acquisition ou détention des matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances.

services de renseignement. Par ailleurs, on rappellera que la mise en œuvre d'appareils ou dispositifs techniques mentionnés au 1° de l'article 226-3 sans autorisation relative à leur fabrication, acquisition et détention par un service de renseignement constitue une infraction pénale.

Ainsi, les techniques de renseignement directement mises en œuvre par des agents sont particulièrement encadrées par un double régime préventif d'autorisation et des contrôles portant donc à la fois sur l'activité de surveillance et sur les outils techniques de surveillance. A ce titre, on remarquera qu'un retrait d'autorisation sur les appareils ou dispositifs techniques pourrait remettre en cause une autorisation de mise en œuvre d'une technique de renseignement, sauf à prévoir un transfert des autorisations à un agent habilité, notamment en application de l'article R. 226-12 du code pénal.

CONCLUSION DU TITRE

La diffusion du droit européen relatif à la vie privée numérique dans l'encadrement juridique des activités de surveillance et la réaffirmation du droit pénal du numérique dans le corpus juridique applicable aux services de renseignement mettent en lumière les intrications inévitables du droit du renseignement et du droit du numérique pour encadrer la numérisation du renseignement d'Etat.

Au fondement de l'élaboration du droit du renseignement numérique, le droit européen n'a pas été seulement une source d'inspiration pour le législateur français, qui n'a pas manqué de s'accorder chaque fois que nécessaire avec la jurisprudence de la CEDH, mais aussi un droit vivant de la surveillance numérique sous le contrôle de la CJUE qui tend à aligner les Etats membres sur des principes communs. Si la jurisprudence des juges européens considère que « la vie privée n'a pas valeur de loi absolue », pour reprendre les termes des Professeurs Loïc Azoulai et Dominique Rittleng à propos de la CJUE¹, il nous semble que le droit européen a le mérite d'avoir clairement interdit de définir la surveillance numérique généralisée par défaut comme la norme en Europe face aux inquiétudes de l'affaire PRISM de 2013². On ne manquera pas non plus, ici, de souligner que les juges européens ont reconnu que la surveillance massive des communications numériques, notamment des journalistes, peut avoir des effets dissuasifs pour l'exercice des libertés d'expression, de communication et d'information³. A cet égard, soulignons que le droit français du renseignement interdit, sur le territoire national, l'utilisation des techniques de renseignement à l'encontre des parlementaires, magistrats, avocats ou journalistes à raison de l'exercice de leur mandat ou profession même en cas d'urgence⁴. On approuvera également l'affirmation de l'importance de l'humain dans le contrôle des machines

¹ Cf. L. Azoulai et D. Rittleng, « *L'État, c'est moi* ». *Le Conseil d'État, la sécurité et la conservation des données*, op. cit..

² Sur les inquiétudes de l'affaire PRISM, voir notamment CNIL, *Rapport d'activité 2013*, p. 4 à 6.

³ Voir notamment les affaires *Weber et Saravia* de 2006 (points 139 et suivants) et *Big Brother Watch* de 2021 (points 428 à 458) de la CEDH et C-511/18, *La Quadrature du Net* (points 118, 173 et 186) et C-623/17, *Privacy International* (point 72) de la CJUE du 6 octobre 2020.

⁴ Article L. 821-7 du code de la sécurité intérieure.

par les juges européens qui sont allés jusqu'à définir le socle d'une régulation du recours au Big data et aux algorithmes d'intelligence artificielle.

On peut toujours s'inquiéter d'un risque de divergence d'interprétation sur le droit à la vie privée numérique entre la CEDH et la CJUE qui pourrait nuire aux activités du renseignement comme le rappelle Fabien Lafouasse¹, mais il est certain que le dialogue bienveillant entretenu entre l'ordre juridique interne français et l'ordre juridique européen renforce l'Etat de droit et la légitimité des services de renseignement. Pour pérenniser ce dialogue bienveillant, le droit du renseignement, d'essence régaliennne, se doit donc d'admettre son indéniable européanisation et, inversement, le droit européen de reconnaître les impératifs étatiques de la sécurité nationale. Au rapport vertical entre le droit du renseignement comme droit dérogatoire au droit au respect de la vie privée, il convient d'ajouter un rapport horizontal entre ces deux droits dans le cadre du dialogue entre les ordres de juridictions. Sauf revirement, le droit européen et le droit du renseignement devraient continuer à s'enrichir l'un de l'autre pour répondre aux défis technologiques et de la construction européenne. D'autant plus qu'une coopération européenne en matière de renseignement se construit progressivement, notamment à travers les échanges entre les instances spécialisées de contrôle, même si le renseignement demeure une compétence de souveraineté encore difficile à transférer à une communauté d'Etats comme l'Union européenne².

En ce qui concerne l'intrication du droit du renseignement avec le droit pénal du numérique, notre analyse tend à démontrer que, contrairement à ce qu'a pu soutenir Jean-Marie Delarue³, le recours à des moyens numériques de renseignement repose juridiquement sur un régime d'autorisation protecteur pour les services en ce qui concerne les techniques les plus intrusives mais aussi sur les infractions pénales relevant de la cybercriminalité s'agissant de l'ensemble des activités du renseignement numérique. Cependant, il convient d'admettre que

¹ Cf. F. Lafouasse, *Le droit du renseignement : un droit conforme aux traités internationaux*, Le droit du renseignement, op. cit., p. 187 à 199.

² Voir en ce sens, Y. Braun-Pivet, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018*, op. cit., p. 67 à 81 et O. Brun, « Union européenne », Hugues Moutouh éd., *Dictionnaire du renseignement*, op. cit., pp. 801-804.

³ Cf. J. -M. Delarue, *Renseignement et sphère privée*, op. cit., p. 89.

le droit du renseignement fait moins preuve de neutralité technologique que le code pénal en matière d'atteintes à la vie privée. Toutefois, on remarquera que le « régime d'autorisation 226-3 » qui établit la liste des appareils et dispositifs techniques d'espionnage prohibés implique nécessairement une régulation suivant les évolutions des technologies comme l'exemple du déploiement de la 5G.

Pour autant, il est vrai que le droit du renseignement a tenu à préserver les agents des services contre les risques de poursuites judiciaires, notamment dans le cadre de la lutte contre la cybercriminalité internationale. Cette conciliation délicate entre le droit pénal du numérique et le droit du renseignement nous apparaît cependant équilibrée pour ne pas compromettre les capacités opérationnelles des services et la souveraineté de la France. Cependant, il nous semble que le législateur aurait pu aller plus loin pour rétablir un certain équilibre en permettant à la formation spécialisée du Conseil d'Etat de statuer sur la déclassification des éléments à transmettre au parquet en cas de contentieux pénal. Pour l'heure, le secret de la défense nationale constitue un obstacle de taille pour invoquer le droit pénal comme une garantie contre les risques d'abus du renseignement d'Etat en l'absence d'une procédure de déclassification réellement contraignante pour l'administration.

Malgré une conciliation favorable aux agents des services de renseignement, le droit pénal du numérique demeure un outil précieux dans la régulation de la numérisation du renseignement. Il permet de délimiter juridiquement les interactions entre les services de renseignement et les acteurs privés exerçant des activités de cyber-renseignement. Et surtout, la référence au « régime d'autorisation 226-3 » a pour conséquence de soumettre les services de renseignement à des contrôles de l'ordre administratif et de l'ordre judiciaire à la fois sur les mesures de surveillance et sur les technologies mobilisées.

Loin d'être suffisamment autonome et complet pour garantir une protection adaptée des individus contre les risques d'une surveillance étatique abusive, le droit du renseignement s'est intriqué avec le droit du numérique. Cette intrication présente l'avantage de renforcer le respect des droits fondamentaux et de l'Etat de droit tout en précisant les responsabilités des agents des services de renseignement. En ce sens, elle participe à l'émergence d'une régulation publique

protectrice du cyberspace qui vise à garantir un cyberspace pacifié et techniquement fiable.

TITRE II

LE RENSEIGNEMENT ET LA PROTECTION DU CYBERESPACE

Depuis les cyberattaques de 2007 visant à perturber les institutions publiques de l'Estonie, la communauté internationale a pris véritablement conscience que le cyberspace est devenu un lieu de conflictualité à part entière où les services de renseignement jouent un rôle de premier plan, notamment d'un point de vue offensif. Cette « militarisation » du cyberspace fait l'objet d'une production juridique intensive pour l'encadrer, les services de renseignement n'étant pas épargnés par cette évolution (**Section I**). De même, l'action de ces derniers dans le cyberspace nécessite de se concilier avec les normes de cybersécurité au risque de perdre la confiance dans l'économie numérique (**Section II**).

CHAPITRE I

L'ENCADREMENT DE LA MILITARISATION DU CYBERESPACE

Dans l'encadrement de la militarisation du cyberspace, deux principales réponses juridiques trouvent à s'appliquer au renseignement numérique qui se voit contraint d'évoluer dans un nouvel environnement juridique : d'une part, l'élaboration progressive d'un droit de la cyberdéfense qui pose des limites juridiques aux cyberopérations étatiques (**Section I**) ; d'autre part, l'adaptation des instruments de contre-prolifération des biens et technologies sensibles aux outils numériques malveillants (**Section II**).

SECTION I : Le droit de la cyberdéfense applicable au renseignement

Les textes relatifs à la cyberdéfense consacrent une participation importante du renseignement dans l'organisation et le fonctionnement de l'action étatique sur les réseaux numériques (§1). Par ailleurs, la dimension internationale de la cyberdéfense impact nécessairement le cadre juridique des cyberopérations des services de renseignement, ces dernières pouvant faire l'objet d'une appréhension par le droit international applicable au cyberspace (§2).

§1. La participation du renseignement à la cyberdéfense

Alors que le cyberspace est un terme employé par la communauté internationale, celui de « cyberdéfense » reste essentiellement utilisé dans une conception française de l'action étatique sur les réseaux numériques¹. Depuis que le Livre blanc sur la défense et la sécurité nationale de 2008 a reconnu l'importance pour la France de se doter de capacités défensives et offensives dans le cyberspace, la notion de cyberdéfense n'a cessé de monter en puissance.

¹ En ce sens, voir A. Cattaruzza, D. Danet et S. Taillat, « *Introduction* », Stéphane Taillat éd., La Cyberdéfense. Politique de l'espace numérique. Armand Colin, 2018, pp. 4-13.

Initialement pensée comme la seule protection des informations de l'Etat¹, la stratégie de la France en matière de défense et de sécurité des systèmes d'information dévoilée par l'ANSSI, le 15 février 2011, a opté pour une proposition de définition plus large de la cyberdéfense : « *ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberspace les systèmes d'information jugés essentiels* »². Par la suite, la notion se précise et se militarise davantage avec l'affirmation du développement de capacités de cyberdéfense militaire dans le Livre blanc de 2013. Selon le vocabulaire de la défense, la cyberdéfense est désormais définie comme un « *ensemble des moyens mis en place par un État pour défendre dans le cyberspace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité* », ce qui implique qu'elle « *met notamment en œuvre la lutte informatique défensive et la lutte informatique offensive* »³. Consolidant ces considérations stratégiques et opérationnelles, la *Revue stratégique de cyberdéfense* du 12 février 2018 souligne que la cyberdéfense constitue l'aspect régalien de la cybersécurité⁴, cette dernière renvoyant à la capacité de résilience numérique de l'ensemble de la société depuis l'adoption de la directive « *NIS 1* » (Network and Information Security) de l'Union européenne du 6 juillet 2016⁵ et de sa loi de transposition du 26 février 2018⁶.

Sur le plan juridique, les lois de programmation militaire (LPM) pour 2014-2019 et 2019-2025 ont défini la cyberdéfense comme une activité régalienne relevant de la responsabilité exclusive de l'Etat dans le cadre de pouvoirs particuliers conférés par la loi⁷. Autrement dit, on reprendra l'affirmation du

¹ Sur ce point, voir J. -M. Bockel, *Rapport d'information sur la cyberdéfense*, Sénat, 18 juillet 2012, p. 76.

² ANSSI, *Défense et sécurité des systèmes d'information, Stratégie de la France*, 15 février 2011, p. 21.

³ Cf. Vocabulaire de la défense : cyberdéfense (liste de termes, expression et définitions adoptés), JORF, 19 septembre 2017, CTNR1724864K.

⁴ En ce sens, voir également M. Quémener, *Revue stratégique de cyberdéfense : cyberdéfense, cybersécurité, cybercriminalité, même combat*, Dalloz IP/IT 2018, p. 176.

⁵ Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

⁶ Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

⁷ En ce sens, voir B. Warusfel, *La cyberdéfense, dimension numérique de la sécurité nationale*, Chapitre 5, Conflits, crimes et régulations dans le cyberspace, Volume 4, Série Cybersécurité, ISTE, 2021, p. 106.

Général Marc Watin-Augouard sur l'instauration d'une « *nouvelle police administrative spéciale relevant du Premier ministre* »¹. En effet, l'article 21 de la LPM 2014-2019² dispose notamment que :

« *dans le cadre de la stratégie de sécurité nationale et de la politique de défense, le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information qui assure la fonction d'autorité nationale de défense des systèmes d'information* »³.

Dans le prolongement de ces dispositions, l'article 22 de la LPM 2014-2019 introduit de nouveaux pouvoirs pour le Premier ministre lui permettant d'imposer des règles et des contrôles de sécurité informatique aux opérateurs publics et privés d'importance vitale⁴. En outre, le législateur n'a pas manqué de confier au gouvernement des dispositifs de « gestion de crise » qui apparaissent indispensables pour répondre aux risques et menaces difficilement prévisibles dans le domaine cyber⁵, notamment avec la création d'une *posture permanente cyber* (PPC) au sein du ministère des Armées⁶ depuis la LPM 2019-2025.

Mais plus encore qu'un droit de police administrative, il convient en réalité d'inscrire le régime juridique de la cyberdéfense dans le droit de la sécurité nationale puisqu'elle vise à lutter contre les cybermenaces susceptibles d'affecter la vie de la Nation pouvant aller jusqu'à la « cyberguerre ». Fidèle à cette

¹ Cf. M. Watin-Augouard, *Cybermenaces et sécurité nationale*, Le droit de la sécurité et de la défense en 2013, op. cit., p. 297 à 312.

² 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.

³ Article L. 2321-1 du code de la défense.

⁴ Articles L. 1332-6-1 à L. 1332-6-6 du code de la défense.

⁵ En ce sens, voir A. Cattaruzza, D. Danet et S. Taillat, « *Introduction* », Stéphane Taillat éd., *La Cyberdéfense. Politique de l'espace numérique*, op. cit., pp. 4-13.

⁶ « *Placée sous le contrôle opérationnel du ComCyber, la PPC regroupe l'ensemble des mesures prises pour assurer la défense des forces armées dans le cyberspace, en temps de paix comme de crise, ou de guerre. Il s'agit d'une posture comparable, dans l'espace numérique, aux traditionnelles postures permanentes de sécurité maritime et aérienne. Elle vise à préserver la liberté d'action des forces armées et du ministère des Armées et recouvre trois missions principales : - la surveillance de l'espace numérique et la détection des atteintes affectant le ministère des Armées ; - la capacité des forces à se déployer en sécurité au regard des menaces provenant du cyberspace, et à accomplir leur mission ; - la réaction aux agressions informatiques ou informationnelles, y compris en prenant des mesures pour en faire cesser les effets* » (cf. C. Cambon, *Rapport relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*, op. cit., p. 30).

conception, l'article L. 2321-2 du code de la défense autorise spécifiquement les services de l'Etat sous la responsabilité du Premier ministre à « *répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* ». En ce sens, la cyberdéfense se rattache au concept de sécurité nationale et à son droit consacré par l'article L. 1111-1 du code de la défense qui dispose, d'une part, que « *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* » et, d'autre part, que « *la politique de défense a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées. Elle contribue à la lutte contre les autres menaces susceptibles de mettre en cause la sécurité nationale* ». On s'accordera avec l'idée du Professeur Bertrand Warusfel selon laquelle la cyberdéfense est la « dimension numérique de la sécurité nationale »¹. Cette analyse semble se confirmer au regard des moyens dérogatoires de lutte informatique accordés aux services en charge de la cyberdéfense qui sont intrusifs dans les libertés du commerce et de l'industrie ou dans le droit à la vie privée des individus, ce qui ne peut être justifié que pour les besoins de la sécurité nationale².

Il ressort de l'ensemble de ces dispositions que les services de renseignement sont amenés à jouer un rôle essentiel dans l'organisation de la cyberdéfense française en raison de leurs missions de sécurité nationale. Toutefois, on remarquera que si les actions du renseignement dans le cyberspace ou de « cyber-renseignement » peuvent consister « *à infiltrer les systèmes informatiques d'une organisation et à s'emparer de données pour exploiter, à des fins opérationnelles, les renseignements ainsi recueillis* »³, il ressort notamment de l'étude de la Délégation parlementaire au renseignement sur la cyberdéfense et les services de renseignement de 2020⁴ que le cyber-renseignement regroupe

¹ Cf. B. Warusfel, *La cyberdéfense, dimension numérique de la sécurité nationale*, Chapitre 5, Conflits, crimes et régulations dans le cyberspace, op. cit., p. 105 et suivantes.

² En ce sens, voir B. Warusfel, *Le contentieux de la sécurité nationale*, Annuaire 2018 du droit de la sécurité et de la défense, op. cit., p. 203 à 2018 et J. -C. Videlin, *La loi de programmation militaire 2019-2025 : une loi financière et... juridique*, AJDA 2018, p. 1894.

³ Cf. Vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés), CTNR1724864K, JORF n°0219 du 19 septembre 2017.

⁴ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 239 et suivantes.

l'ensemble des moyens intrusifs ou non de collecte d'informations d'intérêt cyber (RIC) ou d'origine cyber (ROC) ainsi que d'entrave des cybermenaces. Dans une approche matérielle, les textes relatifs à la cybersécurité laissent entendre que le cyber-renseignement ne se limite pas à l'action des services de renseignement.

A - L'action des services de renseignement dans la cybersécurité

La *Revue stratégique de cybersécurité* de 2018 laisse une large place aux services de renseignement dans les missions de cybersécurité, ce qui entraîne un élargissement du champ d'action du renseignement numérique d'Etat dans la société. S'agissant de leurs moyens, les services recourent aussi bien à l'ensemble de leurs moyens propres, notamment autorisés par les lois relatives au renseignement, qu'à ceux autorisés sous la responsabilité de l'ANSSI et du commandement de la cybersécurité (COMCYBER)¹ par le cadre juridique de la cybersécurité. Depuis sa création en 2009 et sa consécration en service nationale de cybersécurité en 2011² puis en 2013 par la LPM 2014-2019³, l'ANSSI a la responsabilité de la lutte informatique défensive (LID) mise en œuvre par les services de l'Etat. Par dérogation mais en coordination avec l'ANSSI, le COMCYBER a la responsabilité de la LID dans le secteur de la défense⁴. En outre, Le COMCYBER est le service de l'Etat de référence de la lutte informatique offensive (LIO), notamment dans le cadre de la posture permanente cyber (PPC) introduite par la LPM 2019-2025.

Les services de renseignement combinent alors des moyens de renseignement et d'entrave dans l'accomplissement de leurs missions. On relèvera que l'action des services de renseignement traduit un assouplissement pragmatique de la stricte séparation fonctionnelle entre LID et LIO fondant le modèle français de cybersécurité.

¹ Décret n° 2017-743 du 4 mai 2017 relatif aux attributions du chef d'état-major des armées.

² Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » modifié par le décret n° 2011-170 du 11 février 2011.

³ Article L. 2321-1 du code de la défense.

⁴ Alinéa 1 de l'article D. 3121-14-1 du code de la défense.

1. Les missions des services de renseignement dans la cyberdéfense

Selon la *Revue stratégique de cyberdéfense* de 2018, les services de renseignement assurent les missions d'anticipation conduite par l'ANSSI au sein de l'organe technico-opérationnel C4 TECHOPS couvert par le secret de la défense nationale, de détection et d'attribution des cyberattaques via notamment l'utilisation de leurs techniques de renseignement, de réaction en soutien aux opérations de LID, de répression contre la cybercriminalité ou de LIO ou dans le cadre d'opérations spéciales. La Revue ajoute qu'une chaîne opérationnelle « renseignement » sous l'autorité du gouvernement, avec la participation du CNRLT, doit être dédiée à la coordination et à la mutualisation des moyens des services de renseignement pour répondre aux missions de cyberdéfense.

En pratique, les services de renseignement semblent pourtant participer, en fonction de leurs prérogatives respectives, aux autres missions (prévention et protection) et chaînes opérationnelles de cyberdéfense (chaines protection, action militaire et investigation judiciaire) selon le rapport d'activité de la DPR de 2020, ce qui explique d'autant plus leur « contribution majeure »¹. Ainsi, on relèvera que la DRSD, dans le secteur de la défense, et la DGSI et le renseignement territorial participent à la mission de prévention et de sensibilisation des risques cyber dans le prolongement de leurs missions de contre-ingérence, de renseignement sur les menaces, d'intelligence économique et de protection du secret de la défense nationale. S'agissant de la protection des systèmes numériques relevant de la cyberdéfense, la DRSD joue également un rôle dans les mesures et les contrôles de sécurité des informations et matériels sensibles intéressant la défense. De son côté, il convient de souligner que la DGSE est autonome de l'ANSSI et du COMCYBER en ce qui concerne la cyberdéfense de ses systèmes numériques et ses capacités à mener des opérations dans le cyberspace². Enfin, ajoutons qu'en matière de réaction à une cyberattaque constituant une infraction d'atteinte aux intérêts fondamentaux de la Nation, la DGSI est le service enquêteur dans la chaîne

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 256 à 266.

² En ce sens, voir A. Desforges, *Séparation des fonctions offensive et défensive : l'originalité du modèle de cyberdéfense française remis en cause ?*, Chapitre 3, Conflits, crimes et régulations dans le cyberspace, op. cit., 2021, p. 65 à 87.

opérationnelle « investigation judiciaire » en raison de sa particularité d'être à la fois un service de renseignement et un service de police judiciaire.

La contribution des services de renseignement à l'ensemble des missions et chaînes opérationnelles de cyberdéfense a pour conséquence d'élargir la surveillance numérique des services de renseignement dans la société au regard des nombreux systèmes d'information qui sont entrés dans le champ de la cyberdéfense. Depuis la loi de programmation militaire du 18 décembre 2013¹, les missions de cyberdéfense concernent les systèmes d'information des opérateurs d'importance vitale ou « OIV » désignés par le pouvoir réglementaire², c'est-à-dire des personnes morales publiques ou privées indispensables à la vie de la Nation ou impactant la population et qui exercent leurs activités dans les secteurs régaliens civils et militaires, de la santé et de l'environnement, de l'énergie, des transports et des finances ou encore des technologies et de la recherche³. Ajoutons que les systèmes d'information des sous-traitants et prestataires des OIV sont également concernés⁴.

Par la suite, l'élaboration d'un droit européen de la cybersécurité avec l'adoption de la directive *NIS 1 (Network and Information Security)*⁵, qui vise à harmoniser les législations nationales sur les mesures de sécurité numérique et à identifier les opérateurs concernés par ces dernières, a permis d'élargir le champ d'application de la cyberdéfense⁶ et donc du cyber-renseignement aux opérateurs de services essentiels (OSE) relevant également des secteurs de l'énergie, des transports, des banques, des infrastructures de marchés financiers, de la santé, de l'eau potable et des infrastructures du numérique et qui sont identifiables par leur importance pour la société et l'économie, leur dépendance aux systèmes

¹ Article 22 de la loi de programmation militaire du 18 décembre 2013.

² Articles R. 1332-1 à R. 1332-42 du code de la défense.

³ Articles L. 1332-1 et L. 1332-2 du code de la défense.

⁴ Article L. 1332-6-1 du code de la défense.

⁵ Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

⁶ Les articles 5 à 9 de la loi de transposition n° 2018-133 du 26 février 2018 et son décret d'application n° 2018-384 du 23 mai 2018 ont mis en place un dispositif similaire à celui de la loi de programmation militaire pour les opérateurs de services essentiels (OSE) en matière de cyberdéfense.

numériques et par l'effet disruptif sur leurs activités en cas d'incident. Enfin, la directive NIS 2 du 14 décembre 2022¹ a prévu d'élargir à nouveau, et de manière considérable, le périmètre des entités soumises aux mesures de cybersécurité, ce qui devrait augmenter encore le nombre de systèmes d'information entrant dans le champ de la cyberdéfense.

Pouvant être considérés « *comme une des pierres angulaires de la stratégie française de cyberdéfense* » pour reprendre les termes d'Alix Desforges², les services de renseignement occupent une large place dans l'organisation de la cyberdéfense. Ils ont alors à leur disposition des moyens numériques importants et intrusifs de collecte d'informations, notamment pour l'anticipation, la détection et l'attribution des cyberattaques, mais aussi des moyens plus offensifs.

2. Les moyens de renseignement et d'entrave

Dans le cadre du droit de la cyberdéfense, la DGSE et la DGSi sont autorisés à réaliser des opérations techniques sous la responsabilité de l'ANSSI pour caractériser et neutraliser les effets d'une cyberattaque en application des dispositions de l'article L. 2321-2 du code de la défense³. Dans le périmètre du secteur de la défense, les opérations techniques prévues à l'article L. 2321-2 font intervenir la DRSD et la DRM au sein du COMCYBER. Plus concrètement, les opérations techniques consistent à identifier la ou les cybermenaces en cause (sabotage ou espionnage par exemple) en analysant le ou les outils malveillants ayant attaqué le ou les systèmes d'information. Pour ce qui concerne la neutralisation des effets d'une cyberattaque, il s'agit notamment d'isoler les systèmes infectés et d'endiguer la propagation de l'attaque, voire de faire cesser

¹ Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE).

² Cf. A. Desforges, *Séparation des fonctions offensive et défensive : l'originalité du modèle de cyberdéfense française remis en cause ?*, Chapitre 3, Conflits, crimes et régulations dans le cyberspace, op. cit., 2021, p. 65 à 87.

³ Le DGSE et la DGSi sont les services spécialisés de renseignement concernés selon l'arrêté du 17 juillet 2015 déterminant les services de l'Etat mentionnés au second alinéa de l'article 2321-2 du code de la défense et d'une instruction classifiée du 7 mars 2016 précisant les conditions de mises en œuvre du même article.

l'exfiltration de données ou la prise de contrôle à distance du système attaqué en neutralisant le serveur utilisé par l'attaquant¹.

En droit du renseignement, on rappellera que la cyberdéfense constitue une finalité opérationnelle reconnue des missions des services de renseignement par le Plan National d'Orientation du Renseignement (PNOR)². A ce titre, les services peuvent recourir à l'ensemble de leurs moyens, du renseignement d'origine sources ouvertes aux techniques les plus intrusives consacrées par les lois relatives au renseignement, pour anticiper, détecter mais aussi contribuer à l'attribution et à l'entrave des cybermenaces ou de toutes autres menaces en lien avec le cyberspace conformément à leur mission générale définie à l'article L. 811-2 du code de la sécurité intérieure.

Ainsi, les techniques de renseignement sont autorisées en matière de cyberdéfense lorsqu'elles sont justifiées par les finalités de l'article L. 811-3 du code de la sécurité intérieure. Parmi ces techniques, les services recourent principalement aux mesures de surveillance des communications internationales, notamment au dispositif de « vérifications ponctuelles » pour la détection d'une attaque informatique³, et à la captation de données informatiques⁴ pour le RIC comme pour le ROC⁵.

De manière plus offensive, les mesures de piratage informatique à l'étranger excusées par l'article 323-8 du code pénal peuvent être particulièrement invoquées par la DGSE pour mener des cyberopérations de LID contribuant à l'entrave des cybermenaces ou, plus encore, des opérations clandestines d'espionnage, voire de sabotage pouvant s'inscrire théoriquement dans la LIO ou dans des opérations spéciales dépassant le cadre de la cyberdéfense dans les limites des prérogatives du service de renseignement extérieur et de

¹ A titre d'exemple, on peut citer l'affaire des cybergendarmes français qui ont neutralisé en 2019 un serveur utilisé par des cybercriminels depuis 2016 pour infecter de très nombreux ordinateurs pour que ces derniers servent à voler des données ou à saboter des systèmes numériques par exemple (cf. E. Leclère, *Des cybergendarmes français neutralisent un serveur qui a infecté 850 000 ordinateurs à des fins crapuleuses*, franceinfo, France Inter, 28 août 2019).

² Cf. supra. §1 de la Section I du Chapitre I du Titre II de la Ière Partie.

³ Cf. supra. §3 de la Section II du Chapitre I du Titre I de la Ière Partie.

⁴ Article L. 853-2 du code de la sécurité intérieure.

⁵ A ce sujet, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 261 à 263.

l'article L. 811-2 du code de la sécurité intérieure. Ainsi, la DGSE ne devrait pas invoquer les dispositions de l'article 323-8 de façon autonome en matière de LIO. Une coordination avec le COMCYBER devrait s'imposer, notamment au regard des conséquences techniques, juridiques et géopolitiques que peuvent entraîner les mesures de l'article 323-8¹.

Ces considérations appellent deux remarques sur le contrôle des services de renseignement et de la cyberdéfense : d'une part, la DPR est amenée à évaluer la contribution des services dans la cyberdéfense avec l'aide du CNRLT et de l'ISR² mais également à être l'organe parlementaire le plus adapté pour contrôler la politique publique de cyberdéfense en raison de sa sensibilité et de la place qu'occupe le renseignement dans son dispositif³ ; d'autre part, la CNCTR et la formation spécialisée du Conseil d'Etat participent aux contrôles administratif et juridictionnel de la mise en œuvre de la cyberdéfense à travers le recours aux techniques de renseignement et son contentieux.

3. L'assouplissement du modèle français de cyberdéfense

Le modèle français de cyberdéfense repose sur une séparation fonctionnelle plus qu'organisationnelle entre lutte informatique défensive (LID) et lutte informatique offensive (LIO), même si ces fonctions sont principalement placées sous la responsabilité opérationnelle de l'ANSSI et du ministère des Armées. Selon le vocabulaire de la défense, la LID est un « *ensemble coordonné d'actions menées par un État, qui consistent à détecter, à analyser et à prévenir des cyberattaques, et à y réagir le cas échéant* »⁴. En ce qui concerne la LIO, cette fonction est plus restrictive en visant un « *ensemble coordonné d'actions menées dans le cyberspace par un État contre des systèmes d'information ou de données pour les perturber, les modifier, les dégrader ou les détruire* »⁵. Le COMCYBER est le service de l'Etat de référence de la LIO, notamment dans le cadre de la posture permanente cyber (PPC) introduite par la LPM 2019-2025. L'article 35 de cette loi

¹ Cf. supra. §3 de la Section II du Chapitre I du Titre I de la 1ère Partie.

² Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 262 et 263.

³ Dans le même sens, voir J. -M. Bockel, *Rapport d'information sur la cyberdéfense*, op. cit., p. 97.

⁴ Cf. Vocabulaire de la défense, J.O. du 19/09/2017.

⁵ Cf. Vocabulaire de la défense, J.O. du 19/09/2017.

a d'ailleurs consacré officiellement l'existence de la cyberdéfense militaire¹ et du « cyber-combattant » bénéficiant de l'excuse pénale des militaires en opération extérieure prévue à l'article L. 4123-12 du code de la défense².

En réalité, la séparation fonctionnelle entre LID et LIO n'est pas strictement respectée dans l'articulation entre le droit de la cyberdéfense et le droit du renseignement. En effet, la LID peut s'avérer très intrusive, voir même offensive dans sa mission de réaction à une cyberattaque, notamment lorsqu'elle est mise en œuvre par les services de renseignement. Certaines opérations techniques de neutralisation des effets d'une attaque informatique autorisées en vertu de l'article L. 2321-2 peuvent perturber les systèmes numériques de l'attaquant ou de tiers impliqués volontairement ou non. Ainsi, les opérations techniques de réaction dites « *active defense* » en anglais se situent dans une zone grise³. Comme au niveau du droit international applicable aux cyberopérations⁴, le droit français de la cyberdéfense présente une zone grise dans l'application et les conséquences des cyberopérations de LID. Il revient alors au SGDSN ou au COMCYBER de bien évaluer les risques techniques et juridiques d'une réaction coordonnée avec les services de renseignement⁵ à une cyberattaque susceptible d'affecter la vie de la Nation⁶. Les moyens de renseignement jouent un rôle important dans la mise en œuvre de la LID pour obtenir les connaissances nécessaires sur l'attaque informatique et permettre une attribution afin de réagir de manière proportionnée. La même observation s'applique en ce qui concerne la LIO. En outre, on ne manquera pas de rappeler l'excuse pénale de l'article 323-8 du code pénal qui autorise les services spécialisés de renseignement à mener des

¹ « Ensemble coordonné d'actions défensives et offensives menées dans le cyberspace lors de la planification, de la préparation ou de la conduite d'opérations militaires » (vocabulaire de la défense, J.O. du 19/09/2017). Pour en savoir plus, voir la politique ministérielle de LID et la doctrine militaire de LIO du ministère des Armées (2019).

² A ce sujet, voir B. Lachaud et A. Valetta-Ardisson, *Rapport d'information sur la cyberdéfense*, Assemblée nationale, op. cit., p. 85 et 86.

³ En ce sens, voir Center for Cyber and Homeland Security, *Into the gray zone, the private sector and active defense against cyber threats*, The George Washington University, October 2016, p. 9 et suivantes.

⁴ Sur ce point, voir M. N. Schmitt, *Grey Zones in the International Law of Cyberspace* (October 18, 2017). 42:2 Yale Journal of International Law Online 1 (2017).

⁵ Arrêté du 17 juillet 2015 déterminant les services de l'Etat mentionnés au second alinéa de l'article L. 2321-2 du code de la défense.

⁶ Cf. SGDSN, *Revue stratégique de cyberdéfense*, op. cit., p. 47 et 48.

cyberopérations à l'étranger pour la protection des intérêts fondamentaux de la Nation¹ sans préciser si ces opérations s'inscrivent dans la LID ou la LIO. Là encore, les services de renseignement sont au cœur d'une zone grise dans l'articulation entre le droit de la cyberdéfense et le droit du renseignement.

Ces considérations s'inscrivent dans les remarques de la *Revue stratégique de cyberdéfense* de 2018 qui ne manque pas de souligner la nécessité de rapprocher les fonctions de la LID et de la LIO ainsi que les acteurs de la communauté de cyberdéfense pour plus d'efficacité². Par ailleurs, on profitera de notre analyse sur la zone grise de la LID pour rappeler que la France se montre hostile au « *Hack back sauvage* » exercé par le secteur privé sans pour autant être opposé à un « *Hack back sage* » sous la responsabilité de l'Etat et approuver cette position en raison des risques pour la paix et la sécurité du cyberspace³.

Au regard de ces assouplissements sur le modèle français de cyberdéfense, on ne peut que s'interroger sur une remise en cause de la séparation entre LID et LIO ou sur l'adoption d'un nouveau modèle proche de celui anglo-saxon qui centralise l'ensemble des capacités de lutte informatique sous la responsabilité des agences du renseignement numérique (NSA aux Etats-Unis et GCHQ au Royaume-Uni)⁴. Pour notre part, il semble effectivement plus naturel de confier les capacités cyber aux services de renseignement spécialisés dans le domaine du numérique en raison du fait que les cyberopérations se distinguent d'autres types d'opération par leur discrétion, furtivité et leur unicité (lorsqu'elle est détectée, une cyberattaque fait l'objet d'analyses pour être inefficace à l'avenir). Cependant, le modèle français peut être préservé car il ne souffre pas d'incohérences juridiques insurmontables et présente l'intérêt d'une clarification bienvenue des actions de l'Etat dans le cyberspace et ainsi contribuer à sa stabilité et à sa sécurité au niveau international.

¹ Cf. supra. §3 de la Section II du Chapitre I du Titre I de la Ière Partie.

² Cf. SGDSN, *Revue stratégique de cyberdéfense*, op. cit., p. 43 et suivantes.

³ En ce sens, voir K. Bannelier et T. Christakis, « *Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la Revue Stratégique de cyberdéfense de la France et le projet de loi ACDC aux Etats-Unis* », *Stratégique*, vol. 117, no. 4, 2017, pp. 99-118.

⁴ Voir sur ce point A. Desforges, *Séparation des fonctions offensive et défensive : l'originalité du modèle de cyberdéfense française remis en cause ?*, Chapitre 3, Conflits, crimes et régulations dans le cyberspace, op. cit., p. 65 à 87 ; J. Guiffard, « *Sur les rives du Potomac, le centre du système de renseignement et de cyberdéfense des Etats-Unis* », *Études françaises de renseignement et de cyber*, (N° 2), 1, 2024, pp.43-57.

Dans le prolongement de ces considérations, on soutiendra que les textes relatifs à la cyberdéfense adoptent une conception élargie du cyber-renseignement en autorisant d'autres acteurs publics et privés à mener des cyberopérations de renseignement.

B - La concurrence d'autres acteurs publics et privés dans le cyber-renseignement

La participation du renseignement à la cyberdéfense ne se limite pas aux services de renseignement, d'autres acteurs publics et privés mènent des actions de cyber-renseignement selon le cadre juridique de la cyberdéfense. Ces actions concernent principalement la LID, mais aussi la lutte informatique informationnelle ou d'influence (L2I) qui a été introduite en 2021 dans le modèle français de cyberdéfense. On observe alors un enchevêtrement des moyens sur le plan opérationnel qui aboutit à un « mille-feuille » du cyber-renseignement sur le plan organisationnel.

1. L'enchevêtrement des moyens de cyber-renseignement dans la lutte informatique défensive

L'anticipation, la détection et l'attribution des cybermenaces sont des missions primordiales du cyber-renseignement dans un contexte de lutte informatique toujours plus militarisée. Par conséquent, le législateur n'a cessé de renforcer les moyens de cyber-renseignement des administrations en charge de la cyberdéfense autres que les services de renseignement tout en permettant une participation directe d'acteurs privés dans l'anticipation et la détection des cyberattaques¹.

La loi de programmation militaire du 13 juillet 2018 qui complète le dispositif introduit en 2013 a étendu les pouvoirs de l'ANSSI en matière de détection des cyberattaques en l'autorisant à :

- mettre en œuvre sur le réseau des opérateurs du numérique des « marqueurs techniques » ou sondes de détection de cyberattaques menaçant des autorités publiques, des OIV ou des OSE le temps de caractériser la menace. Des agents individuellement désignés et

¹ En ce sens, voir J. -C. Videlin, *La loi de programmation militaire 2019-2025 : une loi financière et... juridique*, op. cit..

spécialement habilités sont autorisés à recueillir les données ainsi collectées et à exploiter les seules données techniques pertinentes¹ ;

- obtenir des opérateurs du numérique, pour les besoins de la cybersécurité des autorités publiques, OIV et OSE, « *l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou l'atteinte de leur système* » ainsi que, en cas d'alerte d'une cyberattaque, l'obtention des données techniques relatives à la menace².

De leur côté, les opérateurs du numérique se sont vus autorisés par l'article 34 de la loi de programmation militaire de 2018 créant l'article L. 33-14 du code des postes et des communications électroniques la possibilité de recourir également à des sondes de détection sur leur réseau de cyberattaques visant leurs abonnés, notamment grâce aux services d'entreprises privées de cybersécurité. De manière dérogatoire, ils sont également autorisés à conserver plus longtemps (six mois maximum) les données techniques permettant de caractériser un événement détecté par leurs sondes. Toutefois, le dispositif prévoit que ces sondes doivent intégrer les « marqueurs techniques » de l'ANSSI à sa demande lorsqu'elle a connaissance d'une cybermenace mais aussi une obligation d'information à l'Agence en cas de cybermenaces détectées ou aux abonnés pour les alerter en cas de vulnérabilité ou d'atteintes sur leurs systèmes numériques.

Les modalités de ce dispositif collaboratif de cyber-renseignement entre l'ANSSI et les opérateurs du numérique ont été précisées par le décret n° 2018-1136 du 13 décembre 2018 qui n'a pas manqué d'être attaqué devant le juge administratif. Par décision du 30 décembre 2021, le Conseil d'Etat a jugé le dispositif suffisamment clair et précis, justifié et proportionné tout en rappelant que la CNIL exerce son contrôle en matière de protection des données personnelles et que les mesures mises en œuvre par l'ANSSI et les opérateurs du numérique sont soumises au pouvoir de contrôle et de sanction de l'ARCEP³. Il est vrai que la loi de programmation militaire de 2018 a confié à l'ARCEP le contrôle

¹ Article L. 2321-2-1 du code de la défense.

² Article L. 2321-3 du code de la défense.

³ Conseil d'Etat, 30 décembre 2021, *La Quadrature du Net et autres*, n° 428028.

des conditions d'application des articles L. 2321-2-1 et L. 2321-3 du code de la défense¹. Ayant un accès complet et permanent aux données recueillies par l'ANSSI, l'autorité de régulation dispose d'un pouvoir de recommandation et d'injonction ainsi que de saisine du Conseil d'Etat en cas de contentieux². Désormais, les opérateurs du numérique coopèrent non seulement avec les services de renseignement mais aussi avec l'ANSSI en matière de détection des cybermenaces, ce qui pourrait causer des risques de doublon dans les opérations techniques portant sur les cybermenaces contre l'Etat, les OIV et les OSE.

Enfin, on n'oubliera pas de mentionner la possibilité pour des « *hackers* blancs » de chercher et de collecter des failles de sécurité informatique et de les transmettre à l'ANSSI sans être pénalement inquiétés pour que cette dernière puisse notamment « *procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace* »³. Là encore, de nouveaux acteurs entrent en concurrence avec les services de renseignement qui sont particulièrement intéressés par les vulnérabilités informatiques pour les besoins de la lutte informatique ou pour leurs besoins en matière de cyberespionnage.

2. Le cyber-renseignement de lutte informatique informationnelle

Considérée comme un véritable enjeu de sécurité nationale dès 2018⁴, la lutte informatique informationnelle (L2I) dans la couche sémantique du cyberespace fait déjà l'objet d'une réponse juridique spécifique avec la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information qui permet notamment, en période électorale, au ministère public de saisir le juge des référés pour demander de faire cesser la diffusion « *des allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir* » lorsqu'ils « *des allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir* »⁵. Dans le prolongement de ces considérations, le SGDSN s'est vu attribué de nouvelles

¹ Article L. 2321-5 du code de la défense.

² Article L. 36-14 du code des postes et des communications électroniques.

³ Article L. 2321-4 du code de la défense.

⁴ En ce sens, voir C. Cambon, *Rapport relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*, op. cit., p. 29.

⁵ Article L. 163-2 du code électoral.

compétences en matière de lutte contre les ingérences numériques étrangères par le décret n° 2021-922 du 13 juillet 2021 :

« il identifie les opérations impliquant, de manière directe ou indirecte, un Etat étranger ou une entité non étatique étrangère, et visant à la diffusion artificielle ou automatisée, massive et délibérée, par le biais d'un service de communication au public en ligne, d'allégations ou imputations de faits manifestement inexacts ou trompeuses de nature à porter atteinte aux intérêts fondamentaux de la Nation. Il anime et coordonne les travaux interministériels en matière de protection contre ces opérations »¹.

Pour remplir les missions de cette nouvelle attribution, le décret de 2021 créé un nouveau service technique et opérationnel du SGDSN à compétence nationale, le Service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM). De son côté, le ministère des Armées s'est également doté d'une compétence spécifique pour mener des cyberopérations en matière de L2I au sein du COMCYBER².

Les prérogatives de VIGINUM nous interrogent sur sa coordination avec les services de renseignement qui disposent, de longue date, de compétences en matière de lutte informationnelle et de désinformation³. Un risque de doublon est susceptible de concerner la collecte de données personnelles et de données de contenus en ligne sur les réseaux sociaux à des fins de L2I avec la création du traitement automatisé de données de VIGINUM dédié à l'identification des ingérences numériques étrangères. En effet, le décret n° 2021-1587 du 7 décembre 2021 autorise VIGINUM à mettre en œuvre sur les réseaux sociaux dépassant un seuil de cinq millions de visiteurs uniques par mois⁴ une collecte automatisée de données :

¹ Article 1 du décret n° 2021-922 du 13 juillet 2021.

² Cf. COMCYBER, *Eléments publics de doctrine militaire de lutte informatique d'influence (L2I)*, 2021.

³ Voir notamment O. Brun, « Désinformation », Hugues Moutouh éd., Dictionnaire du renseignement. op. cit., pp. 250-253.

⁴ Une liste exhaustive des réseaux sociaux a été publiée sur le site internet du SGDSN : Dailymotion, Facebook, Google Search, Instagram, Jeuxvideo.com, LinkedIn, Microsoft Bing, Pinterest, Snapchat, TikTok, Twitch, Twitter, Wikimedia, Yahoo Search, YouTube (<http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/le-service-de-vigilance-et-de-protection-contre-les-ingerences-numeriques-etrangees-viginum/>).

- d'identification de titulaires de comptes ouverts qui diffusent ou relaient des contenus publics ou y réagissent ;
- « *permettant de caractériser l'activité et l'audience de ces comptes, notamment les indicateurs quantitatifs relatifs au nombre d'abonnés et au nombre de publications* » ;
- de contenus publiquement accessibles pour les utilisateurs des plateformes en ligne « *au moyen de ces comptes et les indicateurs d'audience associés* ».

Cette collecte est effectuée à l'issue d'une veille réalisée par une équipe spécialisée dans le renseignement d'origine sources ouvertes chargée de faire respecter le principe de proportionnalité dans le traitement automatisé des données « par application de critères techniques ». On soulignera l'interdiction raisonnable de recourir à la reconnaissance faciale ou vocale. Sinon, les agents de VIGINUM peuvent recourir à un mécanisme de « cyber-patrouilles » avec la création de faux comptes en ligne qui, à la différence de celui autorisé pour les services de renseignement à article L. 863-1 du code de la sécurité intérieure¹, ne peuvent être utilisés que pour l'observation des contenus publiquement accessibles et leur collecte. Autrement dit, il est interdit d'entrer en contact avec des utilisateurs et de collecter d'autres données que celles relatives aux contenus publics intéressant les finalités de lutte contre la manipulation de l'information opérée par un acteur étranger. Pour le reste, le décret du 7 décembre 2021 fait application des principes du droit de la protection des données personnelles (limitations dans la durée de conservation des données et dans les accès par les agents, traçabilité des opérations, droit d'accès indirect et d'opposition). En revanche, si ce dispositif pourrait contribuer « *à l'assainissement des données diffusées sur internet* », il justifie bien « *un contrôle spécifique de son activité incarné par un « comité éthique et scientifique »* » chargé de vérifier la bonne interprétation des agents de VIGINUM lors de la collecte des données comme le remarque le Professeur Sébastien Hourson².

Ce dispositif aurait très bien pu être confié à la communauté nationale du renseignement ou plus particulièrement à la DGSE à l'instar du modèle américain

¹ Cf. supra. §2 de la Section II du Chapitre I du Titre I de la Ière Partie.

² Cf. S. Hourson, *La lutte administrative contre la menace informationnelle*, Droit Administratif n° 10, Octobre 2021, alerte 146.

de lutte contre le phénomène de « *weaponization of social media* » avec le rapprochement des spécialistes du renseignement d'origine sources ouvertes et des analystes de la Central Intelligence Agency (CIA)¹. Toutefois, la mise en place de VIGINUM peut sembler être une solution plus judicieuse. Les moyens limités du service ainsi que la transparence de son action constituent des meilleures garanties pour la sauvegarde de la liberté d'expression sur internet. De plus, cette solution devrait faciliter les relations indispensables que doit avoir le service avec les plateformes numériques dans la gestion des contenus problématiques.

3. Le « mille-feuille » du cyber-renseignement

L'accumulation de dispositifs et d'acteurs en charge de l'anticipation, de la détection, de la caractérisation et de l'attribution des cybermenaces ou encore de la collecte de données en matière de lutte informatique informationnelle a pour conséquence de bâtir un « mille-feuille » du cyber-renseignement à six couches :

- deux couches au niveau interministériel avec, d'une part, l'ANSSI et VIGINUM et, d'autre part, la communauté nationale du renseignement ;
- deux couches au niveau ministériel pour les actions propres à chacun des services de renseignement et pour les actions du COMCYBER ;
- deux couches au niveau du secteur privé avec l'intervention des opérateurs du numérique et d'entreprises de cybersécurité spécialisées dans des solutions de détection des cyberattaques et celle des « hackers blancs » dans la recherche de failles de sécurité informatique.

Cet empilement des acteurs du cyber-renseignement appellent trois remarques sur la surveillance de l'internet, la coordination et le contrôle du cyber-renseignement et la distinction entre la cyberdéfense et le renseignement.

Dès l'adoption des premières mesures juridiques de cyberdéfense dans la loi de programmation militaire de 2013, la question d'un renouvellement de la surveillance massive des individus a été soulevée². Toutefois, on notera que les mesures de cyber-renseignement, notamment renforcée depuis la loi de programmation militaire de 2018, concernent davantage la surveillance du

¹ A ce sujet, voir O. Chopin et B. Oudet, « Chapitre 6. Sources ouvertes, cyber, data : le renseignement et la révolution de l'information », Renseignement et sécurité, op. cit., pp. 169-194.

² En ce sens, voir E. A. Caprioli, *La loi de programmation militaire et sécurité de l'information*, Communication Commerce électronique n° 5, Mai 2014, comm. 50.

comportement des machines plus que celui des individus. Il reste qu'après la lutte contre le terrorisme, la cyberdéfense justifie un accroissement nouveau des moyens intrusifs de renseignement numérique et, par là même, un élargissement de la surveillance de l'internet et des internautes.

Cet élargissement de la surveillance tend à se confirmer avec l'augmentation des acteurs en charge du cyber-renseignement, ce qui nécessite de bien coordonner les actions de chacun. A ce titre, un rapprochement stratégique inéluctable doit s'opérer entre l'ANSSI, le CNRLT et les services de renseignement, VIGINUM et le COMCYBER. Aussi, le « mille-feuille » du cyber-renseignement peut être une source de divergence, et donc d'insécurité juridique, dans l'interprétation du droit applicable au cyber-renseignement en raison de la pluralité et de la différence des acteurs de contrôle. Comme évoqué par le Professeur Jean-Christophe Videlin, le contrôle du dispositif de l'ANSSI aurait notamment pu être confié à la CNCTR afin de « *créer une cohérence fonctionnelle* »¹. A notre sens, l'ARCEP, la CNCTR et la CNIL sont déjà en mesures de dialoguer sur les mesures de cyber-renseignement et de s'apporter assistance dans les contrôles. De son côté, le juge administratif devrait pouvoir assurer la cohérence et l'uniformité du droit en cas de contentieux. La régulation du renseignement de cyberdéfense est, selon nous, amenée à créer une communauté de contrôleur des actions numériques de l'Etat.

Il nous semble également que le choix du législateur français permet d'opérer une séparation claire entre l'activité de cyber-renseignement de l'ANSSI et les activités des services de renseignement qui sont certes enchevêtrées auprès des opérateurs du numérique mais différentes par nature. Citons la DPR qui souligne que « *si l'ANSSI est résolument tournée vers les victimes, les services sont susceptibles d'utiliser leurs capteurs pour détecter « plus au loin » ****** »². Cette affirmation peut être complétée en ajoutant que l'ANSSI intervient pour offrir des compétences de techniques informatiques en matière de cyber-renseignement au service de la protection des systèmes numériques de l'Etat, des OIV et des OSE

¹ Cf. J. -C. Videlin, *La loi de programmation militaire 2019-2025 : une loi financière et... juridique*, op. cit..

² Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 259.

alors que les services de renseignement offrent une analyse plus stratégique, tactique ou opérationnelle à destination du gouvernement, notamment pour l'attribution des cyberattaques qui relève d'une décision de nature politique en France¹.

Les actions des services de renseignement ne doivent donc pas être entièrement confondues avec les actions des autres acteurs du cyberrenseignement, même si des synergies et des convergences peuvent être observées dans le cadre juridique des cyberopérations en droit interne mais aussi en droit international et européen.

§2. L'impact de la dimension internationale de la cyberdéfense sur le renseignement

En raison de leur caractère transnational, les actions de cyberdéfense et notamment de LIO concernent la paix et la sécurité internationales. A ce titre, les cyberopérations conduites par des services de renseignement, notamment au sein du COMCYBER et la DGSE en France, n'échappent pas à l'ambition de la communauté internationale de faire appliquer le droit international aux cyberopérations des Etats. Cette ambition renouvelle l'intérêt du droit international pour l'espionnage face à l'importance et à la prolifération du cyberespionnage.

A - Le droit international applicable aux cyberopérations

Si dans le cadre de négociations au sein de l'Organisation des Nations Unies (ONU) les Etats reconnaissent l'applicabilité du droit international au cyberspace, il reste que les réponses juridiques se limitent à encadrer les cyberopérations commandées par des forces armées ou des services de renseignement dont les effets sont les plus offensifs.

1. La reconnaissance de l'applicabilité du droit international au cyberspace

Dès la fin des années 1990, les Nations Unies (ONU) se sont interrogées sur les conséquences de la numérisation des sociétés en matière de sécurité

¹ A ce sujet, voir B. Lachaud et A. Valetta-Ardisson, *Rapport d'information sur la cyberdéfense, Assemblée nationale*, op. cit., p. 26 et ANSSI, *Rapport d'activité pour l'année 2016*, p. 31.

internationale. Entre 2004 et 2017, cinq groupes d'experts gouvernementaux (GGE) ont été constitués pour examiner les cybermenaces contre la sécurité internationale et les réponses collectives et juridiques qui peuvent y être apportées. On retiendra particulièrement les GGE 2012/2013¹ et 2014/2015² dans lesquels les experts des Etats membres se sont accordés sur l'applicabilité du droit international au cyberspace, notamment la Charte des Nations Unies et les principes de souveraineté, de règlement pacifique des différends ou encore de non-intervention dans les affaires intérieures des Etats. En outre, le GGE 2014/2015 a proposé onze normes, règles et principes de comportement responsable des Etats facultatifs, non contraignants ayant pour objet de renforcer la coopération des Etats dans la gestion des incidents cyber et de limiter les cyberopérations en prohibant, par exemple les actes malveillants contre les infrastructures essentielles des Etats³.

Cependant, les experts du GGE 2016/2017⁴ ne sont pas parvenus à un consensus sur l'interprétation du droit international applicable au cyberspace, que ce soit sur la souveraineté numérique ou sur les réponses juridiques aux cyberopérations (attribution, droit des conflits armés, contre-mesures et légitime défense par exemple). Pour autant, les Etats n'ont pas abandonné les négociations avec l'« Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberspace » porté par des Etats et des acteurs privés et la création à l'ONU d'un nouveau GGE⁵ et d'un groupe de travail à composition non limitée (Open-Ended Working Group ou « OEWG »)⁶ pour la période 2019-2021. Ces deux groupes ont réaffirmé les termes de la résolution A/RES/70/237 de 2015 sur les normes de comportement responsable et l'applicabilité du droit international au cyberspace sans néanmoins réellement définir précisément les modalités de son application,

¹ Cf. Rapport A/68/98* du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale.

² Cf. Rapport A/70/174 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale et la résolution A/RES/70/237 de l'Assemblée générale du 23 décembre 2015.

³ Sur les onze normes, règles et principes de comportement responsable des Etats, voir le rapport A/70/174 du 22 juillet 2015, p. 8 à 10.

⁴ Cf. Rapport A/72/327 du Groupe d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

⁵ Cf. Résolution A/RES/73/266 de l'Assemblée générale du 22 décembre 2018.

⁶ Cf. Résolution A/RES/73/27 de l'Assemblée générale du 5 décembre 2018.

même si le nouveau GGE a tenu à apporter « un nouveau niveau d'interprétation » en évoquant l'application pleine et entière de la Charte des Nations Unies, celle du droit des conflits armés et du droit international humanitaire (DIH) ainsi que le principe de « *due diligence* » dans l'utilisation du territoire des Etats pour commettre des cyberattaques internationalement illicites¹. A l'issue de ces travaux concurrents, un nouveau cycle de négociations a été ouvert pour la période 2021-2025 au sein d'un OEWG². Dans la continuité de ces négociations, il a été décidé en 2022 et 2023 de mettre en place un programme d'action permanent sous l'égide de l'ONU pour renforcer les efforts de coopération internationale en cybersécurité³. Par ailleurs, on notera qu'un projet de Convention des Nations Unies contre la cybercriminalité a été adopté durant l'été 2024 par la Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles⁴.

Dans un contexte de fragmentation de l'internet mondial et d'affirmation des souverainetés numériques où des Etats comme la Russie et la Chine ont des conceptions différentes des Etats occidentaux sur la cybersécurité⁵, il convient de rappeler que les divergences d'interprétation sur l'encadrement du cyberspace s'inscrivent dans les stratégies géopolitiques des Etats qui instrumentalisent le droit international⁶. Cependant, il n'en demeure pas moins que l'applicabilité du droit international au cyberspace semble faire l'unanimité de la communauté internationale et qu'un certain nombre d'Etats, dont la France, ont publié leur stratégie nationale de cyberdéfense et leur interprétation du droit international

¹ Cf. Résolution A/76/135 du 14 juillet 2021, p. 20 et 21.

² Cf. Résolution A/RES/75/240 de l'Assemblée générale du 31 décembre 2020.

³ Cf. Résolutions A/77/36, A/77/37, A/77/512 de 2022 et A/RES/78/237, A/RES/78/16, A/78/541 de 2023.

⁴ Cf. Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, *Projet de texte actualisé de la convention*, New York, 29 juillet-9 août 2024, A/AC.291/22/Rev.3.

⁵ En ce sens, voir S. -Y. Laurent, *Les Etats-Unis, les Etats et les faux semblants de la fin de l'internet mondial*, Chapitre 1, Conflits, crimes et régulations dans le cyberspace, op. cit., 2021, p. 5 à 43.

⁶ En ce sens, voir F. Delerue, F. Douzet et A. Géry, *Les représentations géopolitiques du droit international dans les négociations internationales sur la sécurité et la stabilité du cyberspace*, Étude n° 75, IRSEM/EU Cyber Direct, novembre 2020.

applicable aux cyberopérations pour plus de transparence¹, ce qui n'est pas sans conséquences pour les forces armées et les services de renseignement dans la conduite de leurs cyberopérations. En effet, ces derniers sont contraints d'envisager les réponses juridiques des Etats à leurs actions, notamment lorsqu'elles produisent de graves effets offensifs.

2. Des réponses juridiques limitées aux cyberopérations les plus offensives

Si les forces armées et les services de renseignement compétents en matière de cyberopérations doivent tenir compte des positions nationales des autres Etats sur les modalités d'application du droit international applicable au cyberspace² ou des doctrines non étatiques comme le Manuel de Tallinn 2.0 sur le droit international applicable aux cyberopérations³, leur cadre d'intervention s'inscrit, avant tout, dans la position défendue par leur pays et donc dans celle de la France en ce qui concerne le COMCYBER et la DGSE.

Selon la position française, les réponses du droit international aux cyberopérations étatiques doivent être distinguées selon qu'elles sont conduites en temps de paix ou dans un contexte de conflit armé⁴. Dans le premier cas, la France considère qu'une cyberopération ne constitue pas un fait internationalement illicite, sauf à ce que ses effets entraînent une violation du droit international. S'appuyant sur un « schéma de classement des attaques informatiques » en fonction de leur gravité sur les intérêts fondamentaux de la Nation, la souveraineté et la démocratie, la sécurité intérieure et civile, la population et l'environnement ou l'économie française⁵, l'Etat français distingue

¹ L'interprétation de la France a été clarifiée en 2018 dans la *Revue stratégique de cyberdéfense* et en 2019 dans le rapport du ministère des Armées sur le *Droit international appliqué aux opérations dans le cyberspace*.

² Pour en savoir plus sur les interprétations des Etats sur le droit international applicable au cyberspace, voir les positions nationales publiées sur la page dédiée du site internet « cyberlaw » du Centre d'excellence de cyberdéfense coopérative de l'OTAN ; https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

³ Cf. M. N. Schmitt, *Manuel de Tallinn 2.0 sur le droit international applicable aux cyberopérations*, Cambridge University Press, 2017.

⁴ Cf. Rapport du ministère des Armées sur le *Droit international appliqué aux opérations dans le cyberspace*, 9 septembre 2019.

⁵ Cf. SGDSN, *Revue stratégique de cyberdéfense*, op. cit., p. 79 à 84.

deux niveaux de qualification d'une cyberopération constituant un fait internationalement illicite :

- un premier niveau de violation du droit international qui concerne les principes de souveraineté et de non-intervention et l'interdiction du recours à la force au sens de l'article 2 alinéa 4 de la Charte des Nations Unies. En fonction de la gravité de la cyberattaque, la France se réserve le droit de recourir à des opérations de LID, d'adopter des contre-mesures ou encore de saisir le Conseil de sécurité des Nations Unies (CSNU) ou d'invoquer l'état de détresse ou l'état de nécessité ;
- un deuxième niveau qui qualifie une cyberattaque d'agression armée au sens de l'article 51 de la Charte des Nations Unies et qui ouvre le droit de faire usage de la légitime défense. Cette qualification peut être retenue lorsque les effets et l'ampleur d'une ou plusieurs cyberattaques atteignent une certaine gravité et sont comparables à ceux d'un emploi de la force physique conformément à la jurisprudence *Activités militaires et paramilitaires au Nicaragua et contre celui-ci* de la Cour internationale de justice (CIJ)¹.

Dans le second cas qui concerne une situation de conflit armé, on retiendra principalement que la France considère que des cyberopérations militaires peuvent caractériser l'existence d'un tel conflit et que le DIH trouve à s'appliquer dans la conduite des hostilités cyber (principe de distinction et principes de proportionnalité et de précaution). En outre, une cyberopération militaire peut constituer une attaque au sens de l'article 49 du Protocole additionnel I aux Conventions de Genève du 13 août 1949 lorsque « *les équipements ou les systèmes visés ne rendent plus le service pour lesquels ils ont été mis en place, ceci y compris de manière temporaire et réversible, dès lors qu'une intervention de l'adversaire est nécessaire pour rendre l'infrastructure ou le système de nouveau opérant* »².

A ces réponses juridiques française, il convient d'ajouter que des réponses collectives à une cyberattaque majeure relevant d'une agression armée pourraient

¹ CIJ, 27 juin 1986, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci* (Nicaragua c. Etats-Unis d'Amérique), paragraphes 227 à 238.

² Cf. Rapport du ministère des Armées sur le *Droit international appliqué aux opérations dans le cyberspace*, p.13.

être envisagées par l'OTAN et l'Union européenne dans le cadre des clauses d'assistance mutuelle de l'article 5 du traité de l'Atlantique Nord et de l'article 42-7 du traité sur l'Union européenne, même si ces réponses collectives demeurent incertaines en raison des divergences d'interprétation des Etats¹. En outre, l'Union européenne a pris l'initiative de promouvoir le droit international en réponse aux cybermenaces extérieures contre les intérêts de l'Union ou de ses Etats membres en se dotant de la capacité d'adopter des mesures restrictives contre les cyberattaques² dans le cadre de la *Cyber Diplomacy Toolbox*³. Il s'agit de sanctions économiques à l'encontre de personnes physiques ou morales, d'entités ou organismes qui sont impliqués dans des cyberattaques ou tentatives de cyberattaques extérieures à l'Union européenne « ayant des effets potentiels importants », c'est-à-dire par l'ampleur et la gravité des dommages causés sur les activités publiques, sociales et économiques essentielles de l'Union européenne et des Etats membres⁴.

Si les constats partagés en 2018 sur l'absence d'un véritable recours au droit international pour réguler les cyberopérations sont encore d'actualité⁵, on peut néanmoins considérer que les organisations de cyberdéfense étatiques doivent être désormais préparées à se voir appliquer des réponses fondées sur le droit international dans la conduite de leurs cyberopérations les plus offensives. Autrement dit, les actes cybercriminels ou d'espionnage ne devrait donc pas être concernés. Dans le cas de la France, il est vrai qu'aucune analyse ni de développements spécifiques au cyberespionnage n'ont été formulées dans le rapport du ministère des Armées sur le *Droit international appliqué aux opérations dans le cyberspace*. Ces considérations pourraient laisser entendre que seul le

¹ Sur l'OTAN et l'UE, voir notamment B. Lachaud et A. Valetta-Ardisson, *Rapport d'information sur la cyberdéfense*, op. cit., p. 28 à 31 et G. Lasconjarias, « *L'Otan et le domaine opérationnel cyber* », Stéphane Taillat éd., *La Cyberdéfense. Politique de l'espace numérique*, op. cit., pp. 150-156.

² Règlement UE n° 2019/796 du Conseil, 17 mai 2019.

³ En ce sens, voir A. Géry et E. Noël, *La recherche de son autonomie stratégique numérique par l'Union européenne*, *Revue de l'Union européenne*, 2023, p. 152.

⁴ A ce sujet, voir L. -M. Chauvel et A. Hamonic, *Chronique Action extérieure de l'UE - La diversification des régimes thématiques de mesures restrictives*, RTD Eur., 2019, p.746 et B. Bertrand, *Chronique Droit européen du numérique - La nouvelle approche de la cybersécurité européenne*, RTD Eur., 2021, p. 155.

⁵ En ce sens, voir notamment L. Gautier, « *Cyber : les enjeux pour la défense et la sécurité des Français* », *Politique étrangère*, vol., no. 2, 2018, pp. 29-42 et F. Delerue et A. Gery, « *Chapitre 3. Les aspects juridique et stratégique de la cyberdéfense. Le droit international et la cyberdéfense* », Stéphane Taillat éd., *La Cyberdéfense. Politique de l'espace numérique*, op. cit., pp. 61-70.

COMCYBER et les forces armées étrangères seraient soumis à l'interprétation française du droit international applicable au cyberspace, les cyberopérations de la DGSE et des services de renseignement ne pourraient donc pas être concernées puisqu'elles relèveraient de l'espionnage. Cette dernière analyse, qui distinguerait les cyberopérations du cyberespionnage dans l'application du droit international, nous semble néanmoins trop radicale compte tenu de l'importance, de l'ampleur et de la diversité des activités des services de renseignement dans le cyberspace et dans les organisations étatiques de cyberdéfense. En reconnaissant l'applicabilité du droit international au cyberspace et aux cyberopérations des Etats, la communauté internationale a alors renouvelé l'intérêt que peut avoir le droit international pour réguler l'espionnage.

B - L'intérêt renouvelé du droit international pour l'espionnage

De façon traditionnelle pour la communauté internationale, la position française ne fait qu'éviter la question de la régulation de l'espionnage. Pourtant, cette stratégie d'évitement des Etats est à bout de souffle face aux particularités de la cyberdéfense et du cyberespionnage. D'autant plus qu'il semblerait que ce dernier contribue à la formation d'un « droit international du renseignement ».

1. Une stratégie d'évitement des Etats à bout de souffle

Entendu dans le droit des conflits armés comme le recueil ou la recherche d'informations, de manière clandestine ou sous de faux prétextes, dans la zone d'opérations d'une partie belligérante pour les communiquer à la partie adverse¹, l'espionnage ne fait pas l'objet d'une convention ou d'une coutume internationale particulières applicables en temps de paix. Dans ces conditions, l'acte d'espionnage constitue un acte inamical mais qui n'est pas un fait internationalement illicite ni un droit reconnu aux Etats, même si la doctrine considère l'espionnage comme licite soit parce qu'il ne constitue pas une violation du droit international par lui-même (courant majoritaire) soit du fait de sa propre finalité (courant minoritaire)². Quoi qu'il en soit, les Etats semblent réticents à

¹ Article 29 du règlement de La Haye concernant les lois et coutumes de la guerre du 18 octobre 1907.

² Sur la licéité de l'espionnage en droit international, voir notamment F. Lafouasse, *L'espionnage dans le droit international*, Editions Nouveau Monde, 2012 ; J. -C. Cousseran et P. Hayez, *Renseigner les démocraties, renseigner en démocratie*, Odile Jacob, 2015, p. 215-230 et 285-316 ; H. Moutouh, *Dictionnaire du renseignement*, op. cit., p. 302-304 et 348-359.

clarifier leur position sur l'application du droit international à l'espionnage en adoptant une stratégie d'évitement, y compris en ce qui concerne le cyberespionnage comme en témoigne la position française du ministère des Armées sur les cyberopérations publiée en 2019¹. On relèvera cependant que cette dernière a précisé que :

« La majeure partie des cyberopérations, en particulier celles de LIO menées par la France en contexte de conflit armé, se situe en deçà du seuil de l'attaque, puisqu'il s'agit principalement de collecte d'informations et de brouillage des capacités d'influence adverse. Ces opérations restent, néanmoins, soumises aux principes généraux du DIH »².

Le constat que la majorité des cyberopérations militaires relèvent des activités de renseignement et d'espionnage est également transposable dans les cyberopérations en temps de paix, notamment du fait que les services de renseignement sont les principaux acteurs de la cyberdéfense dans la plupart des pays. A ce titre, il ne peut être écarté que les cyberopérations des services de renseignement puissent outrepasser le cyberespionnage dans leurs intentions et dans leurs effets et ainsi se voir appliquer les positions nationales relatives au droit international applicable au cyberspace, sauf à considérer que toutes les missions des services de renseignement relèvent de l'espionnage et que celui-ci est licite par sa finalité. Autrement dit, les cyberopérations des services de renseignement ne relèveraient pas nécessairement du cyberespionnage ou alors le cyberespionnage ne concernerait pas uniquement la collecte clandestine d'informations mais aussi des opérations de lutte informatique. On remarquera que le code pénal français qualifie le sabotage d'infraction contre les intérêts fondamentaux de la Nation dans un chapitre dédié à l'espionnage³, que l'article L. 811-2 du code de la sécurité intérieure dispose que les services de renseignement contribuent à l'entrave des risques et menaces et que la DGSE a notamment pour

¹ En ce sens, voir I. Navarrete, *L'espionnage en temps de paix en droit international public*, Canadian Yearbook of International Law/Annuaire Canadien De Droit International, 53, 1-65, 2016 ; F. Delerue, F. Douzet et A. Géry, *Les représentations géopolitiques du droit international dans les négociations internationales sur la sécurité et la stabilité du cyberspace*, op. cit. ; T. Moulin, *Le cyber espionnage en droit international*, Editions Pedone, septembre 2021.

² Rapport du ministère des Armées sur le Droit international appliqué aux opérations dans le cyberspace, 2019, p. 14.

³ Articles 411-1 à 411-11 du code pénal.

mission « *de détecter et d'entraver, hors du territoire national, les activités d'espionnage dirigées contre les intérêts français afin d'en prévenir les conséquences* »¹. Par conséquent, il peut être soutenu que les positions nationales des Etats, dont celle de la France, sur le droit international applicable au cyberspace peuvent constituer des réponses juridiques à des cyberopérations conduites par des services de renseignement lorsqu'elles produisent des effets offensifs de cyberdéfense voulus ou non. La DGSE devrait alors tenir compte de la position défendue par la France et celle des autres Etats dans ses cyberopérations d'entrave en collaboration avec le COMCYBER. Par ailleurs, on relèvera que l'Union européenne a adopté des mesures restrictives contre le Central principal des technologies spéciales de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU) pour sa responsabilité dans les cyberattaques de sabotage NotPetya de 2017 et contre un réseau électrique ukrainien dans l'hiver 2015-2016². Le droit de la cyberdéfense bouleverse la conception de l'espionnage en droit international et remet en cause la stratégie d'évitement des Etats.

Mais aussi, les intrusions informatiques aux seules fins d'espionnage étatique dans les systèmes numériques situés sur le territoire d'un autre Etat ou relevant de sa souveraineté concernent bien la paix et la sécurité internationales au regard de leurs risques systémiques pour le cyberspace et devraient donc faire l'objet des négociations internationales³. Soulignons d'ailleurs que les Etats-Unis ont publié leur interprétation du droit international applicable au cyberespionnage en temps de paix qui reconnaît que ce type de cyberopérations clandestines pourrait violer le droit international sans avoir à atteindre le seuil du recours à la force ou d'atteinte au principe de non-intervention en précisant toutefois que ces opérations peuvent se justifier par la conception transnationale de l'Internet et qu'elles ne peuvent pas faire l'objet d'une interdiction absolue⁴. On

¹ Article D. 3126-2 du code de la défense.

² Décision (PESC) 2020/1127 du Conseil du 30 juillet 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres.

³ En ce sens, voir F. Delerue, F. Douzet et A. Géry, *Les représentations géopolitiques du droit international dans les négociations internationales sur la sécurité et la stabilité du cyberspace*, op. cit..

⁴ « *In certain circumstances, one State's non-consensual cyber operation in another State's territory, even if it falls below the threshold of a use of force or non-intervention, could also violate international*

ajoutera que certains actes de cyberespionnage ont pu être dénoncés entre Etats et faire l'objet de réponses plus ou moins juridiques qui remettent également en cause la stratégie d'évitement :

- en 2013, le Timor-Leste a saisi la Cour internationale de justice d'une affaire contre l'Australie soutenant que les services de renseignement australiens avaient capté des documents, des données et une correspondance entre le Timor-Leste et ses conseillers juridiques dans le cadre d'un Arbitrage entre les deux pays sur la mer de Timor en violation des droits de propriété de l'Etat découlant du droit international coutumier et du principe de souveraineté¹. L'affaire n'a finalement pas été jugée, les deux pays ayant réglé à l'amiable leur différend avec la restitution des éléments captés par l'Australie² ;
- en 2015, les Etats-Unis et la Chine ont conclu un accord bilatéral sur la prohibition du cyberespionnage à des fins commerciales et industrielles³, même si la Chine continue d'être régulièrement accusée d'espionnage économique⁴ ;
- les mesures restrictives prises par l'Union européenne en 2020⁵ ont visé des agents du service de renseignement militaire de la Fédération de Russie (GU/GRU) pour leur implication dans la cyberattaque d'espionnage dirigée

law. However, a State's remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law. In other words, there is no absolute prohibition on such operations as a matter of international law. This is perhaps most clear where such activities in another State's territory have no effects or de minimise effects. The very design of the Internet may lead to some encroachment on other sovereign jurisdictions » (Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, 140).

¹ Cf. CIJ, *requête introductive d'instance sur les questions concernant la saisie et la détention de certains documents et données*, Timor-Leste c. Australie, 17 décembre 2013.

² Sur cette affaire, voir la page dédiée du site internet de la CIJ : [Questions concernant la saisie et la détention de certains documents et données \(Timor-Leste c. Australie\) \(icj-cij.org\)](https://www.icj-cij.org/fr/affaire/156) (<https://www.icj-cij.org/fr/affaire/156>).

³ Cf. Joint Statement by Attorney General Loretta E. Lynch and Secretary of Homeland Security Jeh Johnson, Friday, September 25, 2015.

⁴ En ce sens, voir S. de Faletans, S. Renard et C. Moineau, *USA-Chine : accusations d'espionnage économique sur le sol américain*, Portail de l'IE, 3 novembre 2022 ou encore l'article TV5MONDE, *L'espionnage industriel, une arme privilégiée par la Chine ?*, 5 février 2023.

⁵ Cf. Décision (PESC) 2020/1127 du Conseil du 30 juillet 2020.

contre l'Organisation pour l'interdiction des armes chimiques (OIAC) en 2018¹.

Par ailleurs, le droit international des droits de l'homme et, plus particulièrement, le droit au respect de la vie privée et la protection des données personnelles garantis par les instruments juridiques du Conseil de l'Europe et la jurisprudence de la CEDH² ainsi que, dans une moindre mesure, par le Pacte international relatif aux droits civils et politiques (PIDCP) sont désormais à prendre en considération dans la légalité des mesures de cyberespionnage contre les individus³.

Avec la prolifération du cyberespionnage et une stratégie d'évitement normatif à bout de souffle, la question de la formation d'un « droit international du renseignement », pour reprendre les termes de Fabien Lafouasse, semble réellement se poser⁴.

2. La formation d'un « droit international du renseignement »

De nombreuses études doctrinales mettent en lumière des possibles limites juridiques en droit international aux actes d'espionnage étatiques et, plus particulièrement, lorsque ces actes sont commis à travers le cyberspace⁵. Une synthèse des discussions doctrinales sur les cas d'application du droit international et les actes pouvant constituer un fait internationalement illicite peut être faite à partir de distinctions entre différents cas d'espionnage.

Ainsi, le droit des conflits armés et le DIH s'intéressent à « l'espionnage militaire », la doctrine considérant notamment que les interdictions d'acte de

¹ A ce sujet, voir B. Bertrand, *La souveraineté numérique européenne : une « pensée en acte » ?*, op. cit..

² Voir Section I du Chapitre I du Titre I de la Seconde Partie.

³ Sur ce point, voir F. Lafouasse, *Le droit du renseignement : un droit conforme aux traités internationaux*, Le droit du renseignement, op. cit., p. 187 à 199.

⁴ Cf. F. Lafouasse, *L'enjeu des données personnelles et souveraines à l'aune d'un « droit international du renseignement » en formation*, Chapitre 7, Conflits, crimes et régulations dans le cyberspace, op. cit., p. 145 à 165.

⁵ Sur les études doctrinales, voir par exemple I. Navarrete, *L'espionnage en temps de paix en droit international public*, op. cit. ; M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., 2017 ; F. Lafouasse, *Droit international du renseignement*, JurisClasseur Communication, Fascicule 1200, 2018 ; F. Delerue, F. *Internationally Wrongful Cyber Acts : Cyber Operations Breaching Norms of International Law*, In *Cyber Operations and International Law*, Cambridge University Press, 2020 ; R. Buchan, *Cyber Espionage and International Law*, Bloomsbury Publishing, 25 février 2021.

perfidie et de causer des dommages contre les civils sont à prendre en considération. En temps de paix, les débats des experts portent généralement sur « l'espionnage politique » et ses risques de violation des principes de souveraineté, de non-ingérence dans les affaires des Etats, de règlement pacifique des différends et d'interdiction du recours à la force au regard du droit international public général.

Plus spécialement, « l'espionnage diplomatique » pourrait se voir appliquer la Convention de Vienne de 1961 sur les relations diplomatiques pour prohiber l'interception des archives et documents, y compris les données numériques et les communications électroniques, des missions diplomatiques et consulaires qui font l'objet d'un principe d'inviolabilité (article 24). En outre, le recours à des opérations d'espionnage sous couverture diplomatique peut entrer en contradiction avec l'article 41 de la Convention de Vienne sur l'utilisation des fonctions diplomatiques et entraîner une déclaration *persona non grata* en application de l'article 9 de la Convention. Des discussions doctrinales spécifiques ont pu également porter sur « l'espionnage économique » et sur la prohibition du vol de propriété intellectuelle et des secrets d'affaires avec pour possible fondement les droits de la concurrence et de propriété stipulés dans les accords de l'Organisation mondiale du commerce (OMC).

Enfin, on mentionnera le cas de « l'espionnage de lutte contre le terrorisme et la criminalité internationales » qui constitue une part importante des missions contemporaines des services de renseignement et qui s'opère beaucoup dans le cyberspace. En droit international, ce cas d'espionnage est principalement discuté en droit international des droits de l'homme puisqu'il cible essentiellement les individus.

Cependant, on rappellera que les experts s'accordent à conclure que l'espionnage et son volet cyber ne font pas l'objet d'une prohibition absolue et que leur définition en temps de paix n'est pas véritablement établie. En revanche, il est de plus en plus admis que la communauté internationale devrait désormais être en mesure de former conventionnellement ou par la coutume internationale un « droit international du renseignement » avec des règles adaptées aux spécificités du cyberespionnage en tenant compte des nombreuses discussions doctrinales et

de la pratique des relations internationales¹. Ces considérations encouragent les Etats à sortir de leur stratégie d'évitement et à défendre des positions nationales. A cet égard, il nous semble qu'il serait réellement pertinent de clarifier la question du cyberespionnage dans les négociations internationales relatives au droit international applicable au cyberspace, d'autant plus que les Etats-Unis ont ouvert la voie en publiant leur interprétation. Il se pourrait alors qu'un « droit international du cyber-renseignement » fondé sur le croisement des positions nationales en matière de cyberdéfense et de cyberespionnage se formalise en premier lieu. Ce droit apporterait alors une « nouvelle vision régulatoire » des activités numériques pour compléter « l'état régulatoire » du numérique sur le plan international². Plus encore, il participerait à une meilleure appréhension des cyberattaques par le droit international dont l'application des règles existantes demeurent incertaines dans ce domaine³. Enfin, la dimension internationale de la cyberdéfense et sa difficile régulation sont propices à renouveler « les Etats secrets » et à « développer leur aspiration à la clandestinité », notamment à travers l'action des services de renseignement comme le souligne le Professeur Laurent⁴. Cependant, la formation d'un « droit international du cyber-renseignement » nous invite tout de même à penser qu'un processus de légalisation des activités d'espionnage sur le plan national comme international est une problématique partagée des Etats au sein de la communauté internationale dans leur volonté d'encadrer la militarisation du cyberspace et de légitimer leurs cyberopérations.

Cette problématique partagée ne s'arrête pas au contrôle de l'usage des capacités de cyberdéfense et de cyber-renseignement. Elle se traduit aussi dans la nécessité de contrôler la prolifération des outils numériques malveillants à travers le monde. A ce titre, les instruments juridiques de contre-prolifération sont amenés à jouer un rôle dans l'encadrement de la numérisation du renseignement

¹ Voir en ce sens F. Lafouasse, *L'enjeu des données personnelles et souveraines à l'aune d'un « droit international du renseignement » en formation*, Chapitre 7, Conflits, crimes et régulations dans le cyberspace, op. cit..

² Sur les « visions réglementaires » du numérique, voir C. Castets-Renard, V. Ndior et L. Rass-Masson, *Enjeux Internationaux Des Activités Numériques*, Bruxelles, Larcier, 2020.

³ Sur ce point voir notamment M. Grange et A. -T. Norodom, *Cyberattaque et droit international. Problèmes choisis*, Paris, Pedone, 2019.

⁴ Cf. S.- Y. Laurent, *Etat secret, Etat clandestin : essai sur la transparence démocratique*, Editions Gallimard, 2024, p. 242 à 255.

avec le contrôle du commerce des biens et technologies de surveillance numérique.

SECTION II : La lutte contre la prolifération des outils numériques malveillants

Seconde réponse à la militarisation du cyberspace, les instruments juridiques de contre-prolifération des biens et technologies sensibles pour la paix et la sécurité internationales se sont adaptés aux outils numériques malveillants dont l'acquisition intéresse les Etats et leurs services de renseignement, notamment en affirmant un contrôle de la commercialisation de ces outils au niveau international (§1). Une attention particulière doit être portée au niveau de l'Union européenne qui a consacré un régime spécifique à la contre-prolifération des biens de cybersurveillance en se fondant sur le concept de « sécurité humaine » (§2).

§1. Le contrôle du commerce des outils numériques malveillants susceptibles d'intéresser le renseignement

Permettant de lutter contre la prolifération des outils numériques malveillants, y compris dans le domaine du renseignement, on invoquera, d'une part, la Convention de Budapest sur la cybercriminalité et, d'autre part, l'Arrangement de Wassenaar sur le régime de contrôle des exportations de biens et technologies civils et militaires sensibles. Ces deux instruments internationaux très différents ont des stipulations qui visent à contrôler le commerce d'outils numériques malveillants susceptibles d'intéresser les services de renseignement dans leur effort de numérisation.

A - La répression du trafic illicite d'outils numériques malveillants dans la Convention de Budapest

L'article 6 de la Convention de Budapest du 23 novembre 2001 enjoint les Etats signataires à pénaliser le trafic illicite d'outils numériques malveillants dans leur droit interne. Si cette solution a été introduite en France dans le code pénal dès 2004, elle n'est en revanche plus applicable au renseignement numérique extérieur depuis la loi relative au renseignement de 2015, ce qui pose question sur

l'intérêt de cette exclusion pénale et sur sa conformité à la Convention de Budapest. Pour la bonne compréhension de notre analyse, nous exposerons les stipulations de contre-prolifération de l'article 6 de la Convention avant de discuter de l'exclusion l'infraction de trafic illicite d'outils numériques malveillants pour le renseignement extérieur.

1. Les stipulations de contre-prolifération de l'article 6

Les faits incriminés par l'article 6 de la Convention qui concernent la contre-prolifération des outils numériques malveillants sont :

« la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition : i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 [de la Convention] ; ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 »¹.

Précisons que les dispositifs, programmes informatiques et données visées par l'article 6 doivent être en lien matériellement et intentionnellement avec la commission d'actes de piratages informatiques incriminés aux articles 2 à 5 de la Convention, c'est-à-dire l'accès illégal à un système numérique et l'interception illégale de données ainsi que les atteintes à l'intégrité des données ou d'un système numérique.

Il est à noter que le paragraphe 3 de l'article 6 réserve le droit aux Etats signataires de ne pas appliquer les stipulations de contre-prolifération du premier paragraphe, ce qui peut fortement atténuer le dispositif déjà limité par le nombre d'Etats signataires appliquant la Convention et l'existence d'un marché noir sur le *dark web* comme le rappelle Aude Géry, spécialiste de la lutte contre la prolifération des cyberarmes². Cependant, on peut comprendre qu'une telle réserve soit nécessaire pour les besoins des forces de sécurité. En revanche, la réserve stipulée

¹ Paragraphe 1 de l'article 6 de la Convention de Budapest de 2001.

² Cf. A. Géry, « *Droit international et prolifération des cyberarmes* », Politique étrangère, vol. , no. 2, 2018, pp. 43-54.

au paragraphe 3 de l'article 6 ne peut pas porter sur le trafic des données mentionnées au ii du a du paragraphe 1, ce qui nous semble cohérent car il s'agit de faire circuler des données confidentielles qui remettent directement en cause la sécurité de systèmes numériques. Pourtant, le législateur français a fait le choix de ne pas tenir compte de l'ensemble de ces stipulations en ce qui concerne les mesures numériques de renseignement extérieur.

2. L'exclusion de l'infraction de trafic illicite d'outils numériques malveillants pour le renseignement extérieur

Alors que la loi du 21 juin 2004 pour la confiance dans l'économie numérique avait inséré l'incrimination de trafic illicite prévue par la Convention de Budapest dans l'article 323-3-1 du code pénal français, la loi du 24 juillet 2015 relative au renseignement a toutefois exclu l'application de ces dispositions en vertu de l'article 323-8 du même code pour les actions menées par le renseignement extérieur.

D'un point de vue purement juridique, cette exclusion peut apparaître contradictoire avec les stipulations de l'article 6 de la Convention de Budapest. En effet, elle ne respecte pas la clause de réserve stipulée au paragraphe 3, ce qui a pour conséquence de permettre aux agents du renseignement extérieur d'acquérir mais aussi de faire circuler des outils numériques malveillants et des données confidentielles d'accès à des systèmes numériques. En optant pour une excuse pénale visant directement des dispositions ayant pour socle conventionnel la Convention de Budapest, le législateur français a, selon nous, violé les stipulations sur la réserve de l'article 6 dans sa volonté de conférer des moyens d'actions numériques au renseignement extérieur. Pour plus de cohérence juridique sur le plan pénal, il aurait été donc normale que l'excuse pénale de l'article 323-8 ne concerne pas le fait d'offrir, de céder ou de mettre à disposition un mot de passe, un code d'accès ou toute donnée permettant d'accéder à tout ou partie d'un système numérique.

En revanche, du point de vue du renseignement, il peut être soutenu que l'extension de l'excuse pénale au trafic de données permettant l'accès à des systèmes numériques peut présenter une utilité pour l'espionnage et des actions clandestines. A l'instar des cyber-patrouilles qui sont autorisées à partager des

contenus à caractère terroriste¹, les agents du renseignement extérieur pourraient être en mesure de partager des données permettant l'accès à des systèmes numériques pour l'accomplissement de leurs missions. Malgré la généralité des termes de l'article 323-8 du code pénal, ce dispositif ne devrait pas permettre aux agents du renseignement extérieur d'entreprendre de mettre en place un trafic illicite d'outils numériques malveillants à des fins qui ne correspondent pas à la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code de la sécurité intérieure.

B - L'introduction des logiciels intrusifs malveillants dans l'Arrangement de Wassenaar

Régime multilatéral de contrôle des exportations d'armements et des biens et technologies à double usage (civils et militaires) fondé en 1994, l'Arrangement de Wassenaar a pour objet d'éviter la prolifération des capacités militaires d'Etats ou de groupes criminels pouvant nuire à la paix et à la sécurité internationales. Dans le cadre de cet Arrangement de nature juridique informelle, les Etats participants s'engagent politiquement à contrôler, en vertu de leur législation nationale, les exportations des biens figurant sur les deux listes établies par l'Arrangement : la liste relative à l'armement (« *munitions list* » en anglais) et la liste des biens et technologies à double usage (dite « BDU » ou « *dual-use goods and technologies* » en anglais).

Tenant compte de la prolifération des logiciels intrusifs malveillants, les deux listes de l'Arrangement de Wassenaar ont été modifiées à partir des années 2010 pour s'adapter à ce phénomène. On remarquera que ces adaptations concernent particulièrement les outils de cyber-renseignement même si elles demeurent limitées pour restreindre le commerce de ce type d'outils au niveau international.

1. Des adaptations particulièrement applicables au cyber-renseignement

En 2012-2013, les « logiciels d'intrusion » utilisés notamment pour l'interception des télécommunications mobiles, la surveillance des réseaux IP et l'accès non autorisés à des systèmes numériques sont pris en compte par

¹ Article L. 863-1 du code de la sécurité intérieure.

l'Arrangement de Wassenaar sur proposition de la France et du Royaume-Uni en réaction aux révélations sur la vente d'outils de surveillance numérique à des régimes autoritaires pour la répression de leur population¹. Toutefois, si les « logiciels d'intrusion » ont fait l'objet d'une définition dans la liste BDU de l'Arrangement², seuls les systèmes, équipements et composants (4. A. 5.) ainsi que les logiciels (4. D. 4.) et technologies³ (4. E. 1. c.) pouvant servir techniquement à leur fonctionnement ont été introduits dans le régime de contrôle des exportations. Critiquées par les entreprises de cybersécurité en raison de leur effet trop restrictif, ces adaptations feront l'objet de modifications en 2017 afin notamment de prendre en considération les besoins du renseignement d'intérêt cyber⁴. Ainsi, il a été décidé de préciser que les biens soumis au régime de contrôle doivent non plus être seulement techniquement capable de servir au fonctionnement d'un logiciel d'intrusion mais plutôt d'être en mesure de donner des ordres et de faire exécuter des actions à ce type de logiciel. En outre, deux exemptions au contrôle des technologies ont été accordées en ce qui concerne la divulgation légitime de vulnérabilités informatiques et les échanges d'informations nécessaires sur les incidents de cybersécurité. On ne manquera pas de souligner, ici, l'adaptation exceptionnelle de l'Arrangement aux spécificités des outils numériques intrusifs qui s'est intéressé à leurs effets ou à leur usage en plus de leurs briques technologiques⁵.

Dans le cadre de la liste des matériels de guerre ou « *munitions list* », la proposition portée par la France d'y introduire les « armes numériques » ou

¹ Sur l'introduction des « logiciels d'intrusion », voir notamment A. Géry, « *Droit international et prolifération des cyberarmes* », op. cit..

² Le « logiciel d'intrusion » est défini de la façon suivante : « *logiciel spécialement conçu ou modifié pour éviter la détection par un « outil de surveillance », ou pour tromper les « contre-mesures de protection » d'un ordinateur ou d'un dispositif en réseau, et pour effectuer les tâches suivantes: a. extraction de données ou d'informations à partir d'un ordinateur ou d'un dispositif de réseau, ou modification des données système ou utilisateur; ou b. modification du chemin d'exécution standard d'un programme ou d'un processus afin de permettre l'exécution d'instructions provenant de l'extérieur* » (Liste BDU, définitions, Cat 4).

³ Selon l'Arrangement de Wassenaar, le terme « technologie » désigne les connaissances techniques sur un bien à double usage.

⁴ Sur la révision de 2017, voir notamment Observatoire du monde cybernétique, *La révision de l'Arrangement de Wassenaar dans le domaine des logiciels d'intrusion et ses conséquences*, Lettre n° 70, Janvier 2018.

⁵ En ce sens, voir notamment A. Géry, « *Droit international et prolifération des cyberarmes* », op. cit..

« cyberarmes »¹, des logiciels de lutte informatiques offensive ayant vocation à causer des dommages à des systèmes numériques, a été retenue en 2019-2020. Pour notre part, on relèvera que les logiciels espions de « *cyber reconnaissance* » et de « *cyber command and control* » utiles pour l'emploi des cyberarmes ont été inclus dans les logiciels de cyberdéfense militaire soumis au régime de contrôle des matériels de guerre (ML21. b. 5.).

2. Les limites de l'Arrangement de Wassenaar et du contrôle international des exportations

Bien que l'Arrangement ait été adapté à la militarisation du cyberspace et à la prolifération de la surveillance numérique mais aussi aux besoins de la cybersécurité, il convient de reconnaître que cet instrument international a une portée limitée en droit comme en fait. En effet, il s'agit d'un accord informel non contraignant pour les Etats participants qui peuvent adopter discrétionnairement des mesures différentes favorables ou non à la prolifération des outils numériques malveillants². Dans les faits, on retiendra que l'Arrangement n'a pas empêché la vente du logiciel espion israélien « Pegasus », spécialisé dans le piratage de smartphones, à des Etats comme le Maroc, l'Arabie saoudite, l'Inde ou la Hongrie, pour espionner des journalistes, des militants, avocats ou responsables politiques³. En matière de renseignement et de protection des citoyens contre les risques d'une surveillance abusive pour leurs droits et libertés, l'Arrangement reste inadapté sans un consensus sur les conditions d'un refus de licence d'exportation et pour encadrer le marché international des logiciels d'intrusion.

Pour autant, les Etats semblent vouloir toujours plus renforcer le contrôle et la transparence du marché des capacités de cyber-intrusion, ce qui a été exprimé

¹ Sur la proposition de la France, voir SGDSN, *Revue stratégique de cyberdéfense*, op. cit., p. 104 et 105.

² En ce sens, voir A. Géry, « *Droit international et prolifération des cyberarmes* », op. cit. ou plus spécifiquement pour les systèmes de surveillance numérique J. Keller, *L'exportation de systèmes de surveillance informatique par les sociétés privées européennes vers les pays tiers*, La Revue des droits de l'homme [En ligne], 11 | 2017, mis en ligne le 16 janvier 2017.

³ A ce sujet, voir le lien [Projet Pegasus » : révélations sur un système mondial d'espionnage de téléphones, Le Monde, 18 juillet 2021.](https://www.amnesty.fr/liberte-d-expression/actualites/surveillance-revelations-sur-le-logiciel-espion-israelien-pegasus-nso-group?)

dans le cadre du Processus de Pall Mall de 2024 portant sur l'importance des partenariats publics-privés dans le domaine du cyberespace¹.

Il est donc toujours possible de renforcer l'application du régime de contrôle des exportations des BDU aux biens de cybersurveillance², ce qui a été d'ailleurs démontré par l'Union européenne en consacrant un nouveau contrôle fondé sur la « sécurité humaine ».

§2. La consécration d'un contrôle européen spécifique des biens de cybersurveillance fondé sur la « sécurité humaine »

Considérant que les biens de cybersurveillance présentent un « *risque qu'ils soient utilisés à des fins de répression interne ou dans le cadre de la commission de violations graves des droits de l'homme ou du droit humanitaire* »³, l'Union européenne (UE) a profité de la refonte de son régime de contrôle des BDU en 2021 pour appliquer le concept de « sécurité humaine », développé depuis les années 1990 à l'initiative du Programme des Nations unies pour le développement (PNUD)⁴, dans les conditions d'autorisation d'exportation des biens de cybersurveillance.

A - Le risque du commerce des biens de cybersurveillance pour les droits de l'homme et le droit humanitaire

Dans le même contexte de scandale qui a conduit aux adaptations de l'Arrangement de Wassenaar en 2013, l'Union européenne a pris conscience que ses entreprises technologiques ne pouvaient plus librement vendre des biens de cybersurveillance à des régimes autoritaires sans entrer en contradiction avec ses valeurs de défense et de promotion des droits de l'homme. Une réforme du régime de contrôle des BDU a rapidement été proposée mais l'adoption d'un compromis

¹ A ce sujet, voir la note d'actualité « *Processus de Pall Mall : Lutter contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché (Lancaster House, Londres, 6 février 2024)* » en ligne sur le site France diplomatie et la contribution de H. Verdier et L. Rolland, « *L'usage responsable des capacités commerciales de cyber-intrusion : une perspective diplomatique* », dans le rapport de le 8^{ème} rapport de la CNCTR (pages 175 à 179).

² En ce sens, voir R. Klein, *Trimming Pegasus' Wings : International Export Control Law and Cyberweapons* », *Völkerrechtsblog*, 27.10.2021.

³ Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (considérant 2).

⁴ Cf. PNUD, Rapport sur le développement humain de 1994, Paris, Economica, 1994, p. 13.

entre les intérêts stratégiques et commerciaux et la prise en compte jugée nécessaire du risque pour les droits de l'homme fut lente.

1. Le scandale des ventes de biens de cybersurveillance à des régimes autoritaires

Généralement mis à disposition des Etats par des entreprises privées du numérique pour les besoins de la sécurité nationale, de la lutte contre le terrorisme ou de la cybercriminalité, les biens de cybersurveillance peuvent s'avérer être de véritables outils de contrôle et de répression des populations ou de violations du droit international humanitaire en situation de conflit armé. Concrètement, ces biens peuvent constituer une menace directe pour le respect du droit à la vie privée mais aussi avoir des effets dissuasifs pour les libertés d'expression, de communication et d'information lorsqu'ils permettent une surveillance massive des communications, ce que confirme la jurisprudence des juges européens¹. Plus encore, les biens de cybersurveillance peuvent contribuer à restreindre les libertés d'association et de réunion, voir même à des risques de détentions arbitraires et d'atteintes à l'intégrité physique des personnes².

Malheureusement, de nombreuses enquêtes journalistiques ont démontré que ces violations des droits de l'homme et du droit humanitaire ont réellement été permises par la vente de biens de cybersurveillance par des entreprises européennes à des régimes autoritaires, notamment lors du « Printemps arabe » pour réprimer spécifiquement les mouvements de contestation³. A titre d'exemple, on mentionnera que la société française de cybersurveillance, Amesys, et ses dirigeants ont été mis en examen en 2021 pour complicité de torture en Libye entre 2007 et 2011 pour avoir fourni un outil de surveillance au régime autoritaire de Mouammar Kadhafi⁴. Les révélations de l'affaire du logiciel espion

¹ Voir notamment les affaires *Weber et Saravia* de 2006 (points 139 et suivants) et *Big Brother Watch* de 2021 (points 428 à 458) de la CEDH et C-511/18, *La Quadrature du Net* (points 118, 173 et 186) et C-623/17, *Privacy International* (point 72) de la CJUE du 6 octobre 2020.

² En ce sens, voir M. Bromley, *Export controls, human security and cyber-surveillance technology : examining the proposed changes to the EU dual-use regulation*, Stockholm International Peace Research Institute, December 2017.

³ A ce sujet, voir M. Kanetake, *The EU's dual-use export control and human rights risks : the case of cyber surveillance technology*. Eur. World. 2019. Vol. 3(1) ou encore M. Goupy, « *La bienveillante neutralité des technologies d'espionnage des communications : le cas tunisien* », Cultures & Conflits, 93 | 2014, 109-124.

⁴ Cf. FIDH, « *Surveillance et torture en Libye : la Cour d'appel de Paris confirme la mise en examen d'Amesys et de ses dirigeants, et annule celle de deux salariés* », 21 novembre 2022.

israélien « Pegasus » citée précédemment semble également confirmer les atteintes effectives aux droits de l'homme et au droit humanitaire à travers le monde par la prolifération des biens de cybersurveillance.

2. La lente adoption d'une réforme jugée nécessaire du régime européen des biens à double usage

Les parlementaires européens ont rapidement réagi aux révélations sur le « Printemps arabe » en déplorant « *le rôle joué par les entreprises européennes dans l'exportation d'armes et de biens à double usage vers des régimes répressifs, et dans la participation à des ruptures technologiques orchestrées par les dictatures* » tout en appelant la Commission européenne « *à élaborer des lignes directrices afin d'amener les entreprises européennes à agir en cohérence avec les principes fondamentaux de l'Union dans de telles situations* »¹, notamment en adaptant le règlement (CE) n° 428/2009 du Conseil du 5 mai instituant le régime de contrôle des BDU aux enjeux des systèmes de surveillance numérique pour les droits de l'homme².

Après les modifications du règlement (CE) n° 428/2009 pour y introduire les adaptations de l'Arrangement de Wassenaar relatives aux « logiciels d'intrusion »³, la Commission a rédigé une proposition de refonte et de simplification du régime européen de contrôle des BDU en 2016 dans laquelle il a été proposé de définir une liste autonome de l'Union européenne de technologies de cybersurveillance systématiquement soumis à un contrôle et de soumettre les technologies similaires non inscrites sur la liste à un contrôle « attrape-tout » ciblé lorsqu'elles sont envisagées par l'utilisateur final à des fins de violations graves des droit de l'homme ou du droit humanitaire⁴. Cette proposition a entraîné certaines tensions entre les Etats membres et les industriels de la

¹ Résolution du Parlement européen du 10 mai 2012 sur le commerce pour le changement : stratégie de l'Union européenne en matière de commerce et d'investissements pour le sud de la Méditerranée après les révolutions du Printemps arabe (2011/2113(INI)).

² Résolution du Parlement européen du 8 septembre 2015 concernant les droits de l'homme et la technologie : incidences des systèmes d'intrusion et de surveillance sur les droits de l'homme dans les pays tiers (2014/2232(INI)).

³ Le régime européen de contrôle des exportations des BDU se conforme aux règles établies par l'Arrangement de Wassenaar et à ses listes sur les armes conventionnelles et les BDU.

⁴ Proposition de règlement du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte).

cybersurveillance. Révélateurs d'un enjeu de gouvernance de l'Internet et de son économie, les désaccords ont porté sur les points suivants : la constitution d'une liste autonome de biens de cybersurveillance ; l'application du concept de « sécurité humaine »¹ dans la politique commerciale de l'Union européenne, c'est-à-dire de la primauté des droits de l'homme ou du droit humanitaire sur les intérêts stratégiques et commerciaux, et d'une logique de contrôle fondé sur l'usage finale des biens de cybersurveillance à la place d'un contrôle portant sur des briques technologiques présentant un risque de militarisation ; l'application d'un principe de « *due diligence* » aux industriels de la cybersurveillance pour garantir le respect du principe de « sécurité humaine » ; le risque d'une restriction excessive impactant le commerce international des biens numériques et de cybersécurité utiles à la société².

Finalement, une proposition moins ambitieuse a été adoptée le 20 mai 2021 dans le règlement (UE) 2021/821 du Parlement et du Conseil de refonte du régime des BDU. Toutefois, l'application du concept de « sécurité humaine », qui est au fondement de l'élaboration d'un nouveau contrôle des biens de cybersurveillance³, n'a pas été remise en cause. Si on peut critiquer la lenteur des négociations et de l'adaptation du régime européen des BDU au risque reconnu en 2012 du commerce des biens de cybersurveillance pour les droits de l'homme et le droit humanitaire, il convient de mesurer nos propos en rappelant que cette adaptation s'inscrit dans une refonte plus globale du régime de contrôle des exportations.

Désormais, la question se pose de savoir si l'application du concept de « sécurité humaine » dans le régime de contrôle des biens de cybersurveillance permet de lutter efficacement contre la prolifération de ces biens et, par là même, de constituer une mesure de protection effective des droits de l'homme et du droit humanitaire.

¹ Sur ce concept, voir notamment M. Kaldor, « *La sécurité humaine : un concept pertinent ?* », *Politique étrangère*, vol., no. 4, 2006, pp. 901-914.

² A ce sujet, voir M. Kanetake, *The EU's dual-use export control and human rights risks : the case of cyber surveillance technology*. op. cit. et C. Perarnaud, « *Les contrôles aux exportations comme instruments de pouvoir dans la gouvernance de l'Internet* », *Terminal* [En ligne], 132-133 | 2022, mis en ligne le 28 février 2022.

³ Voir en ce sens J. Ancelin, « *L'Union européenne et les biens à double usage : La politique commerciale commune à l'aune de la sécurité humaine* », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 18 octobre 2017.

B - L'application du concept de « sécurité humaine » dans le contrôle des exportations des biens de cybersurveillance

En matière de cybersurveillance, la solution retenue par le nouveau règlement (UE) 2021/821 ne consacre qu'un nouveau régime d'autorisation dans le cadre d'un contrôle « attrape-tout » ciblé pour les biens non répertoriés qui risquent d'être utilisés pour la répression interne et/ou la commission de violations graves et systématiques des droits de l'homme et du droit humanitaire. Bien que le respect du concept de « sécurité humaine » conditionne les exportations des biens de cybersurveillance non répertoriés, certaines critiques peuvent être soulevées sur la cohérence de ce nouveau dispositif.

1. Un régime d'autorisation ciblé, le contrôle « attrape-tout » des biens de cybersurveillance non répertoriés

Depuis la création des régimes de contrôle des exportations des armes et des biens à double usage, un contrôle appelé « attrape-tout » a été envisagé pour appréhender les biens non-listés mais susceptibles d'être utilisés à des fins militaires¹. En droit européen, un contrôle général « attrape-tout » des BDU est prévu à l'article 4 du nouveau règlement (UE) 2021/821.

Pour ce qui concerne notre étude, l'article 5 du règlement européen de 2021 prévoit une obligation spécifique d'autorisation préalable d'exportation de certains biens de cybersurveillance qui ne sont pas énumérés dans la liste des BDU (annexe I du règlement), c'est-à-dire des biens autres que ceux utiles au fonctionnement des « logiciels d'intrusion » définis par l'Arrangement de Wassenaar. Les biens à double usage soumis à ce contrôle « attrape-tout » particulier sont ceux *« conçus spécifiquement pour permettre la surveillance discrète de personnes physiques par la surveillance, l'extraction, la collecte ou l'analyse de données provenant de systèmes d'information et de télécommunications »* (point 20 de l'article 2 du règlement). Parmi ces biens de cybersurveillance, seuls sont concernés par une autorisation les biens considérés comme pouvant être *« destinés, entièrement ou en partie, à une utilisation*

¹ Le contrôle « attrape-tout » a été envisagé dans la directive n° 7 du Missile Technology Control Regime (MTCR), par le Nuclear Suppliers Group (NSG) pour les BDU pour l'armement nucléaire dans une décision de la réunion plénière de 2004 à Göteborg, par le Groupe d'Australie (GA) sur le contrôle des armes chimiques et biologiques ainsi que par l'Arrangement de Wassenaar.

impliquant la répression interne et/ou la commission de violations graves et systématiques des droits de l'homme et du droit humanitaire international » (paragraphe 1 de l'article 5).

La caractérisation d'un risque pour les droits de l'homme ou le droit humanitaire est opéré par l'autorité de contrôle compétente dans les Etats membres qui en informe l'exportateur ou par ce dernier dans le cadre de ses obligations de vigilance et d'information (paragraphe 2 de l'article 5)¹. Cependant, la décision de soumettre l'exportation à autorisation ou non revient uniquement à l'autorité nationale de contrôle. En France, cette autorité est le Service des biens à double usage (SBDU)² qui est assisté par la Commission interministérielle des biens à double usage (CIBDU)³.

Afin d'éviter le contournement du contrôle « attrape-tout » et d'une décision de refus d'autorisation, le règlement prévoit un mécanisme de coordination et d'échanges d'informations entre les Etats membres et la Commission européenne sur les biens de cybersurveillance identifiés comme problématiques et les décisions d'autorisation (paragraphe 4 et suivants de l'article 5).

Les biens de cybersurveillance non répertoriés soumis au régime d'autorisation et au contrôle « attrape-tout » devraient se préciser au fur et à mesure des cas d'exportation et des échanges d'informations entre les Etats membres et la Commission. Néanmoins, il est théoriquement possible d'envisager que certains biens non répertoriés comme les technologies biométriques de reconnaissance faciale, les appareils de géolocalisation ou les logiciels de renseignement d'origine sources ouvertes soient systématiquement soumis au contrôle « attrape-tout » lorsqu'ils ont vocation à permettre discrètement la collecte et/ou le traitement automatisé de données sensibles ou de données de

¹ Ministère de l'économie, *Rapport au Parlement sur les exportations des biens à double usage de la France*, Direction générale des Entreprises, juillet 2022, p. 13.

² Décret n° 2020-74 du 31 janvier 2020 relatif au service à compétence nationale dénommé « service des biens à double usage ».

³ Décret n° 2010-294 du 18 mars 2010 portant création d'une commission interministérielle des biens à double usage (CIBDU).

façon massive d'individus ou lorsqu'ils sont « essentiels » à la surveillance numérique¹.

2. Les critiques sur la cohérence du régime européen de contrôle des exportations des biens de cybersurveillance

Une première critique peut être soulevée concernant l'objectif de simplification du régime de contrôle des BDU, notamment en ce qui concerne l'ensemble des biens et technologies de cybersurveillance. En effet, l'introduction de ce nouveau contrôle « attrape-tout » a pour conséquence de morceler en deux régimes distincts dans leur fondement les autorisations d'exportation² :

- le régime des biens et technologies utiles au fonctionnement des « logiciels d'intrusion » qui contribuent à la militarisation du cyberspace ;
- le régime des biens dont l'usage final est prévu pour la répression interne et la violation grave des droits de l'homme ou du droit humanitaire.

Autrement dit, tous les biens de cybersurveillance ne sont pas nécessairement soumis à un contrôle qui applique le concept de « sécurité humaine », même si les autorités nationales compétentes devraient pouvoir, en droit interne, systématiquement fonder cumulativement leur contrôle sur les risques pour la militarisation du cyberspace et les droits de l'homme.

D'autres critiques concernent l'effectivité du concept de « sécurité humaine » dans la lutte contre la prolifération des biens de cybersurveillance. Pour les autorités nationales comme pour l'exportateur dans le cadre de son obligation de vigilance, il peut s'avérer difficile en pratique de caractériser un risque de violation grave des droits de l'homme ou du droit humanitaire dans l'usage final de ces biens qui ont normalement vocation à porter atteinte à des droits et libertés comme le droit au respect de la vie privée mais pour des motifs légitimes tels que la lutte contre le terrorisme ou la cybercriminalité. Cette difficulté est de nature à entraîner un important contentieux des décisions de refus d'autorisation

¹ A ce sujet, voir O. L. van Daalen, J.V.J. van Hoboken, M. Rucz, *Export control of cybersurveillance items in the new dual-use regulation : The challenges of applying human rights logic to export control*, Computer Law & Security Review : The International Journal of Technology Law and Practice, April 2023.

² Dans le même sens, voir L. -M. Chauvel, *Chronique Action extérieure de l'UE : La refonte en demi-teinte du règlement relatif aux biens à double usage*, RTD Eur. 2021, p.705.

d'exportation avec les entreprises de cybersurveillance qui pourraient se plaindre de mesures trop restrictives pour leur liberté du commerce et de l'industrie.

En outre, le mécanisme anti-contournement prévu par le règlement européen demeure fragile et son application pourrait varier selon les intérêts stratégiques et économiques des Etats. De leur côté, les entreprises de cybersurveillance pourraient se montrer méfiantes à l'égard du nouveau contrôle « attrape-tout » pour la protection de leurs informations commerciales sensibles, bien que le règlement européen exige le respect du secret et de la confidentialité des informations protégées dans les échanges d'informations¹. En revanche, Il convient de souligner qu'en France le non-respect par l'exportateur des procédures d'autorisation d'exportation est constitutif d'un délit douanier².

Quoi qu'il en soit, l'application du concept de « sécurité humaine » dans la contre-prolifération des biens de cybersurveillance doit être saluée malgré les incertitudes sur son effectivité. A cet égard, des évaluations sur le nouveau dispositif de contrôle de ces biens sont prévues par le règlement européen³ qui devraient permettre de répondre aux critiques soulevées précédemment.

Au regard de la protection du cyberspace, on prolongera notre étude sur la diffusion et l'utilisation des technologies de surveillance intrusive pour le renseignement en soutenant qu'elles doivent également être limitées par le biais des législations et réglementations liées à la cybersécurité dans un souci de confiance dans l'économie numérique⁴.

¹ Paragraphe 9 de l'article 5 du nouveau règlement (UE) 2021/821.

² Article 414 du code des douanes.

³ Article 26 du nouveau règlement (UE) 2021/821.

⁴ Dans le même sens, voir l'Avis n° 8/2015 du contrôleur européen de la protection des données sur la diffusion et l'utilisation de technologies de surveillance intrusive du 15 décembre 2015.

CHAPITRE II

LE RENSEIGNEMENT NUMERIQUE ET LA CYBERSECURITE

L'encadrement de la numérisation du renseignement constitue un défi pour la confiance dans l'économie numérique dont la sauvegarde repose pour une grande partie sur la sécurité des systèmes numériques. Comme dans toutes les organisations publiques ou privées, les systèmes numériques des services de renseignement ne sont pas infailibles, ils constituent même des cibles privilégiées des cyberattaques. En ce sens, on rappellera l'acquisition frauduleuse de cyberarmes de la NSA par des cybercriminels qui a conduit aux cyberattaques *WannaCry* et *NotPetya* en 2017, ce qui soulève la question de la cyberprotection des services de renseignement¹ (**Section II**). D'une large portée aux contours incertains, cette dernière notion correspond aux mesures technico-juridiques de préservation de la sécurité des systèmes numériques².

Du point de vue de la société dans son ensemble, les besoins du renseignement ne doivent pas aboutir à fragiliser ou remettre en cause des exigences de sa cybersécurité (**Section II**).

¹ Dans le même sens, voir A. Géry, « *La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense* », Les Champs de Mars, vol. 30+s, no. 1, 2018, pp. 307-316.

² Cf. Vocabulaire de la défense, JORF, 19 septembre 2017, NOR : CTNR1724864K.

SECTION I : La cyberprotection du renseignement

A titre liminaire, il convient de préciser qu'il est difficile de fournir une véritable analyse juridique documentée de la cyberprotection du renseignement en raison du caractère très secret de cette activité de la numérisation des services de renseignement. Toutefois, le peu d'éléments publiquement disponibles nous a conduit à faire ressortir un certain nombre de mesures technico-juridiques de sécurité des systèmes numériques sensibles de l'Etat qui, de façon plus ou moins évidente, nous semble trouver à s'appliquer aux services de renseignement.

Ainsi, on invoquera tout d'abord les règles de protection relatives à la dématérialisation des informations classifiées du droit du secret de la défense nationale qui s'appliquent indéniablement au renseignement (§1). Ensuite, on relèvera que certaines règles du droit du renseignement et du droit de la cyberdéfense contribuent indirectement à la cyberprotection du renseignement (§2). Enfin, on soulèvera la problématique de la maîtrise des technologies et services numériques nécessaires à la numérisation du renseignement qui peuvent être fournies par les industriels du numérique (§3).

§1. Les exigences du secret de la défense nationale sur la dématérialisation des informations classifiées

Dans le domaine de la sécurité nationale, la classification des informations est une mesure destinée à restreindre leur diffusion ou leur accès en raison de leur caractère secret. Les informations classifiées relèvent ainsi du droit du secret de la défense nationale dont le régime de protection est de nature pénale¹. Dans son volet administratif, les articles R. 2311-1 et suivants du code de la défense et l'Instruction générale interministérielle n° 1300 (IGI 1300) du 9 août 2021² formalisent les exigences pratiquées à mettre en œuvre dans les administrations et les entreprises depositaires pour assurer la protection des informations classifiées selon deux niveaux « Secret » et « Très Secret »³. Quatre principes

¹ Article 413-9 et suivants du code pénal.

² Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

³ Depuis le décret n° 2019-1271 du 2 décembre 2019, le système de classification français s'est aligné sur les standards internationaux de classification des secrets de défense et de sécurité. Avant le 1^{er} juillet 2021, l'ancien système français de classification comprenait trois niveaux : « Confidentiel-Défense », qui est devenu le niveau « Secret » ; « Secret-Défense », qui est devenu le

rigoureux gouvernement notamment l'application de cette protection selon l'IGI 1300 : la matérialité du secret dans un document électronique ou non permettant de lui apposer un « timbre de classification » ; le contrôle de confiance préalable incarné par une procédure d'habilitation des personnes ou d'homologation des biens et la règle du « besoin d'en connaître », c'est-à-dire d'accès à une information classifiée que dans le cadre de l'exercice d'une fonction ou de l'accomplissement d'une mission ; le cloisonnement des informations classifiées par des règles limitant notamment leur partage ; la traçabilité de ces informations tout le long de leur cycle de vie.

La protection des informations classifiées concerne directement le renseignement, les services étant assujettis au secret de la défense nationale du fait de leurs missions qui relèvent de la surveillance secrète de sécurité nationale. On relèvera ainsi que les études générales, synthèses, comptes rendus de renseignement sont généralement classifiées au niveau « Secret » et, dans certains cas, au niveau « Très secret »¹. En ce sens, la protection du secret vaut alors protection du renseignement. Par ailleurs, on notera que la Direction générale de la sécurité intérieure (DGSI), notamment pour les enquêtes judiciaires sur la compromission du secret, la Direction du renseignement et de la sécurité de la défense (DRSD) et la Direction générale de la sécurité extérieure (DGSE) sont les services chargés du respect de cette protection dans leur mission de contre-espionnage².

Dans le cadre de notre étude, on peut observer que les dispositions réglementaires générales applicables aux entités dépositaires d'informations classifiées consacrent des mesures spécifiques en matière de sécurité numérique. Ces dispositions semblent être invocables pour encadrer la cyberprotection des services de renseignement, d'autant plus que les dispositions relatives à la sécurité des systèmes d'information et de communication de l'Etat ne s'appliquent pas aux

niveau « Très Secret » sans classification spéciale ; « Très Secret-Défense », qui est le niveau « Très Secret » faisant l'objet d'une classification spéciale.

¹ cf. Instruction ministérielle sur la protection du secret de la défense nationale du Premier ministre du 1er décembre 2021.

² Cf. IGI 1300, « Procédure à suivre en cas de compromission ».

systèmes et moyens de communication de la défense, de la DGSE et de la DGSI¹. Toutefois, on soulignera que les textes classifiés relatifs aux services de renseignement peuvent prévoir des conditions plus spécifiques aux besoins du renseignement ou encore des dérogations aux textes de portée générale.

A – Les mesures spécifiques à la sécurité numérique

Selon le décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale, trois types de mesures de sécurité numérique doivent être distingués : l'homologation des systèmes d'information contenant des informations classifiées² ; le déploiement de dispositifs, matériels ou logiciels agréés de cyberprotection³ ; et, la mise en place d'une organisation dédiée à la cybersécurité des informations classifiées sous la responsabilité d'une autorité qualifiée en sécurité des systèmes d'information⁴. L'ensemble de ces mesures sont précisées par l'IGI 1300 qui constitue le principal texte pratique de référence mis à la disposition du public et qui doit être suivi par tout organisme amené à traiter des informations classifiées.

1. L'homologation des systèmes d'information classifiés

Parallèlement à la procédure d'habilitation des personnes physiques et morales qui participe indirectement à la cybersécurité des informations classifiées, les systèmes d'information traitant ces informations doivent être homologués préalablement à leur emploi, sauf en cas d'urgence opérationnelle sous réserve d'une autorisation provisoire d'emploi. Reposant sur une analyse de risques globale qui inclut les risques de l'usage de supports amovibles sur le système d'information, des interconnexions avec d'autres systèmes, de l'accès à distance ou encore des moyens d'hébergement et d'assistance technique, la décision d'homologation atteste que les mesures de protection nécessaires sont mises en œuvre. Dans cette démarche, l'IGI 1300 précise que la décision d'homologation vaut décision de classification pour une durée maximale de trois ans pour le niveau « Secret » et de deux ans pour le niveau « Très Secret » et qu'il

¹ Article 1 du décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique (DINUM).

² Al. 1 et 2 de l'article R. 2311-6-1 du code de la défense.

³ Al. 3 de l'article R. 2311-6-1 du code de la défense.

⁴ Article R. 2311-6-2 du code de la défense.

est interdit de recourir à un système d'information classifié pour traiter des informations dont le niveau de classification est supérieur au système homologué. Ce même texte exige également une décision d'homologation spécifique pour les interconnexions entre les systèmes d'information classifiés de même niveau et prohibe toutes interconnexions entre des systèmes d'information de niveaux de classification différents ou entre des systèmes classifiés et non-classifiés, sauf pour un besoin opérationnel strictement nécessaire. Dans ce dernier cas, l'interconnexion est homologuée au niveau du système d'information le plus élevé.

S'agissant du contrôle de l'homologation, il est assuré tout au long du cycle de vie du système d'information classifié par l'autorité d'homologation qui en fixe les conditions de maintien et réalise des audits de sécurité. Toutefois, notons qu'une nouvelle décision d'homologation est obligatoire en cas de modifications significatives du système, d'une nouvelle interconnexion ou de risques avérés ou nouveaux ou d'un incident de sécurité. L'autorité d'homologation est le SGDSN, avec l'assistance de l'ANSSI, pour les systèmes d'information classifiés relevant du Premier ministre ou pour ceux classifiés au niveau « Très Secret » faisant l'objet d'une classification spéciale. Pour les systèmes d'information « Secret » ou « Très secret », hors classifications spéciales, l'autorité qualifiée en sécurité des systèmes d'information (AQSSI) est l'autorité d'homologation. Une commission d'homologation, composée des représentants de l'autorité d'emploi du système d'information, assiste le SGDSN ou l'AQSSI. Enfin, cette commission peut convier l'ANSSI qui est obligatoirement destinataire de toute décision d'homologation et qui doit être en mesure de contrôler, à tout moment, les rapports d'audit et le dossier d'homologation. Ce dernier contient toutes les mesures qui répondent aux règles strictes et précises de cyberprotection que doit respecter le système d'information homologué.

2. Le déploiement de dispositifs de cyberprotection

Au minimum, les mesures de sécurité des systèmes d'information classifiés doivent respecter deux types de barrières de sécurité et certaines règles spécifiques de sécurité consacrées par l'IGI 1300. Ces dispositions peuvent être complétées par des instructions plus ciblées de l'ANSSI.

Les barrières de sécurité

Le premier type de barrière est physique, c'est-à-dire que les lieux abritant des systèmes d'information classifiés et les matériels utilisés pour leur fonctionnement doivent être sécurisés par les mêmes mesures de sécurité physiques applicables à l'accès aux informations et supports classifiés prévues par l'IGI 1300. S'ajoute à ces mesures de sécurité physique, la prise en compte de la réglementation en matière de protection contre les signaux compromettants prévue par l'Instruction interministérielle n° 300/SGDSN/ANSSI. Il s'agit des mesures de lutte contre la « menace TEMPEST », c'est-à-dire de contre-espionnage des moyens d'interception et d'exploitation des périphériques et technologies de communication sans fil ou pour faire face aux risques de signaux parasites.

Le second type de barrière est inhérent aux systèmes d'information classifié ou « logique », c'est-à-dire qu'il consiste à équiper le système de dispositifs matériels ou logiciels de sécurité agréés par l'ANSSI. Ces dispositifs mettent notamment en œuvre des fonctionnalités de chiffrement des données et des communications ou encore de détection des cyberattaques. Les fonctionnalités des dispositifs sont davantage précisées dans les différentes règles spécifiques à certains aspects de la sécurité des systèmes d'information classifiés.

Les règles de sécurité spécifiques

Dès sa conception et durant toute la durée d'exploitation du système d'information classifié, les services de sécurité informatique de l'autorité d'emploi veillent à assurer :

- la sécurité des privilèges d'administration du système d'information, c'est-à-dire à recourir à un personnel habilité, spécialement formé et sensibilisé au niveau de classification du système et à séparer les ressources et flux métier de ceux d'administration du système ;
- la minimisation de l'exploitation du système d'information classifié en n'installant que les fonctionnalités uniquement indispensables à son fonctionnement et à sa sécurité ;
- le contrôle et la traçabilité des accès, avec leur revue périodique, des personnes physiques au système d'information sur la base du principe de « moindre privilège » qui est le corolaire informatique de la règle du

« besoin d'en connaître ». Autrement dit, l'IGI 1300 exige la création d'un compte individuel avec restriction des droits d'accès en fonction du besoin d'en connaître. Pour le niveau « Très Secret », un mécanisme d'authentification forte avec traçabilité systématique des accès doit être prévu. En ce qui concerne les informations classifiées avec une mention complémentaire telle que « Spéciale France », leur stockage est zoné et cloisonné dans le système d'information. Il peut être dérogé à ces règles si des mesures organisationnelles sont mises en œuvre et sur autorisation de l'ANSSI ;

- la mise en œuvre de dispositifs de sécurité informatique : journalisation des événements avec horodatage synchronisé et mécanisme d'imputabilité des opérations sans toutefois traiter les informations d'authentification ; systèmes de détection des incidents de sécurité informatiques, notamment des sondes de détection de marqueurs techniques d'attaques ou d'anomalies basées sur les référentiels de l'ANSSI prévus pour l'application du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information, et organisation d'une réponse à incident en liaison avec l'ANSSI ; systèmes de mises à jour et de veille sur les vulnérabilités informatiques et leur correction. On ajoutera, ici, que l'IGI 1300 exige le respect de l'Instruction interministérielle n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI) qui vise à assurer la traçabilité et l'intégrité, de manière spécifique, des dispositifs de sécurité ;
- le cloisonnement des systèmes d'information classifiés selon leur niveau de classification et le filtrage de leurs flux de données avec un mécanisme de blocage selon un principe de minimisation des flux ;
- le plan de continuité ou de reprise informatique qui doit être tenu à jour et régulièrement testé.

Les services de sécurité informatique de l'autorité d'emploi veillent également à préserver la sécurité des informations classifiées dans les situations de mobilité :

- d'une part, ils fournissent les équipements informatiques agréés traitant d'informations classifiées pour les déplacements. De son côté, l'utilisateur est soumis à une obligation de surveillance permanente de l'équipement et à une interdiction de son utilisation dès lorsqu'il y a un risque de compromission. En cas de sortie du territoire national de l'équipement, une autorisation préalable de l'officier de sécurité des systèmes d'information est obligatoire ;
- d'autre part, les accès à distance à un système d'information classifié est en principe interdit, sauf nécessité absolue pour des raisons opérationnelles avec la mise en œuvre de dispositifs de sécurité agréés et adaptés.

En ce qui concerne la connexion ou l'installation de supports amovibles (clés usb, cartes mémoires ou disques dur externes par exemple) au système d'information classifié, l'IGI 1300 énonce :

- une interdiction de connexion ou d'installation d'équipements amovibles personnels et une interdiction similaire pour les équipements d'un niveau de classification différent. Dans ce dernier cas, une dérogation peut être prévue pour la stricte nécessité d'un besoin opérationnel ;
- l'obligation que les supports amovibles prévus d'être utilisés sur le système d'information classifié soient inscrits dans le dossier d'homologation et qu'ils soient gérés par l'autorité d'emploi, notamment en dédiant des points de connexion et d'installation des supports amovibles spécialement prévus pour le système d'information classifié.

Une organisation dédiée à la mise en œuvre de ces mesures doit être mise en place, il s'agit du troisième type de mesures de sécurité numérique en matière de secret de la défense nationale.

3. Une organisation dédiée à la cybersécurité du secret

L'un des principaux apports du décret n° 2019-1271 du 2 décembre 2019 dans la protection du secret de la défense nationale est d'obliger les organismes disposant de systèmes d'information classifiés de placer leur sécurité sous la responsabilité d'une autorité qualifiée en sécurité des systèmes d'information (AQSSI)¹. Au sein de la chaîne fonctionnelle de sécurité des systèmes d'information définie par l'IGI 1300, l'AQSSI est désigné par le ministre de tutelle de l'organisme concerné ou, dans les autres cas, par le responsable de l'organisme lui-même. Il est chargé de la politique de sécurité des systèmes d'information classifiés (PSSI) et de leur cartographie. Il désigne l'officier de sécurité des systèmes d'information (OSSI) parmi son personnel. Ce dernier conçoit et met notamment en œuvre le management de la sécurité des systèmes d'information en collaboration étroite et quotidienne avec l'officier de sécurité (OS) en charge de la chaîne fonctionnelle de protection du secret au sein de l'organisme. En outre, un responsable de la sécurité du système d'information (RSSI) est également désigné pour piloter et contrôler la démarche d'homologation d'un système d'information classifié. Selon l'IGI 1300, *« il est garant de la cohérence des mécanismes et des procédures de sécurité ainsi que du maintien du niveau de sécurité dans le temps »* et *« assure principalement les fonctions opérationnelles liées à la sécurité des systèmes d'information classifiés relevant de son périmètre de responsabilité »*².

Cette chaîne fonctionnelle de sécurité des systèmes d'information s'articule ainsi avec la chaîne fonctionnelle de protection du secret de la défense nationale, notamment en suivant les directives des fonctionnaires de sécurité des systèmes d'information (FSSI) relevant des hauts fonctionnaires de défense et de sécurité (HFDS), qui animent, coordonnent et contrôlent l'application des règles de la protection du secret de la défense nationale au niveau ministériel. Le SGDSN et l'ANSSI supervisent cette articulation pour les services du Premier ministre. On relèvera la création par décret n° 2020-455 du 21 avril 2020 de l'Opérateur des systèmes d'information interministériels classifiés (OSIIC) rattaché au SGDSN et

¹ Article R. 2311-6-2 du code de la défense.

² Cf. IGI 1300, « Le responsable de la sécurité du système d'information (RSSI) », p. 44.

spécialement chargé des moyens numériques sécurisés interministériels utilisés par le Président de la République et le Gouvernement.

Si les textes réglementaires du code de la défense relatifs à la protection numérique du secret de la défense nationale, complétés par les règles pratiques de l'IGI 1300, constituent des sources non négligeables pour les services de renseignement dans leur cyberprotection, il reste que l'application de ces dispositions de portée générale devrait faire l'objet d'aménagements spécifiques aux besoins du renseignement.

B - L'application des mesures de sécurité numérique au renseignement

A priori, les services de renseignement se conforment aux trois types de mesures de sécurité numérique précédemment exposés tout en ayant la possibilité d'appliquer des conditions plus adaptées à leurs besoins. Néanmoins, le secret de la défense nationale peut soulever des difficultés dans les développements de la numérisation du renseignement.

1. Des mesures de sécurité numérique adaptables aux besoins du renseignement

Certains textes administratifs font applications des mesures de sécurité numérique du secret de la défense nationale prévues au code de la défense et dans l'IGI 1300 dans les services de renseignement. Ainsi, l'arrêté du 20 mai 2016 portant désignation et attributions des autorités qualifiées en sécurité des systèmes d'information du ministère de l'intérieur dispose que le directeur général de la DGSi est désigné AQSSI dans le cadre de l'organisation dédiée à la cybersécurité du secret. De même, l'arrêté du 22 octobre 2013 portant organisation de la direction du renseignement et de la sécurité de la défense désigne comme AQSSI le directeur de la DRSD qui est assisté par son sous-directeur technique dans cette fonction. En matière d'homologation des systèmes d'information classifiés, on relèvera que l'article 2 de l'arrêté du 9 mai 2014 relatif à la protection du secret de la défense nationale au sein de la DGSi dispose que : *« les systèmes d'information de la direction générale de la sécurité intérieure contenant des informations classifiées font l'objet, préalablement à leur emploi, d'une homologation de sécurité à un niveau au moins égal au niveau de classification*

de ces informations dans les conditions prévues par une instruction classifiée et non publiée du directeur général de la sécurité intérieure ».

Par ailleurs, le rapport de la DPR 2019-2020 nous révèle, dans une partie intitulée « la sécurité interne des systèmes d'information », que les services de renseignement mettent en œuvre des dispositifs de cyberprotection similaires à ceux prévus par l'IGI 1300, tout en signalant que des lacunes dans ce domaine ont été partagées par les services aux parlementaires¹. A ce sujet, soulignons que la DPR recommande de « *procéder à un audit régulier des systèmes d'information des services de renseignement et, en tant que de besoin, accompagner ces services dans la démarche d'homologation visant à protéger le secret de la défense nationale* ». On ajoutera que le rapport note que « *la DPR ne dispose toutefois ni des ressources ni des compétences pour entreprendre de tels audits, mais sollicite des services compétents – en l'espèce l'ANSSI et le GIC pour les techniques de recueil de renseignement – la conduite de telles missions qui permettront aux services de mieux protéger les informations et les supports classifiés dont ils disposent. Le CNRLT pourrait veiller à ce qu'un plan d'audits soit établi au bénéfice des services qui n'ont pas encore reçu d'homologation* ».

Deux remarques doivent être faites pour compléter ces considérations. Premièrement, les systèmes numériques des services de renseignement font l'objet d'instructions classifiées et non publiées qui devraient établir les conditions particulières applicables en matière de sécurité numérique. Ces conditions pourraient prévoir des aménagements par rapport aux mesures édictées par l'IGI 1300. Deuxièmement, ce dernier texte de portée générale prévoit des dérogations aux procédures et règles de sécurité numérique d'informations classifiées pour la stricte nécessité d'un besoin opérationnel, ce qui peut être invoqué par les services de renseignement dans l'acquisition, le développement et l'utilisation de nouveaux moyens numériques de renseignement.

Ces aménagements et dérogations peuvent s'avérer utiles afin d'éviter une application trop rigide des exigences du secret de la défense nationale à la numérisation du renseignement.

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 174 à 180.

2. La conciliation des exigences du secret avec la numérisation du renseignement

La nécessaire application d'exigences de sécurité numérique du secret de la défense nationale dans les services de renseignement constitue un défi pour ces derniers. En effet, ces exigences importantes peuvent constituer un frein au déploiement opérationnel rapide et croissant des moyens numériques de renseignement. On soulignera d'ailleurs que la mise en conformité des règles de cybersécurité du secret est un nouveau défi de la communauté du renseignement en termes de recrutement et d'investissement. En effet, la DPR constate notamment que des efforts conséquents sont à mener par les services spécialisés, le GIC, le CNRLT ou la CNCTR pour disposer des personnels compétents en cyberdéfense et en cybersécurité. A ce titre, la fidélisation des personnels de haut niveau apparaît notamment essentielle pour la cyberprotection du renseignement mais nécessite, tout de même, d'adapter la gestion des ressources humaines de la communauté du renseignement pour concurrencer les offres plus lucratives du secteur privé¹.

En outre, la *Stratégie nationale du renseignement* de juillet 2019 souligne l'importance d'une « *culture de l'innovation en lien avec la Recherche et l'industrie* » et du partage des informations dans la communauté du renseignement², ce qui peut entrer en contradiction avec les restrictions qu'impose le secret de la défense nationale. Ayant pu être perçu comme une procédure rigide d'échanges de données sensibles du ministère de la défense pour lutter contre les vulnérabilités³ ou présenté comme une limite à l'ouverture des données de sécurité et de défense⁴, il est vrai que la cyberprotection du secret de la défense nationale pose des interdictions de nature à faire obstacle à l'automatisation des échanges d'informations (accès à distance ou interconnexions par exemple).

¹ A ce sujet, voir notamment C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 272 et suivantes ; B. Lachaud et A. Valetta-Ardisson, *Rapport d'information sur la cyberdéfense*, op. cit., p. 109 à 111.

² Cf. *Stratégie nationale du renseignement* de juillet 2019, p. 11.

³ En ce sens, voir, A. Cammilleri Subrenat, « *Téléservices et confidentialités en matière de défense* », *Revue française d'administration publique*, vol. 146, no. 2, 2013, pp. 325-337.

⁴ En ce sens, voir B. Warusfel, « *Enjeux et limites de l'ouverture des données en matière de sécurité et de défense* », op. cit.

La protection du secret peut aller à l'encontre de la culture de l'innovation numérique qui est fondée sur le risque et la rapidité de mise en œuvre des solutions innovantes¹. Toutefois, on relèvera que la réglementation du secret de la défense nationale ne manque pas de prendre en compte les besoins d'échanges avec les acteurs privés et les partenaires étrangers à travers des dispositions spécifiques aux relations contractuelles et aux classifications de l'OTAN et de l'Union européenne².

La conciliation entre la numérisation du renseignement et la sécurité des systèmes d'information classifiés devrait pouvoir trouver ses solutions dans les textes classifiés spécifiques à chacun des services de renseignement et dans la mise en place des AQSSI. Ces derniers se voient confier la responsabilité d'assurer l'adaptation rapide du renseignement numérique aux innovations et aux besoins de partage des données des services, tant sur les aspects juridiques, techniques et opérationnels. Ajoutons que certaines dispositions du droit de la cyberdéfense et du droit du renseignement peuvent indirectement contribuer à la cyberprotection du renseignement et être complémentaires des exigences du secret de la défense nationale.

§2. La contribution indirecte des droits de la cyberdéfense et du renseignement

Initialement édictées pour encadrer les moyens numériques de cyberdéfense ou de renseignement, des règles du droit de la cyberdéfense relatives à la mise en œuvre de la lutte informatique défensive ainsi que des règles du droit du renseignement relatives à la sécurité des données personnelles traitées par les services de renseignement peuvent contribuer à la cyberprotection du renseignement. En outre, différents mécanismes de contrôle du renseignement numérique peuvent jouer un rôle dans cette cyberprotection.

¹ A ce sujet, voir par exemple C. Perrin et J. -N. Guérini, *Rapport d'information sur l'innovation et la défense*, Sénat, 10 juillet 2019, p. 7

² En ce sens, voir SGDSN, *Rapport d'activité 2019-2020*, p. 19

A – Le recours au droit de la cyberdéfense

En réponse à une cybermenace ciblant leurs systèmes numériques, les services de renseignement sont en droit d'invoquer les mesures techniques de lutte informatique défensive prévues par le code de la défense¹. A ce titre, le rapport de la DPR 2019-2020 nous révèle que pour la DGSE « *des outils ont été développés en interne pour détecter l'extraction massive de données. Par ailleurs, l'ANSSI participe à la sécurité des systèmes d'information de la DGSE grâce à la mise à disposition, depuis l'été 2019, de sondes sur les accès extérieurs du réseau. L'exploitation et le traitement des alertes restent toutefois de la compétence du service* »². La DPR recommande d'ailleurs de reproduire ce dispositif pour la DRM avec le soutien du COMCYBER³.

On ajoutera que les obligations de cyberdéfense pouvant être imposées par le Premier ministre aux administrations, aux opérateurs d'importance vitale (OIV) ou aux opérateurs de services essentiels (OSE) pour assurer la sécurité de leurs systèmes numériques⁴ pourraient servir à renforcer la cyberprotection du renseignement dans ses relations avec d'autres administrations ou avec les industriels de la défense.

B - La sécurité des données personnelles traitées par les services de renseignement

Le droit du renseignement impose aux services de renseignement d'adopter des mesures techniques de sécurité adaptées à la protection des données personnelles qu'ils sont amenés à traiter⁵, ce qui n'est pas sans rappeler l'article 32 du RGPD qui impose une obligation générale de sécurité des traitements de données personnelles et qui laisse penser que la protection des données personnelles contribue à la cybersécurité⁶.

¹ Articles L. 2321-2 à L. 2321-3 du code de la défense.

² En ce sens, voir C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 176.

³ Ibid, p. 178.

⁴ Articles L. 1332-6-1 à L. 1332-6-6 du code de la défense.

⁵ En ce sens, voir E. Petit-Prévost-Weygand, *L'activité extraterritoriale des services de renseignement numérique : recherche de solutions technico-juridiques de protection des données*, op. cit..

⁶ Sur ce point, voir A. Jomni, *Le RGPD : un atout ou un frein pour la cybersécurité ?*, Dalloz IP/IT, 2019, p. 352.

On mentionnera quatre types de mesures prévues par le droit du renseignement portant sur la sécurité des données personnelles collectées :

- les restrictions relatives aux différents accès aux données pour les agents ou aux interconnexions entre les différents fichiers qui sont prévues par les textes réglementaires relatifs aux fichiers de renseignement mais aussi en matière de techniques de renseignement pour les renseignements collectés¹ ;
- l'organisation de la traçabilité et de la centralisation des renseignements collectés avec notamment la mise en place de systèmes d'information et de réseaux solides et sécurisés² ;
- les exigences techniques d'anonymisation ou de pseudonymisation dans le cadre de la technique algorithmique de renseignement³ et des données conservées à des fins de recherche et développement en matière d'intelligence artificielle⁴ ;
- le recours au chiffrement des communications et des données des individus dans le cadre de la surveillance des communications satellitaires⁵.

C – La cyberprotection du renseignement dans les contrôles du renseignement numérique

On rappellera que la Commission nationale de contrôle des techniques de renseignement (CNCTR) veille à ce que la centralisation des renseignements collectés soit assurée par des systèmes numériques solides et sécurisés et à ce que les services de renseignement respectent les mesures relatives aux techniques de renseignement prévues par le code de la sécurité intérieure que nous avons précédemment citées.

¹ Voir nos développements sur la limitation du nombre d'agents susceptibles d'accéder aux données collectées par les techniques de renseignement dans les garanties portant sur les renseignements collectés dans la Section I du Chapitre I du Titre II de la Première partie.

² Voir nos développements sur la centralisation et la traçabilité des renseignements collectés dans les garanties portant sur les renseignements collectés dans la Section I du Chapitre I du Titre II de la Première partie.

³ Article L. 851-3 du code de la sécurité intérieure.

⁴ Article L. 822-2-III du code de la sécurité intérieure.

⁵ Article L. 852-3-III du code de la sécurité intérieure.

Dans le contrôle interne des services de renseignement, le rapport de la DPR 2019-2020 nous rappelle que le contrôle de la cybersécurité relève des dispositions relatives au secret de la défense nationale¹. Au niveau interministériel, l'Inspection des services de renseignement (ISR) peut être amenée à réaliser des « *missions de contrôle, d'audit, d'étude, de conseil et d'évaluation* » qui pourraient concerner la sécurité des systèmes numériques utilisés par les services².

S'agissant du Groupement interministériel de contrôle (GIC), le service du Premier ministre assure particulièrement le développement et la sécurité quotidienne des systèmes numériques impliqués dans les techniques de renseignement dans le respect des conditions fixées par la CNCTR et sous son contrôle³. On notera que, selon le Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), les compétences recherchées par le GIC « *relèvent principalement du domaine de l'informatique, des réseaux, des télécoms et de la cybersécurité* »⁴. Enfin, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est susceptible d'intervenir auprès du GIC et, plus globalement, de la communauté du renseignement dans les contrôles de sécurité informatique en plus de son contrôle prévu par le « régime d'autorisation 226-3 » sur les appareils et dispositifs techniques de surveillance⁵.

A la suite des exigences du secret de la défense nationale qui se complètent avec la contribution indirecte des droits de la cyberdéfense et du renseignement, on prolongera notre étude sur la cyberprotection du renseignement en soulevant la problématique de la maîtrise des technologies et services numériques nécessaires à la numérisation du renseignement qui peuvent être proposés et fournies par des industriels.

¹ Cf. C. Cambon, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020, op. cit., p. 174 à 180.

² Décret n° 2014-833 du 24 juillet 2014.

³ Sur le contrôle du GIC sur les systèmes numériques, voir dans la Première partie les paragraphes dédiés aux garanties portant sur les renseignements collectés (Section I du Chapitre I du Titre II) et au rôle technico-juridique du service du Premier ministre (Section I du Chapitre II du Titre II).

⁴ Cf. SGDSN, *Rapport d'activité 2021*, p. 38 et 39.

⁵ Sur le « régime d'autorisation 226-3 », voir le Chapitre II du Titre I de la Seconde partie.

§3. La maîtrise des technologies et services numériques nécessaires à la numérisation du renseignement

La *Revue stratégique de cyberdéfense* française de 2018 identifie certaines technologies et services numériques comme essentiels pour la France. Il s'agit alors du chiffrement des communications, des systèmes de détection des cyberattaques, des radios mobiles professionnelles ou encore de l'informatique en nuage (« *cloud* » anglais) pour le stockage des données qui se combine avec le développement de solutions innovantes de Big data et d'intelligence artificielle¹. Le rapport d'information du 29 juin 2021 des députés Jean-Luc Warsmann et Philippe Latombe sur la souveraineté numérique mentionne également d'autres technologies telles que la « *blockchain* », l'informatique quantique et les satellites².

Ces technologies et services numériques sont particulièrement sensibles pour les administrations de l'Etat³, d'autant plus pour les besoins de la sécurité nationale et des services de renseignement. Leur acquisition constitue un problème de cyberprotection pour les services de renseignement dans un écosystème numérique international dominé et influencé par les entreprises américaines (GAFAM) ou chinoises (BATX) et dans lequel il est difficile de maîtriser la circulation des données. Cependant, on observera que des solutions sont mises en œuvre pour garantir la confiance des services de renseignement dans l'écosystème numérique.

¹ Cf. *Revue stratégique de cyberdéfense* française de 2018, p. 93 à 100.

² Cf. J. -L. Warsmann et P. Latombe, *Rapport d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »*, op. cit., p. 144 et suivantes.

³ En ce sens, voir H. Oberdorff, *La transformation numérique de l'administration publique*, RDP, septembre 2020, p. 1173.

A – Un écosystème numérique problématique pour la cyberprotection du renseignement

Le recours à des industriels du numérique apparaît comme une nécessité pour les services de renseignement mais il s'agit d'un véritable enjeu de souveraineté numérique.

1. Le recours aux industriels du numérique

La course technologique à laquelle se livre les Etats et le secteur privé oblige le renseignement français à recourir à des industriels du numérique pour maintenir un haut niveau de technicité et « *conserver un niveau d'efficacité comparable aux autres services partenaires* » britanniques ou américains comme le souligne la DPR dans son rapport 2019-2020¹. Ce même rapport nous confirme l'existence d'initiatives visant à rapprocher les services de renseignement et certains industriels français des technologies pour fournir des solutions numériques de confiance en matière de traitement des données ou de cybersécurité² :

- l'initiative « Data Intelligence » qui regroupe 22 sociétés françaises dont Atos, Airbus Defence & Space et Thalès pour proposer une solution de Big data adaptée aux services de renseignement, notamment pour la DGSi. On citera le rapport de la DPR qui nous informe que « *la DRSD a signé un marché pour son système d'information SIRCID [système d'information du renseignement de contre-ingérence de la défense] avec Airbus Defence & Space* » ;
- l'initiative « Artemis » de la DGA qui implique Atos-Bull, Capgemini et le groupement Thalès-Sopra-Stéria pour faire émerger des solutions d'intelligence artificielle spécifiques à la défense ;
- l'initiative « Intelligence Campus » de la DRM qui concerne notamment des solutions civiles innovantes de renseignement d'origine sources ouvertes pouvant être utiles au renseignement³ ;

¹ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 278 à 284.

² Ibid, p. 279.

³ Voir notamment A. Léger et N. Fiocre, *L'intelligence campus, nouveau vecteur du renseignement militaire*, Portail de l'IE, 26 février 2019.

- l'initiative « Campus Cyber » de l'ANSSI qui rassemble les acteurs de la cybersécurité pour partager leur savoir-faire, notamment avec les acteurs de la cyberdéfense dont les services de renseignement¹.

Par ailleurs, le rapport d'activité 2023 de la CNCTR révèle que les services de renseignement recourent aux logiciels de l'entreprise française Systran², spécialisée dans le traitement automatique du langage, et aux logiciels de la société française spécialisée en géo-intelligence, Preligens³, qui « assurent le traitement et l'exploitation automatisés de grandes masses de données, en particulier satellitaires, au profit du renseignement interarmées français »⁴.

On remarquera que ces initiatives concernent des entreprises essentiellement françaises, ce qui s'explique par le souci de s'affranchir des offres étrangères et notamment américaines. En effet, on rappellera que la DGSI avait eu recours à l'offre de la société américaine Palantir pour pouvoir traiter efficacement ses données⁵, ce qui peut poser un problème pour la cyberprotection du renseignement. Cette préoccupation est un enjeu de souveraineté numérique.

2. Un enjeu de souveraineté numérique

Dans un contexte d'augmentation continue des cyberattaques et des risques de perte de contrôle des données ou d'application extraterritoriale de lois sur les réquisitions de données comme le CLOUD Act américain⁶, la cybersécurité est devenue un enjeu de la souveraineté numérique⁷.

la notion difficile à délimiter de « souveraineté numérique » a émergé pour signifier la reprise en main de la numérisation par les Etats sur le plan juridique,

¹ Voir le site internet dédié : [Construisons ensemble une société numérique de confiance. \(campuscyber.fr\)](https://campuscyber.fr).

² Voir le site internet dédié à la société Systran : [Traduire gratuitement vos textes \(systransoft.com\)](https://systransoft.com).

³ Voir le site internet dédié à la société Preligens : [Preligens | Pioneering AI for a safer world \(preligens.com\)](https://preligens.com).

⁴ Cf. CNCTR, 8^{ème} rapport d'activité (2023), p. 144.

⁵ Sur ce point, voir J. Saint-Jalm, J. Freani et N. Fiocre, *L'initiative française « Data Intelligence » : la stratégie du cluster pour s'affranchir de Palantir*, Club Cyber de l'AEGE, Portail de l'IE, 26 octobre 2018.

⁶ Voir notamment D. Frederick T et C. Gunka. « Perquisitionner les nuages - CLOUD Act, souveraineté européenne et accès à la preuve dans l'espace pénal numérique », *Revue critique de droit international privé*, vol. 1, no. 1, 2021, pp. 43-66.

⁷ En ce sens, voir M. Watin-Augouard, *La cybersécurité, enjeu de la souveraineté à l'ère numérique*, Dalloz IP/IT, 2021, p. 130.

politique, économique ou culturelle¹. Au sens de la *Revue stratégique de cyberdéfense* française de 2018 :

« La souveraineté numérique peut être entendue comme la capacité de la France d'une part, d'agir de manière souveraine dans l'espace numérique, en y conservant une capacité autonome d'appréciation, de décision et d'action et d'autre part, de préserver les composantes les plus traditionnelles de sa souveraineté vis-à-vis de menaces nouvelles tirant partie de la numérisation croissante de la société ».

La loi « 5G » ou « anti-Huawei » visant à préserver les intérêts de la défense et de la sécurité nationale dans le cadre de l'exploitation des réseaux radioélectrique mobiles² ou encore le renforcement de l'application de la loi dite « blocage » de 1968 pour contrer notamment les lois à portée extraterritoriale applicables au cloud³, s'inscrivent dans cet objectif de souveraineté numérique.

Toutefois, l'industrie numérique en France doit non seulement prendre en considération l'application de législations extraterritoriales sur l'écosystème numérique mais aussi la concurrence du droit européen qui tend à devenir le cadre juridique de référence de l'économie numérique et de la cybersécurité⁴. A ce titre,

¹ Pour une compréhension récente de la notion de souveraineté numérique, voir notamment A. -T. Norodom, *Souveraineté, cybersécurité et Union européenne*, " In *L'Europe de La Cybersécurité, Pour Une Liberté Sécurisée*, TransEuropeExperts pour le FIC 2020, p. 32 et 33 et, dans le même ouvrage, l'article de A. Desforges, *Souveraineté numérique et autonomie stratégique : la nécessaire clarification pour une ambition européenne*, p. 34 et 35. Voir également J. -L. Warasmann et P. Latombe, *Rapport d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »*, Tome I, Assemblée nationale, 29 juin 2021, p. 17 à 31 ou encore P. Türk, *Définition et enjeux de la souveraineté numérique*, Parole d'expert, Vie publique, 14 septembre 2020.

² La loi n° 2019-810 du 1er août 2019, dont les dispositions législatives et réglementaires ont été jugées conformes à la Constitution et à la liberté d'entreprendre et au droit de propriété par les décisions du Conseil constitutionnel n° 2020-882 QPC du 5 février 2021, *Société Bouygues télécom et autre* et du Conseil d'Etat, 8 avril 2021, *Société Bouygues télécom et SFR*, organise une procédure d'autorisation préalable pour l'exploitation des équipements de réseaux 5G justifiée par les besoins de la sécurité nationale.

³ La loi n° 68-678 du 26 juillet 1968 « *interdit à toute personne physique de nationalité française ou résidant habituellement sur le territoire français et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement de communiquer par écrit, oralement ou sous toute autre forme, en quelque lieu que ce soit, à des autorités publiques étrangères, les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin* » (article 1). Le décret n° 2022-207 du 18 février 2022 et l'arrêté n° 2022-207 du 18 février 2022 sont venus clarifier la procédure d'alerte qu'implique la loi de 1968 et renforcer la sécurité juridique des entreprises par un accompagnement sur la situation de leur patrimoine informationnel.

⁴ En ce sens, voir notamment P. Türk, *La conservation des données, quels enjeux pour la souveraineté numérique ?*, op. cit. ; P. Achilleas, *La sécurité des réseaux 5G : un enjeu de souveraineté pour l'Europe et la France*, Communication Commerce électronique n° 12, Décembre 2020, étude 21 ; A. Tricaud,

l'harmonisation européenne des réglementations sur les industriels du numérique de confiance devraient donc aboutir à prendre en considération la nationalité française ou européenne de l'industriel, y compris pour les besoins de défense et de sécurité nationale, pour acquérir les meilleures innovations. On notera que la *Revue stratégique de cyberdéfense* de 2018 tient compte d'une souveraineté numérique à l'échelle européenne dans les critères d'offres pour les besoins de sécurité et de souveraineté tout en ajoutant que le critère de la nationalité n'est « pas toujours opposable, ni pertinent ».

Dans sa conception politique, économique et technologique, la souveraineté numérique nationale ou européenne demeure, en effet, en construction. La France et l'Europe sont encore fortement dépendantes des acteurs américains qui conservent l'avantage technologique pour répondre à des labellisations de haut niveau et à des appels d'offres exigeants¹.

Dans ce contexte, la DPR souligne dans son rapport 2019-2020 la nécessité de faire émerger « une filière industrielle souveraine » qui contribuerait à la cybersécurité du renseignement dans ses relations avec les entreprises du numérique². Afin de répondre à cet objectif, un certain nombre de règles visant à garantir la maîtrise des technologies et services numériques ont été édictées. Ces solutions contribuent à établir une confiance dans l'écosystème numérique pour les besoins sensibles de l'Etat, notamment pour les services de renseignement.

B – Les solutions de confiance dans l'écosystème numérique

On distinguera, d'une part, les solutions envisagées par l'Etat pour les besoins de ses administrations sensibles comme celles du renseignement et, d'autre part, celles qui concernent les industriels pouvant répondre aux besoins des services de renseignement.

« Vers une co-souveraineté nationale et européenne en matière de cybersécurité », *Revue Défense Nationale*, vol. 855, no. 10, 2022, pp. 22-28.

¹ En ce sens, voir J. -L. Warasman et P. Latombe, *Rapport d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »*, op. cit., p. 31 et suivantes ; P. Achilleas, *La sécurité des réseaux 5G : un enjeu de souveraineté pour l'Europe et la France*, op. cit. ; A. Fitzjean Ó Cobhthaigh, *Le cloud et la souveraineté numérique dans le nouveau monde*, *Revue pratique de la prospective et de l'innovation* n° 1, Avril 2021, dossier 2.

² Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 278 à 280.

1. Les règles internes à l'administration de l'Etat

De manière générale, la circulaire du Premier ministre n°5725/SG du 17 juillet 2014 consacrant la politique de sécurité des systèmes d'information de l'État (PSSIE) précise que « *en préambule, sont énoncés des principes de sécurité incontournables, notamment l'obligation d'acquérir des produits et des services de sécurité labellisés par l'ANSSI et l'hébergement des données sensibles sur le territoire national* » et que « *il appartient aux responsables des entités concernées d'assurer une cohérence entre les dispositions de la présente PSSIE et la réglementation relative à la protection des informations classifiées de défense* ».

Pour ce qui concerne l'hébergement des données sur le territoire national, le droit européen s'oppose en principe à des exigences de localisation des données, « *sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité* »¹. Dans ces conditions, la France s'est dotée d'une doctrine d'utilisation de l'informatique en nuage par l'Etat² avec le développement d'un « cloud souverain » divisé en trois niveaux selon la sensibilité des données : le cloud interne de l'Etat pour les données classifiées ; le cloud personnalisé fourni par un prestataire ; le cloud externe³. Il convient d'ajouter que le ministère des Armées dispose également de son propre cloud interne⁴. Selon cette doctrine, la communauté du renseignement est amenée à devoir recourir à l'offre de cloud interne pour ses besoins.

Sinon, aucune réglementation ne s'oppose de manière absolue au recours à des offres externes de prestations ou de produits numériques pour des besoins de sécurité et de souveraineté, y compris en matière de sécurité nationale.

¹ Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (article 4).

² Sur la doctrine d'utilisation de l'informatique en nuage par l'Etat, voir F. Montaugé et G. Longuet, *Rapport de la commission d'enquête sur la souveraineté numérique*, Tome 1, Sénat, 1^{er} octobre 2019, p. 116 et 144 ainsi que P. Türk, *La conservation des données, quels enjeux pour la souveraineté numérique ?*, La Semaine Juridique Administrations et Collectivités territoriales n° 50, 19 décembre 2022, 2348 ou encore B. Clotilde, « *Maîtriser le cloud computing pour assurer sa souveraineté* », Stéphane Taillat éd., La Cyberdéfense. Politique de l'espace numérique. op. cit., pp. 91-97.

³ Circulaire n° 6049-SG du 8 novembre 2018.

⁴ Circulaire n° 6282-SG du 5 juillet 2021.

2. Les règles applicables aux industriels

La *Revue stratégique de cyberdéfense* de 2018 exige d'apprécier cinq critères pour qualifier une offre industrielle qui devrait correspondre aux attentes des besoins sensibles de l'Etat et donc du renseignement : une entreprise maîtrisant ses développements et processus industriels ; le degré de transparence sur la fabrication des produits ; l'autonomie de décision de l'entreprise ; l'acceptation de contrôles par la puissance publique ; le respect des exigences de la protection du secret¹.

Plus concrètement, le recours à des solutions numériques externes dans le domaine de la défense et de la sécurité nationale nécessite de recourir à des produits de sécurité et prestataires de confiance qualifiés par l'ANSSI. Pour les industriels du secteur de la défense, la loi de programmation militaire du 18 décembre 2013 a créé une obligation pour les OIV de recourir tout particulièrement à des services qualifiés de cyberdéfense². Pour répondre à ces obligations, le décret n° 2015-350 du 27 mars 2015 instaure une procédure de qualification des solutions³. Cette qualification est un processus qui atteste la conformité des solutions aux « *exigences réglementaires, techniques et de sécurité promues par l'ANSSI* » et qui permet l'obtention d'un « visa de sécurité ANSSI »⁴. L'Agence peut contrôler à tout moment le respect des exigences de la qualification et dispose d'un pouvoir de sanction lui permettant de suspendre ou d'abroger la qualification⁵.

¹ Cf. *Revue stratégique de cyberdéfense* de 2018, p. 94 à 96.

² Articles L. 1332-6-1 et L. 1332-6-3 du code de la défense.

³ Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes.

⁴ Voir la brochure dédiée de l'ANSSI disponible sur son site internet (<https://www.ssi.gouv.fr/administration/qualifications/>).

⁵ Articles 7 et 15 du décret n° 2015-350 du 27 mars 2015.

Produits de sécurité et services de confiance qualifiés

▶ QUELS TYPES DE PRODUITS OU SERVICES SONT ÉLIGIBLES À LA QUALIFICATION ?

TOUS LES PRODUITS OU SERVICES DE CYBERSÉCURITÉ, EN PARTICULIER CEUX QUI RÉPONDENT EN PRIORITÉ AUX BESOINS DE L'ADMINISTRATION ET DES OPÉRATEURS D'IMPORTANCE VITALE (OIV), SONT CONCERNÉS PAR LA QUALIFICATION.

CATÉGORIE DE PRODUITS	FONCTIONS DE SÉCURITÉ
CHIFFREMENT RÉSEAU	Solutions offrant des fonctions de chiffrement des flux de communication.
INFRASTRUCTURES DE GESTION DE CLÉS (IGC) CARTES À PUCE	Solutions implémentant des fonctions de gestion des clés cryptographiques telles que les cartes à puce, les modules cryptographiques, les jetons d'authentification.
SIGNATURE ET GESTION DE LA PREUVE	Solutions de création et de validation de signatures électroniques, de gestion de la preuve électronique (conservation et horodatage des documents).
TITRE D'IDENTITÉ ÉLECTRONIQUE	Solutions sécurisées pour la gestion des titres d'identité (passeport, carte agent, etc.).
STOCKAGE SÉCURISÉ EN NUAGE	Solutions de sécurisation des données utilisateurs stockées, gérées ou manipulées chez des hébergeurs via des offres IaaS, PaaS, SaaS.
MOBILITÉ	Solutions offrant des services sécurisés en mobilité (ex. terminaux nomades, solutions de voix sécurisées, etc.).
PROTECTION DES SYSTÈMES INDUSTRIELS	Solutions de sécurisation des systèmes industriels.
PROTECTION DU POSTE DE TRAVAIL	Solutions de protection des données utilisateurs stockées localement sur un poste de travail.
PROTECTION RÉSEAUX ET TÉLÉCOMS	Solutions de filtrage web, pare-feu, dispositif de détection d'intrusion ou sondes.
PROTECTION SYSTÈMES	Solutions de gestion des droits d'accès aux réseaux ou de gestion de parcs.

LES SERVICES ÉLIGIBLES À LA QUALIFICATION DOIVENT CORRESPONDRE AUX FAMILLES IDENTIFIÉES POUR RÉPONDRE AUX BESOINS RÉGLEMENTAIRES :

■ Les prestataires de services de cyberdéfense :

- prestataires d'audit de la sécurité des systèmes d'information (PASSI),
- prestataires de détection des incidents de sécurité (PDIS),
- prestataires de réponse aux incidents de sécurité (PRIS).

■ Les prestataires de services d'informatique en nuage (SecNumCloud).

■ Les prestataires de services relatifs à la confiance numériques :

- prestataires de certification électronique (PSCE),
- prestataires de service d'horodatage électronique (PSHE),
- prestataires de service de validation de signatures et cachets électroniques,
- prestataires de service de conservation de signatures et cachets électroniques,
- prestataires de service d'envoi recommandé électronique.

Source : Brochure de l'ANSSI sur la qualification et les visas de sécurité (pages 6 et 7)

Suivant les innovations des produits et services numériques, il faut s'attendre à ce que d'autres qualifications soient élaborées par l'ANSSI. Néanmoins, les qualifications existantes, notamment le « cloud de confiance », interrogent sur leur adéquation réelle à des besoins souverains sensibles comme ceux du renseignement¹, même si l'article 10 du décret n° 2015-350 du 27 mars 2015 prévoit que les référentiels de l'ANSSI fixant les règles d'évaluation des prestataires peuvent imposer le respect des exigences du secret de la défense nationale et que l'article 18 s'oppose à ce qu'un centre d'évaluation soit agréé pour les besoins de la sécurité nationale s'il n'est pas en mesure de respecter ces mêmes exigences.

Par ailleurs, on soulignera que le recours à des produits de sécurité et prestataires de services de confiance numérique pour les besoins de la sécurité nationale relève des marchés publics de défense ou de sécurité qui dérogent largement au droit de la commande publique français et européen². Dans le cadre

¹ En ce sens, voir L. Dominique, « *Cloud souverain : souveraineté et résilience, ou confiance ?* », Revue Défense Nationale, vol. 855, no. 10, 2022, pp. 14-21.

² Articles R. 2311-1 à R. 2313-3 du code de la commande publique.

de la passation de ces contrats administratifs spéciaux, les services de l'Etat sont en droit d'exiger aux prestataires qualifiés le respect de règles plus sévères que les référentiels de l'ANSSI¹.

S'agissant d'une externalisation impliquant des entreprises étrangères lorsque les industriels français ne sont pas en mesure de satisfaire les besoins sensibles des services de l'Etat, une approche pragmatique ou réaliste pourrait être envisagée en acceptant l'idée d'une « souveraineté numérique partagée »². En droit, la réalisation de cette approche exige deux conditions cumulatives en matière de localisation des données : l'obligation de localisation des données sur le territoire national et l'obligation de « localisation légale »³, c'est-à-dire de soumettre les données exclusivement au droit français et européen. On retrouve, ici, le devoir de mise en cohérence de la PSSIE avec la réglementation sur le secret de la défense nationale qui constitue la norme dans les services sensibles de l'Etat mais qui peut s'avérer trop contraignante pour les entreprises du numérique. En outre, l'approche d'une « souveraineté numérique partagée » nécessite de recourir à des solutions technologiques étrangères partageant les mêmes valeurs dans la régulation des activités numériques que celles de la France⁴.

On élargira ainsi la recommandation du rapport de la DPR de 2020 sur l'association des services « *au travail prospectif d'élaboration d'une nouvelle stratégie industrielle de souveraineté en cybersécurité* »⁵ à l'ensemble des problématiques de souveraineté numérique, notamment sur les leviers juridiques français et européens qui pourraient s'appliquer à des besoins de sécurité nationale.

On ne manquera pas d'évoquer la conception « libérale » de la souveraineté numérique qui veut promouvoir l'autonomie des citoyens dans le cyberspace,

¹ Articles R. 2311-1 à R. 2313-3 du code de la commande publique.

² En ce sens, voir G. -H. Bricet, « *Les technologies de renseignement en France : à la recherche d'un modèle de développement* », op. cit..

³ Voir A. Cattaruzza, « *Chapitre 4. Les enjeux de souveraineté de l'espace numérique. Quelle souveraineté pour l'espace numérique ?* », Stéphane Taillat éd., La Cyberdéfense. Politique de l'espace numérique. op. cit., pp. 83-91.

⁴ En ce sens, voir les réflexions sur la souveraineté numérique dans l'ouvrage C. Castets-Renard, V. Ndior et L. Rass-Masson, *Enjeux Internationaux Des Activités Numériques*, Bruxelles, Larcier, 2020.

⁵ Cf. C. Cambon, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, op. cit., p. 280.

notamment par le respect de leurs droits et libertés ainsi que leur capacité à choisir librement leurs services numériques. Cette conception participe pleinement à la confiance dans l'économie numérique et nécessite le respect de certaines exigences de la cybersécurité de la société.

SECTION II : Le respect d'exigences de la cybersécurité de la société

En affirmant que l'Etat est « garant de la cybersécurité de la société »¹, la *Revue stratégique de cyberdéfense* de 2018 nous invite à soutenir que les pouvoirs publics doivent privilégier une réglementation protectrice des individus et de la société sur certains enjeux de sécurité numérique, même si elle peut apparaître défavorable pour le renseignement. Il en va ainsi notamment de la cryptologie et de son contrôle par les pouvoirs publics qui ne cesse d'être débattu (§1.) et de la « course aux vulnérabilités » des systèmes numériques entre l'Etat, la société civile et les cybercriminels dont les conséquences sont susceptibles d'être dramatiques pour la protection du cyberspace et la confiance dans l'économie numérique (§2.).

§1. L'éternel débat sur l'encadrement de la cryptologie

« Science du secret », la cryptologie a pour objet premier la confidentialité de l'information par la création de codes par des procédés cryptographiques dont leur robustesse et leur déchiffrement sont étudiés par la cryptanalyse². Depuis l'Antiquité, des linguistes, mathématiciens, physiciens mais aussi des militaires, diplomates, espions, criminels, commerçants ou simples citoyens pratiquent l'art du chiffrement et prennent part à la lutte qui oppose ceux qui chiffrent à ceux qui déchiffrent³.

La cryptologie contribue directement aux progrès techniques de l'informatique au XXème siècle, notamment à la suite des travaux du mathématicien Alan Turing sur le déchiffrement du système cryptographique

¹ Revue stratégique de cyberdéfense de 2018, p. 93.

² Sur la définition de la cryptologie, voir J. Stern, *La Science du secret*, Odile Jacob, 1998 ; P. Guillot, *La cryptologie, l'art des codes secrets*, EDP Sciences, 2013.

³ Sur l'histoire de la cryptologie, voir S. Signh, *Histoire de codes secrets*, Lattès, 1999.

« Enigma »¹ utilisé par l'armée allemande durant la Seconde Guerre mondiale, et constitue une véritable branche à part entière de l'informatique qui s'inscrit « au cœur du numérique » avec les développements d'Internet². En particulier, le chiffrement des communications et des données numériques est devenu une condition technique de la confiance dans l'économie numérique puisqu'il permet non seulement d'assurer la confidentialité des informations mais également de contrôler leur authentification et leur intégrité³.

Sur la plan politique et juridique, les Etats, encouragés par leurs services de sécurité et de renseignement, ont rapidement cherché à encadrer et contrôler les développements et l'usage de la cryptologie dans la société afin notamment d'éviter sa démocratisation qui est perçue comme un risque pour la défense et la sécurité nationale, ce qui aboutira à une controverse avec la mouvance « *Cypherpunk* » et les défenseurs des libertés sur internet qui luttent contre la surveillance de masse et les secrets d'Etat ainsi qu'avec les entreprises du numérique favorables à la généralisation du chiffrement dans leurs solutions commerciales⁴.

Dans un contexte de transformation numérique croissante des sociétés, la perte du contrôle des Etats sur les moyens de cryptologie est apparue inévitable malgré les difficultés qu'elle entraîne pour les services de sécurité et de renseignement dans leurs activités. Plus encore, la liberté de chiffrement devient une nécessité, voir même l'une des « clés », pour garantir le respect des libertés et droits fondamentaux dans les sociétés numérisées et la cybersécurité de ces dernières.

¹ Cf. C. Tibère, « *Enigma* », Dictionnaire du renseignement, op. cit., p. 335 à 341.

² Cf. J. Stern, *La cryptologie au cœur du numérique*, Les Grandes Voix de la Recherche, CNRS éditions, 2021.

³ En ce sens, voir J. Dionis du Séjour, *Rapport sur le projet de loi (n° 528) pour la confiance dans l'économie numérique*, 1^{ère} partie, Assemblée nationale, 12 février 2003, p. 59 à 61.

⁴ A ce sujet, voir F. Tréguer, *De la dépêche secrète aux Crypto Wars (brève histoire politique du chiffrement)*, 2017, halshs-01649969.

A – La perte du contrôle des Etats sur la cryptologie

Le choix d'une libéralisation du chiffrement s'est imposé face à l'incapacité des Etats à pouvoir maintenir un contrôle plein et entier sur les évolutions de la cryptologie. Cette perte de contrôle a suscité des réactions favorables au rétablissement d'un encadrement plus restrictif du chiffrement face à la montée du terrorisme sans néanmoins présenter des arguments suffisamment convaincants.

1. L'apanage impossible des pouvoirs publics sur la cryptologie

Il ne fait aucun doute que les moyens de cryptologie, dont l'élaboration et les usages se sont d'abord répandus dans les domaines militaires et diplomatiques, constituent une préoccupation majeure des Etats dans la protection des informations sensibles¹ et occupent aujourd'hui une place déterminante dans leur recherche de souveraineté numérique². Plus particulièrement pour les services de sécurité et de renseignement, l'apanage de l'Etat sur la cryptologie constituerait un double avantage : garantir aux mieux le secret de leurs activités et, surtout, s'assurer de ne pas être mis en difficulté dans leurs enquêtes et opérations de surveillance ou militaires. En France, on ne manquera pas de rappeler, ici, que l'ANSSI est l'héritière directe de la Direction technique des chiffres (DTC) créée en 1943 à Alger et indirecte de la section du Chiffre militaire qui, durant la Grande Guerre, a démontré l'importance du contrôle de l'Etat sur les moyens de cryptologie³.

Les pouvoirs publics entretiennent alors une relation de méfiance à l'égard de la cryptologie qui s'est accentuée avec les développements du numérique, d'autant plus en l'absence d'un véritable monopole de l'Etat sur les moyens cryptographiques. En effet, il s'est avéré que les pouvoirs publics n'ont pas réussi à limiter la prolifération du chiffrement dans la société civile malgré leurs efforts politiques, juridiques et techniques.

¹ En France, on ne manquera pas de rappeler, ici, que l'ANSSI est l'héritière directe de la Direction technique des chiffres (DTC) créée en 1943 à Alger et indirecte de la section du Chiffre militaire de la Grande Guerre.

² En ce sens, voir T. Sirvent, *La cryptographie, socle de la souveraineté numérique*, Revue Défense Nationale, vol. 855, no. 10, 2022, pp. 59-66.

³ Cf. A. Couderc, *Renseignement technique et secret militaire : le Chiffre français pendant les premiers mois de la Grande Guerre*, Stratégique, vol. 105, no. 1, 2014, pp. 57-72.

Ainsi, dans le contexte réglementaire libéral des Etats-Unis sur l'usage de la cryptologie, les projets de la NSA visant, en opposition avec sa mission de cybersécurité¹, à affaiblir techniquement le chiffrement des communications et des données numériques, notamment en introduisant des « portes dérobées » dans les matériels et logiciels, se sont heurtés aux défenseurs du droit à la vie privée et de la lutte contre la surveillance de masse dans le cadre des « Crypto Wars »². Alors que la défense du chiffrement s'est initialement organisée dans les années 1990 au sein de la communauté « *Cypherpunk* » ou de la « cyberpiratrie »³, elle a pris une nouvelle dimension à partir de 2013 avec la décision des GAFAM de renforcer la généralisation du chiffrement dans leurs services numériques à la suite des « révélations Snowden » sur le programme de cryptanalyse « *Bullrun* »⁴. La persévérance des autorités américaines à remettre en cause le chiffrement dans la société civile et les réactions des grandes plateformes du numérique conduisent, d'une certaine manière, à entrer dans une logique de « Raison d'Etat vs. Réseaux sociaux » dans laquelle aucun ne semble disposer du monopole légitime de la cryptologie.

De son côté, la France a adopté l'une des positions les plus restrictives d'Europe en matière de contrôle des moyens cryptographiques, de la Seconde Guerre mondiale jusque dans les années 1990, en qualifiant juridiquement ces moyens de matériels de guerre, ce qui impliquait un régime draconien d'autorisation ou de prohibition sur l'usage et le commerce de la cryptologie qui est apparu de plus en plus contradictoire avec le droit au secret des correspondances électroniques et à la protection des données personnelles ainsi qu'avec l'émergence d'un marché européen du numérique⁵. Dans ces conditions, les pouvoirs publics français se sont engagés dans la voie d'une libéralisation du

¹ Sur ce paradoxe, voir C. Delesse, *La NSA, mauvais génie du cybermonde ?*, Sécurité globale, vol. 8, no. 4, 2016, pp. 67-104.

² Cf. C. Jarvis, *Crypto Wars : The fight for privacy in the digital age : a political history of digital encryption*, CRC Press, 2021.

³ A ce sujet, voir F. Douzet, J. -L. Samaan et A. Desforges, *Les pirates du cyberspace*, Hérodote, vol. 134, no. 3, 2009, pp. 176-193.

⁴ Voir notamment N. Rauline, *Bullrun, l'autre programme de la NSA qui ébranle la high-tech*, Les Echos, 6 septembre 2013.

⁵ Sur la réglementation française applicable à la cryptologie jusque dans les années 1990, voir notamment F. Goliard, *Télécommunications et réglementation française du cryptage*, Recueil Dalloz 1998, p. 120.

chiffrement, tout en cherchant à maintenir un certain contrôle sur les moyens cryptographiques sans réellement y parvenir.

2. Le choix de la libéralisation du chiffrement

A la même époque des premières « Crypto Wars » aux Etats-Unis, les pouvoirs publics français entrent dans une période transitoire vers la libéralisation de la cryptologie. Tout d'abord, la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, qui s'intéresse plus aux prestations de cryptologie qu'à son usage, est venue différencier clairement, d'une part, les fonctions d'authentification et d'intégrité des moyens de cryptologie tels que la signature électronique et, d'autre part, celles de confidentialité. Pour les premières, un régime de déclaration préalable est mis en place pour l'utilisation et le commerce alors qu'un régime d'autorisation du Premier ministre, via le Service central pour la sécurité des systèmes d'information (SCSSI), est prévu pour les moyens assurant des fonctions de confidentialité. Si cette évolution tient compte des besoins d'authentification et d'intégrité des informations pour l'économie numérique, le dispositif demeure dissuasif contre l'usage du chiffrement et favorable aux services de renseignement, notamment en n'autorisant que des moyens cryptographiques faibles et donc aisément déchiffrables¹.

Cependant, la montée en puissance de l'Internet et de la piraterie informatique a contraint les pouvoirs publics à renforcer la cybersécurité des entreprises en leur permettant d'accéder à des moyens robustes de chiffrement. Dans une recherche de conciliation entre la sauvegarde de la sécurité nationale et le développement des télécommunications, le législateur français a alors introduit, par l'article 17 de loi n° 96-659 du 26 juillet 1996 modifiant la loi de 1990, un nouveau dispositif consacrant une liberté de chiffrement à des fins de confidentialité dès lors que les conventions secrètes des moyens de cryptologie utilisés font l'objet d'un séquestre auprès d'organismes agréés par le Premier ministre. Précisons que les conventions secrètes sont des « clés non publiées » qui permettent la transformation des informations en données chiffrées ou en claires selon la loi de 1996 et le décret d'application n° 98-102 du 24 février 1998 relatif

¹ En ce sens, voir B. Warusfel, *Dix ans de réglementation de la cryptologie en France : du contrôle étatique à la liberté concédée*, Annuaire français de relations internationales, n° 1, 2000, pp. 657-661 et F. Goliard, *Télécommunications et réglementation française du cryptage*, op. cit..

aux organismes agréés. Cette solution de compromis, qui devait assurer aux services de renseignement et d'enquêtes judiciaires l'efficacité des interceptions autorisées par la loi n° 91-646 du 10 juillet 1991, n'a finalement pas tenu ses promesses en raison de retards administratifs et de l'inadaptation des pouvoirs publics français à faire face à la rapidité des évolutions technologiques et à un marché du numérique libéral et globalisé mais dominé par les américains¹.

Envisagée dès 1999 par le Premier ministre, Lionel Jospin, en invoquant la liberté de communication comme fondement de l'Internet², la libéralisation du chiffrement est véritablement consacrée cinq ans plus tard à l'article 30 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) : « *l'utilisation des moyens de cryptologie est libre* ». Toutefois, ce changement de paradigme n'a pas remis en cause la complexité et la sensibilité de l'encadrement des prestations des moyens de cryptologie qui sont classés « biens à double usage »³. En outre, la LCEN n'a pas eu pour effet immédiat de généraliser le chiffrement, il a fallu attendre que ce dernier devienne un véritable enjeu de la cybersécurité et de la protection des données avec les « révélations Snowden » et l'arrivée du « *cloud computing* »⁴. Ainsi, on assiste à une prolifération croissante de l'utilisation libre du chiffrement depuis 2013 et à des évolutions techniques rapides, parfois aux conséquences difficiles à évaluer pour ce qui concerne la cryptographie post-quantique par exemple⁵, et qui suscitent alors des réactions en faveur d'un retour du contrôle des pouvoirs publics.

¹ Sur les critiques, voir notamment B. Warusfel, *Dix ans de réglementation de la cryptologie en France : du contrôle étatique à la liberté concédée*, op. cit..

² Déclaration de M. Lionel Jospin, Premier ministre, sur la mise en œuvre et les orientations de développement du Programme d'action gouvernementale pour la société de l'information (PAGSI), Hourtin le 26 août 1999.

³ En ce sens, voir E. A. Caprioli, *La nouvelle réglementation sur la cryptologie : un cadre juridique enfin complet*, Communication Commerce électronique n° 10, Octobre 2007, comm. 128.

⁴ A ce sujet, voir B. Warusfel, *La cryptologie au cœur de la cybersécurité : enjeux et choix*, Revue de la Gendarmerie Nationale, 4^{ème} trimestre 2015, p. 107 à 114.

⁵ A ce sujet, voir ANSSI, *Algorithmes de cryptographie post-quantique*, Papiers numériques, Edition 2020, p. 47.

3. Les souhaits peu convaincant d'un rétablissement du contrôle sur le chiffrement

Bien que la loi du 10 juillet 1991 sur les interceptions de sécurité et, par la suite, la loi du 24 juillet 2015 relative au renseignement aient prévu une obligation de remise des conventions secrètes ou de déchiffrement à la charge des prestataires de cryptologie pour les besoins des techniques de renseignement, il semble que l'apparition de la 5G et, plus particulièrement, du chiffrement de bout-en-bout des communications devraient remettre en cause ces réquisitions légales mais aussi les capacités techniques d'interception¹.

Il est vrai que ces difficultés se sont révélées dans le cadre de la lutte contre le terrorisme, ce qui suscite régulièrement des réactions polémiques des pouvoirs publics contre le chiffrement et, notamment, sur la légalisation des « portes dérobées ». Plusieurs responsables politiques se sont ainsi positionnés en ce sens². Dans l'affaire *FBI vs. Apple* de 2016, les autorités américaines avaient également demandé en justice l'autorisation d'introduire une « porte dérobée » dans les iPhones à la suite de l'attentat de San Bernardino³. Ayant réussi à accéder au smartphone de l'auteur présumé de l'attentat sans l'assistance d'Apple, le FBI a donc mis fin à sa demande avant qu'un juge ne se soit prononcé⁴. Une proposition similaire avait été envisagée mais finalement retirée en France dans les discussions de 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 pénale⁵.

On peut comprendre les critiques d'une certaine « privatisation » de la cryptologie au profit d'intérêts commerciaux et la crainte d'une libéralisation sans

¹ A ce sujet, voir Cf. G. Larrivé, *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, op. cit., p. 108 à 112.

² Par exemple, voir dans les médias l'article de A. Griffin, *WhatsApp and iMessage could be banned under new surveillance plans*, The Independent, 12 January 2015 sur la position du Premier ministre britannique, David Cameron, ou encore le Grand entretien de France Inter du ministre de l'Intérieur, Gérard Darmanin, du mercredi 28 avril 2021.

³ Voir à ce sujet M. Isaac, *Explaining Apple's fight with the FBI*, The New York Times, feb. 17, 2016.

⁴ Sur cette affaire, voir D. Yadron, *San Bernardino iPhone : US ends Apple case after accessing data without assistance*, The Guardian, 29 mars 2016.

⁵ Sur ce point, voir C. Féral-Schuhl, *Vers un renforcement de l'obligation de déchiffrement ?* Section 5 - Déchiffrement des moyens de cryptologie (532.81 - 532.84). Chapitre 532 - Régime actuel de la cryptologie. Praxis Cyberdroit, 2020-2021.

limite du chiffrement qui serait principalement favorable aux organisations criminelles¹. Toutefois, ce discours, déjà ancien, ce dirige manifestement dans une impasse au regard d'une liberté de chiffrement robuste considérée désormais comme une nécessité dans les sociétés numérisées².

B – La nécessité d'une liberté de chiffrement robuste dans les sociétés numérisées

Deux arguments nous incitent à considérer que la liberté de chiffrement, notamment le droit à recourir à des moyens robustes de cryptologie, est aujourd'hui indispensable : d'une part, cette liberté constitue une garantie effective des droits et libertés des citoyens dans l'espace numérique et, d'autre part, elle est une composante essentielle d'une sécurité du numérique qui entre en concurrence avec la sécurité nationale.

1. « Permis de chiffrer », une garantie effective des droits et libertés à l'ère du numérique

Comme le rappelle Félix Tréguer, le chiffrement est un outil technique historique et incontournable de l'anonymat et, en ce sens, la liberté de son usage constitue pour les citoyens et la société civile une réelle garantie pour l'exercice effectif de leur droit au respect à la vie privée et de leur liberté d'expression et de communication, d'autant plus depuis que la numérisation des sociétés s'accompagne d'une montée en puissance des capacités de surveillance secrète des Etats dont les potentialités liberticides sont à craindre³.

Ainsi, la libéralisation du chiffrement ne peut pas être réduite à simplement assurer la confiance dans l'économie numérique à des fins d'intérêts commerciaux. Elle constitue un rempart contre les risques d'une surveillance abusive de l'Etat ou contre le traitement inconséquent des données personnelles des individus. Sur ce dernier point, on ne manquera pas de souligner que le RGPD a tenu à citer le

¹ En ce sens, voir B. Hurel et V. Lemonier, *L'enquête pénale à l'épreuve du chiffrement*, Délibérée, vol. 4, no. 2, 2018, pp. 53-57 ou encore la tribune de magistrats dont le procureur de Paris, François Molins, « *When Phone Encryption Blocks Justice* », publiée en 2015 par le « New York Times ».

² En ce sens, voir M. Schulze, *Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016*, Media and Communication, 2017, Volume 5, Issue 1, Pages 54–62.

³ Cf. F. Tréguer, *Anonymat et chiffrement, composantes essentielles de la liberté de communication*, in Quentin Van Enis, Cécile De Terwangne, *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, inPress, 2019.

chiffrement comme l'une des mesures techniques permettant de satisfaire à l'obligation générale de sécurité des responsables de traitement de données personnelles, sans pour autant aller jusqu'à consacrer une obligation de chiffrement¹.

Plus encore pour les défenseurs des libertés, l'importance du chiffrement à l'ère numérique est telle que : d'une part, sa restriction peut se révéler une atteinte au droit au respect de la vie privée et à la liberté d'expression, ce qui implique que l'atteinte à la liberté de chiffrement ne pourrait être justifiée que par la loi et dans le respect des principes de proportionnalité et de nécessité² ; et, d'autre part, il doit être garanti l'accès à un chiffrement numérique robuste à toute personne³.

Pour notre part, nous souscrivons à ces considérations qui s'opposent à toutes mesures d'affaiblissement du chiffrement comme la création de « portes dérobées ». Cette position a été consacrée par la CEDH en février 2024⁴, la Cour considérant que les obligations légales d'installation de « portes dérobées » ou de divulgation de clés de chiffrement pour les messageries cryptées n'apparaissent pas proportionnelles au regard du droit au respect à la vie privée⁵. Ainsi, il est préférable d'accepter la perte du contrôle des pouvoirs publics sur le chiffrement dans un contexte où « *la sécurité du numérique est définitivement l'affaire de tous* », pour reprendre les termes de Guillaume Poupard⁶.

¹ Sur le RGPD et le chiffrement, voir A. Jomni, *Le RGPD : un atout ou un frein pour la cybersécurité ?*, op. cit..

² Voir D. Kaye, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, Conseil des droits de l'homme, 22 mai 2015.

³ En ce sens, voir les propositions de l'Observatoire des libertés et du Numérique, « *Chiffrement, sécurité et libertés* », janvier 2017.

⁴ CEDH, 13 février 2024, n° 33696/19, *Podchasov c. Russie*, points 78 et 79.

⁵ Sur cette décision, voir A. Latil, *Les « portes dérobées » incompatibles avec le droit à la vie privée des utilisateurs de messageries cryptées*, Communication Commerce électronique n° 5, Mai 2024, comm. 5.

⁶ Cf. G. Poupard, *De la cryptographie à la sécurité numérique : une décennie et la suite*, Sécurité globale, vol. 19, no. 3, 2019, pp. 5-10.

2. « *Vivre et laisser chiffrer* », l'acceptation d'une sécurité nationale concurrencée par la sécurité du numérique

En contrepartie des innovations technologiques et de l'Internet, les sociétés numérisées et, plus particulièrement, les démocraties doivent faire face à des risques et menaces en cybersécurité toujours plus critiques pour leur organisation et fonctionnement, la militarisation du cyberspace pouvant aller même jusqu'à remettre en cause la paix et la sécurité internationale¹. Par conséquent, les institutions publiques de cybersécurité telles que l'ANSSI² et l'Agence de l'Union européenne pour la cybersécurité (ENISA)³ considèrent désormais que la libéralisation et la démocratisation du chiffrement doivent être encouragées par les Etats et qu'un rétablissement du contrôle de la cryptologie ne pourrait avoir que pour effets un impact négatif sur l'économie numérique et de rendre vulnérable l'ensemble de l'écosystème.

Dans ces conditions, on ne peut que constater que le droit à un chiffrement robuste devient une nécessité dans les sociétés numérisées et qu'il incarne avec force le principe selon lequel la liberté et la sécurité ne s'opposent pas mais s'accordent⁴. En matière de renseignement, on reprendra l'analyse du Professeur Bertrand Warusfel qui conduit à accepter le risque de limitation des moyens de sauvegarde de la sécurité nationale au bénéfice de la sécurité numérique de la société⁵, voir même du cyberspace.

Cette acceptation d'une sécurité nationale concurrencée par la sécurité du numérique à travers le droit au chiffrement robuste apparait ainsi la meilleure solution dans les régimes démocratiques respectant l'Etat de droit ou pour l'établissement d'un tel régime⁶, *a fortiori* lorsque les pouvoirs publics disposent légalement de nombreux moyens techniques d'investigation tels que la possibilité

¹ Cf. supra. Chapitre I du Titre II de la Seconde partie.

² Cf. Note de l'ANSSI sur le chiffrement du 24 mars 2016 publiée par Libération.

³ Cf. ENISA, *On the free use of cryptographic tools for (self) protection of EU citizens*, January 20, 2016.

⁴ En ce sens, voir également l'avis du CNNum de septembre 2017, « *Prédictions, chiffrement et libertés* » ou encore L. Blisson, *Petits vices et grandes vertus du chiffrement*, *Délibérée*, vol. 7, no. 2, 2019, pp. 56-59.

⁵ Cf. B. Warusfel, *La cryptologie au cœur de la cybersécurité : enjeux et choix*, op. cit..

⁶ En ce sens, voir K. Macnish, *An End to Encryption ? Surveillance and Proportionality in the Crypto-Wars*, In : Henschke, A., Reed, A., Robbins, S., Miller, S. (eds) *Counter-Terrorism, Ethics and Technology. Advanced Sciences and Technologies for Security Applications*, 2021.

de capter des données informatiques avant qu'elles ne soient chiffrées ou le recours à la captation massive de données de connexion qui ne sont pas chiffrées¹. En France, on rappellera que ces moyens sont prévus par les lois relatives au renseignement et qu'ils n'ont cessé d'être renforcés². En revanche, il convient d'être plus réservé sur la possibilité pour les services de renseignement et d'enquêtes judiciaires d'utiliser des vulnérabilités informatiques encore inconnues pour contourner le chiffrement, il s'agit là d'un nouvel enjeu tout aussi majeur que la cryptologie pour la cybersécurité de la société.

§2. Le nouvel enjeu de la « course aux vulnérabilités »

Pas un jour ne passe sans que les autorités nationales et entreprises de cybersécurité et les médias révèlent l'existence de nouvelles vulnérabilités informatiques ou « failles de sécurité » dont l'exploitation permet le piratage d'un système numérique et les fuites de données.

Au sens large, les vulnérabilités informatiques peuvent résulter d'un défaut de conception ou de sécurité du système, d'un mauvais paramétrage du système ou d'un usage inapproprié par les utilisateurs³. Pour les organismes experts en vulnérabilités informatiques, ces dernières se caractérisent généralement par trois éléments : l'existence d'une faiblesse dans le système qui peut être découverte et utilisée par des « *hackers* » et qui a pour effet de compromettre la sécurité du logiciel ou du matériel concerné⁴.

Ainsi, toutes les vulnérabilités n'ont pas la même valeur en matière de cybersécurité : d'une part, une vulnérabilité se transforme en arme informatique pour les « *hackers* » lorsqu'elle peut être accompagnée d'un « *exploit* », c'est-à-dire d'un code malveillant tirant profit de la vulnérabilité afin de s'attaquer au système numérique ciblé⁵ ; d'autre part, parmi les vulnérabilités exploitables, celles dites

¹ En ce sens, voir C. C. Murphy, *The Crypto-Wars myth : The reality of state access to encrypted communications*, Common Law World Review, 49(3-4), 2020, 245-261.

² Cf. supra. Titre I de la Première partie.

³ Sur cette définition, voir J. -M. Bockel, *Rapport d'information sur la cyberdéfense*, op. cit., p. 29.

⁴ En ce sens, voir le document de l'ENISA, *Good Practice Guide on Vulnerability Disclosure*, novembre 2015, p. 14 à 16.

⁵ A ce sujet, voir A. Sudres, « *Cyberespace et dimension stratégique de la force informatique* », *Stratégie*, vol. 117, no. 4, 2017, pp. 65-82.

« *zero-day* » qui ne sont pas encore connues par les concepteurs constituent les vulnérabilités les plus redoutées puisqu'elles ne peuvent pas faire l'objet de corrections et rendent donc leur exploitation imparable¹. Toutefois, notons que la majorité des vulnérabilités exploitées sont connues².

La découverte des vulnérabilités informatiques est une véritable course entre les « *hackers* » qui souhaitent les exploiter et les acteurs de la cybersécurité et les entreprises du numérique qui ont pour objectif leur divulgation afin de les corriger. Sur le plan opérationnel, les pouvoirs publics et le secteur privé organisent un système de veille et de partage d'informations, initié aux Etats-Unis, aux niveaux international et national sur les failles de sécurité dans le cadre de leur centre de réponse à incident informatique ou « CERT » (« *Computer Emergency Response Team* » en anglais) selon le format universel « *Common Vulnerabilities and Exposure* » (CVE) d'identification et de classification des vulnérabilités³. En France, la fonction de CERT national est assurée par le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques de l'ANSSI qui est membres de plusieurs réseaux européens et internationaux dont le « *Computer Security Incident response Teams Network* » (CSIRTs Network), créé par la Directive NIS⁴ qui regroupe les CERT des pays de l'Union européenne et l'ENISA, ou encore le « *Forum of incident response and security teams* » (FIRST), qui offre un espace de partage d'informations international entre CERT nationaux et d'autres équipes de réponse aux incidents informatiques.

Toutefois, les CERT publics ou privés sont concurrencés dans leur recherche de vulnérabilités par des « *hackers* » solitaires ou organisés, voir même des entreprises spécialisées dans la collecte de failles de sécurité, qui agissent pour leur propre compte dans un but lucratif. Leurs services peuvent être sollicités par

¹ A ce sujet, voir notamment L. Urban, « *La vie privée révélée et la vulnérabilité exploitée – une approche comparée du piratage informatique en tant que méthode occulte d'enquête policière* », Archives de politique criminelle, vol. 43, no. 1, 2021, pp. 207-219.

² En ce sens, voir S. Bombal et V. Le Bihan, « *Planifier et conduire les opérations numériques* », Stéphane Taillat éd., La Cyberdéfense. Politique de l'espace numérique. op. cit., pp. 218-232.

³ Sur l'organisation de la réponse opérationnelle contre les failles de sécurité, voir notamment A. - Y. Le Dain et B. Sido, *Rapport sur la sécurité numérique et risques : enjeux et chances pour les entreprises*, Office parlementaire d'évaluation des choix scientifiques et technologiques, Tome 1, 2 février 2015, p. 179 et suivantes.

⁴ Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

les pouvoirs publics ou les entreprises dans le cadre de programmes de « *Bug Bounty* », mais il s'avère que ces services sont également mis à disposition de clients désireux de se voir communiquer des failles de sécurité dans la plus grande discrétion, comme par exemple l'entreprise Zerodium dont la vocation est de fournir des vulnérabilités à des institutions gouvernementales telles que la NSA¹.

Dans un contexte d'augmentation des capacités de cyberespionnage et de cyberdéfense des services de renseignement, notamment en France avec la possibilité de recourir aux captations de données informatiques sur le territoire national² ou aux mesures de piratage informatique à l'étranger pour le renseignement extérieur³, la rétention secrète de vulnérabilités informatiques tend à devenir un besoin opérationnel essentiel qui doit, toutefois, être mis en balance avec la sécurité du cyberspace, d'autant plus depuis l'affaire *WannaCry* de 2017⁴.

Sur le plan juridique, la « course aux vulnérabilités » se traduit par une responsabilisation de la divulgation des vulnérabilités pour répondre aux besoins de la sécurité numérique. En revanche, si la rétention des vulnérabilités pour les intérêts de l'Etat fait l'objet d'une certaine rationalisation administrative, elle demeure insuffisamment affirmée en droit et à contre-courant du mouvement de responsabilisation porté par le droit du numérique.

A – La responsabilisation de la divulgation des vulnérabilités pour la sécurité numérique

Il peut être distinguées deux cas de figure dans lesquels le droit du numérique responsabilise la divulgation des vulnérabilités : d'une part, dans le cas des obligations de notification des failles de sécurité dans les procédures de réponse à incident informatique ; et d'autre part, dans le cas de la divulgation intentionnelle de vulnérabilités par des chercheurs ou « *hackers éthiques* ».

¹ Sur le marché des vulnérabilités informatiques, voir notamment J. -A. Fines Schlumberger, *Le marché lucratif des vulnérabilités informatiques*, La revue européenne des médias et du numérique, n° 60, mai 2022 et F. Massit-Folléa, *La « sécurité offensive », La régulation de l'internet : fictions et frictions*, In : Les débats du numérique, Paris : Presse des Mines, 2013.

² Article L. 853-2 du code de la sécurité intérieure.

³ Article 323-8 du Code pénal.

⁴ En ce sens, voir notamment L. Urban, « *La vie privée révélée et la vulnérabilité exploitée – une approche comparée du piratage informatique en tant que méthode occulte d'enquête policière* », op. cit..

1. Les obligations de notification des failles de sécurité

En matière de protection des données personnelles et de protection des systèmes numériques des opérateurs jugés essentiels pour la société, les textes imposent aux administrations et entreprises concernées de notifier aux autorités nationales compétentes leurs incidents de sécurité informatique, ce qui implique de divulguer les vulnérabilités en cause.

En cas de violation des données personnelles, les articles 33 et 34 du Règlement général sur la protection des données (RGPD) dispose ainsi que le responsable du traitement concerné doit, sous peine d'être condamné à une amende administrative, procéder à une notification à l'autorité de contrôle compétente, la CNIL en France, dans un délai maximum de 72 heures et informer, dans les meilleurs délais, les personnes dont les données ont été compromises lorsque la violation est susceptible de porter une atteinte à leurs droits et libertés. Déjà prévue pour les opérateurs du numérique avant l'adoption du RGPD¹, cette obligation de notification vise les failles de sécurité au sens large puisqu'elle comprend aussi bien les vulnérabilités des logiciels et matériels exploités ou non par un « *hackers* » que celles qui résultent d'une erreur, d'une faute ou d'une négligence du responsable du traitement².

On notera que dans son contrôle, la CNIL s'est montrée sévère dans la gestion des failles de sécurité en considérant que la notification et la correction de ces dernières par le responsable du traitement compromis n'exonère pas ce dernier de toute responsabilité, notamment lorsque le respect de son obligation générale de sécurité, désormais prévue à l'article 32 du RGPD, lui aurait permis d'avoir eu connaissance de la vulnérabilité³. En revanche, la CNIL ne peut pas

¹ Sur la réglementation antérieure au RGPD, voir E. A. Caprioli, *Les notifications de violation de données à caractère personnel et le droit : des questions en suspens*, Communication Commerce électronique n° 5, Mai 2010, comm. 54.

² En ce sens, voir C. Torres, *3 questions. Les failles de sécurité : quel régime juridique ?*, La Semaine Juridique Entreprise et Affaires n° 4, 22 Janvier 2015, 63.

³ Sur le contrôle de la CNIL sur les failles de sécurité, voir notamment la délibération n° 2014-298 du 7 août 2014 de la CNIL sanctionnant Orange et l'étude par R. Perray et L. Ferrando, *Les failles de sécurité : la CNIL met sa politique de sanction en ordre de marche*, Communication Commerce électronique n° 12, Décembre 2017, étude 20.

sanctionner le défaut de notification lorsqu'elle informe elle-même le responsable du traitement de l'existence d'une faille de sécurité¹.

En ce qui concerne les opérateurs jugés essentiels, la loi de programmation militaire du 18 décembre 2013 a consacré à l'article L. 1332-6-2 du code de la défense une obligation d'information à l'ANSSI pour les OIV des incidents affectant leurs systèmes numériques qui permet à l'autorité nationale de cybersécurité d'être alertée sur des vulnérabilités. Le manquement à cette obligation est sanctionné d'une amende précédée d'une mise en demeure². Ajoutons que les contrôles de sécurité des systèmes numériques des OIV prévus par les textes réglementaires ne manquent pas de porter une attention particulière sur la détection et la correction des vulnérabilités³. De manière similaire aux dispositions du code de la défense, une obligation de déclaration d'incidents à l'ANSSI a été introduite pour les OSE depuis l'adoption de la directive NIS et sa loi de transposition de 2018⁴. On notera que les OIV et les OSE peuvent être soumis à une double obligation de notification des failles de sécurité à la CNIL et à l'ANSSI en cas d'incident entraînant une violation de données personnelles, ce qui peut être redondant mais aussi un atout pour le partage d'informations sur les vulnérabilités, leurs risques et leurs menaces pour les personnes physiques et morales⁵. Par ailleurs, on relèvera que l'article 34 de la loi de programmation militaire du 13 juillet 2018 créant l'article L. 33-14 du Code des postes et communications électroniques a introduit deux obligations d'information sur les vulnérabilités pour les opérateurs de télécommunications : d'une part, informer sans délai l'ANSSI des événements détectés qui sont susceptibles d'affecter la sécurité des systèmes numériques de leurs abonnés ; et d'autre part, informer les abonnés sur les vulnérabilités de leurs systèmes à la demande de l'autorité nationale de cybersécurité. Par ailleurs, l'ANSSI peut recueillir auprès de ces

¹ Conseil d'Etat, 22 juillet 2022, requête n° 449694.

² Article L. 1332-7 du code de la défense.

³ Articles R. 1332-41-12 et R. 1332-41-15 du code de la défense.

⁴ Articles 7 et 9 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

⁵ A ce sujet, voir notamment S. Schmitz-Berndt et S. Schiffner, *Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR*, *International Review of Law, Computers & Technology*, 2021, vol. 35, N° 2, p. 101-115.

opérateurs du numérique des informations pour identifier les utilisateurs ou détenteurs de systèmes compromis ou menacés « *afin de les alerter sur la vulnérabilité ou l'atteinte de leur système* »¹.

Par la suite, la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 a prévu une obligation spécifique de notification à l'ANSSI de « vulnérabilité significative » à la charge des éditeurs de logiciels soumis à la législation française². Un fichier dédié au suivi et à la gestion de ces vulnérabilités est placé sous la responsabilité du directeur de l'ANSSI³.

2. La divulgation intentionnelle des vulnérabilités

Principalement le fait de chercheurs ou de « *hackers* éthiques », la divulgation intentionnelle des vulnérabilités de systèmes numériques est tolérée en droit, à la condition de justifier d'un motif légitime ou d'emprunter, de bonne foi, une procédure légitime de partage d'informations.

Depuis la signature de la Convention de Budapest de 2001 sur la cybercriminalité et l'adoption par le législateur français de l'article 323-3-1 du code pénal par la loi pour la confiance dans l'économie numérique (LCEN) de 2004 qui incriminent le trafic, sans motif légitime, des moyens de porter atteinte aux systèmes numériques, il a été jugé que la divulgation de failles de sécurité informatique entre dans le champ d'application de ces textes. Dans son arrêt du 27 octobre 2009, la Chambre criminelle de la Cour de cassation⁴ a ainsi précisé que cette divulgation est constitutive du délit prévu à l'article 323-3-1 du code pénal dès lors qu'elle contient des éléments d'exploitation de la vulnérabilité concernée et qu'elle est adressée à un large public⁵. Suivant la logique préventive des dispositions de l'article 323-3-1, la Cour de cassation a estimé que la divulgation litigieuse avait pour risque de faciliter le piratage informatique du système

¹ Article L. 2321-3 du code de la défense.

² Article L. 2321-4-1 du code de la défense.

³ Arrêté du 18 juin 2024 portant création d'un traitement automatisé de données à caractère personnel dénommé « Suivi des signalements de vulnérabilités par des éditeurs de logiciel ».

⁴ Cass. crim., 27 octobre 2009, n° 09-82.346.

⁵ Sur l'arrêt, voir notamment B. Bouloc, *Communication d'une faille dans un système informatique*, RTD Com. 2010, p. 441 ; M. Véron, *La diffusion d'informations présentant un risque d'utilisation à des fins de piratage*, Droit pénal n° 1, janvier 2010, comm. 3.

vulnérable¹. En ce sens, la haute juridiction judiciaire ne condamne pas la simple divulgation d'une vulnérabilité mais consacre la doctrine de la « divulgation responsable » des failles de sécurité (ou « *responsible disclosure* » en anglais) par opposition à celle de « divulgation complète » (ou « *full disclosure* »)². Si cette solution pourrait apparaître trop restrictive pour les chercheurs en informatique³, elle responsabilise les acteurs du marché des vulnérabilités. Encore faut-il que la divulgation poursuive un motif légitime qui ne peut pas se limiter à la volonté d'informer le public selon la Cour de cassation dont la décision de 2009 indique implicitement que l'article 323-3-1 ne devrait pas faire obstacle à une divulgation responsable à des fins d'alerte de sécurité informatique⁴. A cet égard, la loi de programmation militaire du 18 décembre 2013 est venue, par la suite, textuellement consacrer deux motifs légitimes dans les dispositions du code pénal : « *notamment de recherche ou de sécurité informatique* ». Cet ajout bienvenu permet d'offrir aux programmes de « *Bug Bounty* » un cadre légal et une légitimité.

En revanche, il reste que les chercheurs et « *hackers éthiques* » en vulnérabilités sont toujours susceptibles d'être condamnés pour les faits d'intrusion informatique ou de maintien frauduleux dans un système d'information⁵ dans le cadre de leur démarche de divulgation selon les jurisprudences « *Kitetoo* » et « *Bluetouff* » de la Cour de cassation ou encore pour « *trouble manifestement illicite* » au regard de l'affaire « *Zataz* » jugée par la Cour d'appel de Paris en 2009⁶.

Pour répondre aux inquiétudes des experts en cybersécurité, une procédure légitime de divulgation des vulnérabilités tenant compte des risques

¹ En ce sens, voir J. Francillon, *Piratage informatique. Révélation de failles de sécurité informatique*, RSC 2010, p. 178.

² A ce sujet, voir Observatoire du Monde Cybernétique, *Point juridique sur la publication de failles de sécurité*, Lettre n° 7 – juillet 2012, p. 11 à 13.

³ En ce sens, voir P. Arrigo et D. Blin, *Publier les moyens d'exploiter la vulnérabilité d'un système informatique constitue un délit*, Gazette du Palais, n° 37, 6 février 2010, p. 32.

⁴ Sur l'intention et le motif légitime de divulgation d'une faille de sécurité, voir notamment A. Lepage, *La volonté d'information ne constitue pas, en soi, un motif légitime en matière de publication des vulnérabilités*, La Semaine Juridique Edition Générale n° 1-2, 11 janvier 2010, act. 19.

⁵ Article 323-1 du code pénal.

⁶ Sur ce point, voir C. Legris, *Le lanceur d'alerte informatique, ce hacker incompris*, Revue Lamy Droit de l'Immatériel, N° 145, 1er février 2018 ou encore J. Francillon, *Piratage informatique. Révélation de failles de sécurité informatique*, op. cit..

juridiques liés au piratage informatique est désormais envisagée. Ainsi, la loi pour une République numérique du 7 octobre 2016 a créé l'article 2321-4 du code de la défense qui dispose dans ses deux premiers alinéas que :

« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée ».

La protection offerte par ce texte demeure néanmoins relative puisque son appréciation dépend de l'ANSSI et qu'elle n'est pas opposable aux tiers, notamment au détenteur du système vulnérable qui a fait l'objet d'une intrusion par le « lanceur d'alerte » et qui reste libre d'engager des actions juridiques contre ce dernier sur le plan pénal, civil ou social¹. Autrement dit, les pouvoirs publics reconnaissent le rôle important que jouent les chercheurs et « *hackers éthiques* » dans la « course aux vulnérabilités », sans pour autant leur reconnaître un véritable statut de lanceur d'alerte spécifique. On peut regretter le caractère inabouti de la procédure prévue par l'article L. 2321-4 dans ses effets juridiques, mais elle a le mérite de renforcer le mouvement de responsabilisation de la divulgation des vulnérabilités et de favoriser le partage d'informations avec l'ANSSI, autorité défensive en charge de garantir la cybersécurité de la société.

On ajoutera que dans ce mouvement de responsabilisation, le régime multilatéral de contrôle des exportations des biens à double usage reconnu par l'Union européenne et la France, l'Arrangement de Wassenaar, a fait l'objet d'une révision en 2017 dans l'objectif, là encore, de favoriser les procédures légitimes de partage international d'informations sur les vulnérabilités avec les organisations chargées de leur remédiation². Plus concrètement, la divulgation de vulnérabilités

¹ En ce sens, voir notamment S. Meurant et R. Cardon, *Rapport d'information relatif à la cybersécurité des entreprises*, Sénat, 10 juin 2021, p. 136 à 138.

² A ce sujet, voir notamment A. Gery, *La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense*, op. cit..

entre dans les exemptions au contrôle des exportations des technologies pouvant servir au développement des « logiciels d'intrusion »¹.

La responsabilisation par le droit de la « course aux vulnérabilités » est un progrès dans la lutte contre les risques et menaces des failles de sécurité informatiques, notamment en sécurisant et ordonnant les relations verticales ascendantes que peuvent entretenir les chercheurs et « *hackers* éthiques » avec les autorités publiques de cybersécurité. A contrario, on peut critiquer le manque de rationalisation de la part des Etats dans leurs choix de ne pas divulguer des vulnérabilités pour satisfaire leurs intérêts, notamment de renseignement, qui a pour conséquence de rompre le cycle du partage d'informations et les relations descendantes avec les utilisateurs et détenteurs des systèmes vulnérables.

B – Une rationalisation insuffisante de la rétention des vulnérabilités pour les intérêts de l'Etat

Au préalable, il convient d'admettre qu'il ne peut être dénié à l'Etat le droit de refuser de divulguer des vulnérabilités informatiques pour les besoins de sa cyberdéfense, de ses services de renseignement ou d'enquête judiciaire. Pour autant, certains pays comme les Etats-Unis ou le Royaume-Uni se sont engagés dans une doctrine de contrôle administratif pour rationaliser la mise en balance de la rétention des vulnérabilités face aux dommages réels que cette rétention a pu causer pour la sécurité des systèmes numériques. Malgré l'insuffisance de l'exemple de la doctrine américaine, il est devenu souhaitable de consacrer juridiquement ce type de contrôle administratif.

1. L'affirmation administrative balbutiante d'une mise en balance de la rétention des vulnérabilités

A la suite des révélations de la vulnérabilité « *Heartbleed* » affectant de nombreux sites internet, applications ou systèmes d'exploitation en 2014, le coordinateur américain à la cybersécurité de l'administration Obama, Michael Daniel, avait publiquement reconnu la connaissance de cette faille de sécurité par

¹ Pour plus de détails sur la révision de 2017 de l'Arrangement de Wassenaar, voir notamment Observatoire du Monde Cybernétique, *La révision de l'Arrangement de Wassenaar dans le domaine des logiciels d'intrusion et ses conséquences*, op. cit., p. 2 à 9.

la NSA et révélé l'existence d'une doctrine, adoptée en 2010¹, dite « *Vulnerabilities Equities Process* » (VEP) de contrôle administratif de la mise en balance des rétentions des vulnérabilités à partir de questions soulevant leurs avantages et leurs inconvénients pour les intérêts de l'Etat et la sécurité du numérique². Cependant, il faut attendre les révélations de l'utilisation de vulnérabilités développées par la NSA dans les cyberattaques internationales *WannaCry* et *NotPetya* de 2017³ et l'appel de Microsoft à obliger les Etats à divulguer les failles de sécurité en leur possession⁴ pour qu'une véritable « Charte VEP » soit publiée par l'administration américaine⁵.

Cette Charte organise un contrôle administratif de la rétention ou de la divulgation des vulnérabilités nouvellement découvertes par les administrations américaines et qui ne sont pas encore connues du public. Ces dernières sont invitées à notifier les failles de sécurité à un service neutre de la NSA dédié à leur gestion afin de les soumettre au contrôle d'une commission composée de représentants des différents ministères concernés et présidée par le coordinateur à la cybersécurité du Président des Etats-Unis. Après discussions sur les avantages et les inconvénients d'une rétention ou d'une divulgation, la commission décide par consensus, ou par un vote qui peut être contesté au niveau du Conseil de sécurité nationale. Il est intéressant de noter qu'une décision de rétention de vulnérabilité est annuellement revue par la commission de contrôle. Cette dernière motive sa décision en tenant compte de considérations portant sur la lutte informatique défensive (LID) ou offensive (LIO), les besoins en matière de

¹ The Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process, February 16, 2010.

² Cf. M. Daniel, *Heartbleed : Understanding When We Disclose Cyber Vulnerabilities*, White House, avril 28, 2014.

³ Sur les révélations portant sur la NSA et les cyberattaques *WannaCry* et *NotPetya*, voir notamment E. Georgelin et J. -V. Holeindre. « *Des ruses de guerre numériques ? Le hacking comme ressource stratégique dans les conflits contemporains* », Quaderni, vol. 103, no. 2, 2021, pp. 89-104 ; F. Douzet et S. Taillat. « *Chapitre 6. Les enjeux de politique internationale. L'affirmation du leadership américain* », Stéphane Taillat éd., La Cyberdéfense. Politique de l'espace numérique, op. cit., pp. 111-122 ; C. Delesse. « *La NSA, « mauvais génie » du cybermonde ?* », op. cit. ; G. Hilary, *WannaCry and the Diffusion of Zero Day Exploits*, CREOGEN Research Note no. 25, 2017.

⁴ Sur les déclarations de Microsoft, voir notamment B. Smith, *The need for a Digital Geneva Convention*, Microsoft On the Issues, february 14, 2017 et J. Nocetti, *Géopolitique de la cyber-conflictualité*, Politique Étrangère 83, no. 2 (2018) : 15-27.

⁵ Cf. Vulnerabilities Equities Policy and Process for the United States Government, November 15, 2017.

renseignement ou d'enquête judiciaire¹, les conséquences pour l'économie numérique et les relations internationales. Notons que certaines catégories limitées de vulnérabilités peuvent être exclues du contrôle pour des raisons de sécurité nationale et de confidentialité. Pour faire preuve de transparence et instaurer la confiance entre l'Etat et l'économie numérique, la Charte prévoit la publication d'un rapport annuel sur le traitement des vulnérabilités rédigé par la NSA et soumis au Conseil de sécurité nationale via le coordinateur à la cybersécurité.

L'élaboration d'une doctrine administrative de VEP similaire à celle des Etats-Unis a été implémentée au Royaume-Uni en 2018 dont l'application est assurée par le renseignement numérique britannique avec le National Cyber Security Centre (NCSC) et le GCHQ². D'autres pays adoptent la même démarche comme l'Australie, le Canada ou encore l'Allemagne et l'introduction du concept de VEP n'a pas manqué d'être discuté au niveau international³. Toutefois, l'absence de valeur juridique contraignante du VEP et la place prépondérante qu'occupent les agences de renseignement dans le dispositif n'offrent pas les garanties effectives de proportionnalité, de transparence et de contrôle attendues par la société civile et adaptées aux enjeux de la protection du cyberspace.

¹ En matière de renseignement et d'enquête, la commission de contrôle s'assure de répondre aux questions suivantes : la vulnérabilité peut-elle être exploitée pour soutenir la collecte de renseignements, les cyber-opérations ou la collecte de preuves des forces de l'ordre ? Quelle est la valeur démontrée de la vulnérabilité pour la collecte de renseignements, les cyberopérations et/ou la collecte de preuves en matière d'application de la loi ? Quelle est sa valeur potentielle (future) ? Quelle est l'efficacité opérationnelle de la vulnérabilité ? L'exploitation de la vulnérabilité offre-t-elle une valeur opérationnelle spécialisée contre les cybermenaces ou leurs opérations ? Existe-t-il d'autres moyens de réaliser les avantages opérationnels de l'exploitation de la vulnérabilité ? La divulgation de la vulnérabilité révélerait-elle des sources ou des méthodes de renseignement ?

² Sur le modèle britannique, voir The Equities Process - GCHQ.GOV.UK (<https://www.gchq.gov.uk/information/equities-process>).

³ A ce sujet, voir notamment M. Schulze, *Quo Vadis Cyber Arms Control ? A Sketch of an International Vulnerability Equities Process and a 0-Day Emissions Trading Regime*, Science Peace Security '19. Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research Christian Reuter, Jürgen Altmann, Malte Götttsche, and Mirko Himmel (Editors). TUprints, Darmstadt, 2019.

2. Une consécration juridique souhaitable d'un contrôle de la rétention des vulnérabilités

Le modèle VEP américain est aujourd'hui considéré comme insuffisant sur le plan juridique. Désormais, certains spécialistes souhaitent notamment consacrer par la loi ou par un décret présidentiel (« *Executive Order* » en anglais) le contrôle de la rétention des vulnérabilités et confier cette mission à un organisme de cybersécurité ne relevant pas du renseignement¹.

En Europe, on relèvera que le Centre for European Policy Studies (CEPS), think tank basé à Bruxelles spécialisé sur les affaires européennes, a également publié une étude qui recommande aux Etats et à l'Union européenne l'élaboration d'un cadre juridique contraignant organisant un contrôle de la divulgation ou de la rétention des vulnérabilités pour les intérêts des autorités publiques par un organisme public neutre, indépendant et transparent².

Pour notre part, on proposera d'établir un cadre juridique réglementaire interministériel en France dans le sillage du concept de VEP en tenant compte des spécificités du modèle français de cyberdéfense. Tout d'abord, ce cadre réglementaire fixé par le Premier ministre établirait le périmètre des ministères et administrations concernés qui devrait naturellement comprendre la communauté nationale du renseignement et la communauté de cyberdéfense.

Ensuite, il déterminerait le service chargé de la gestion des vulnérabilités découvertes qui serait, à notre sens, l'ANSSI au regard du modèle français de cyberdéfense. Le texte réaffirmerait ainsi la primauté du caractère défensif de la gestion des vulnérabilités dans la logique des dispositions de l'article L. 2321-4 du code de la défense. Autrement dit, les administrations telles que la DGSE ou le COMCYBER seraient contraintes de communiquer leurs découvertes à l'autorité nationale de cybersécurité, sauf exception lorsque des vulnérabilités concernent spécifiquement des systèmes militaires ou de renseignement.

¹ En ce sens, voir par exemple A. Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter*, Lawfare blog, Wednesday, January 13, 2021 et A. C. Gaudion, *It's time to reform the U.S. Vulnerabilities Equities Process*, U.S. Army War College, September 2, 2021.

² Cf. M. Schaake, L. Pupillo, A. Ferreira, G. Varisco, *Software Vulnerability Disclosure in Europe, Technology, Policies and Legal Challenges*, Report of a CEPS Task Force, June 2018.

Enfin, en s'inspirant du contrôle du régime d'autorisation de l'article 226-3 du code pénal¹, une commission composée des représentants des différentes administrations et présidée par l'ANSSI pourrait contrôler, au cas par cas, la nécessité et la proportionnalité de la divulgation ou de la rétention des vulnérabilités sur la base de critères objectifs. Elle exercerait également un contrôle *a posteriori* sur les décisions de rétention. En outre, il pourrait être envisagé que la composition de la commission puisse intégrer des représentants de l'ARCEP, de la CNIL et de la CNCTR pour renforcer la légitimité de son contrôle et la confiance. On ne manquera pas de proposer l'élaboration d'un rapport annuel sur le traitement des vulnérabilités, notamment sur les décisions de rétention et leur statistique.

Pour finir, on soutiendra que la divulgation des vulnérabilités devrait constituer la règle et leur rétention l'exception, ce dernier cas pouvant être justifié pour des besoins de sécurité nationale ou d'investigation judiciaire mais servant également les intérêts des cybercriminels. Et, la consécration d'un mécanisme de contrôle apporte une réponse de responsabilisation de l'Etat dans la protection du cyberspace qui s'inscrit dans une logique de « due diligence » cyber sur le plan international en cohérence avec les réalités de la « course aux vulnérabilités » et ses conséquences révélées par l'affaire *WannaCry* de 2017².

¹ A ce sujet, voir la Section II du Chapitre II du Titre I de la Seconde partie.

² A ce sujet, on citera Aude Géry qui expliquait que : « *L'exemple des armes cyber volées à la NSA a en effet soulevé la question du stockage de ces armes et des mesures devant être prises afin d'empêcher leur vol. Cette question est d'autant plus importante qu'en cas d'utilisation malveillante à la suite d'un vol, la question de la responsabilité de l'État pour violation de l'obligation de due diligence pourra être soulevée* » (A. Géry, « *La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense* », op. cit.).

CONCLUSION DU TITRE

La reconnaissance du cyberspace comme lieu mondial d'échanges et de conflictualités par les Etats a nettement eu pour effet d'accentuer la numérisation du renseignement pour répondre aux enjeux de cyberdéfense et de cybersécurité. Il convient d'admettre que l'intervention des services de renseignement dans le cyberspace n'est pas un phénomène entièrement nouveau, notamment aux Etats-Unis où la NSA s'est rapidement immiscée dans les développements de l'internet et de l'économie numérique. Cependant, le cadre juridique des services de renseignement se voit confronté à l'augmentation des normes du droit du numérique qui ont pour objet la protection du cyberspace au regard des risques et menaces que peuvent engendrer sa perturbation pour les sociétés numérisées. Cette confrontation se traduit par un élargissement du cadre juridique applicable au renseignement numérique qui n'est pas sans remettre en question l'organisation et le fonctionnement même du renseignement au sein de l'Etat.

Ainsi en est-il de l'encadrement de la « militarisation » du cyberspace à travers le droit national de la cyberdéfense dont les dispositions mettent en concurrence les services de renseignement avec d'autres acteurs publics et privés de la lutte informatique réalisant des missions de cyber-renseignement. L'émergence d'un « mille-feuille » du cyber-renseignement brouille la fonction stratégique même du renseignement d'Etat, en plus de renforcer la surveillance de l'internet.

De même, la recherche d'un encadrement international adapté aux cyberopérations étatiques et à la proliférations des « cyberarmes » tend vers la formalisation d'un droit international du renseignement numérique qui interroge sur l'étendue de la notion d'espionnage, pouvant être entendue restrictivement comme la collecte clandestine de renseignements ou, plus largement au regard du cyber-espionnage, comme les actions clandestines de collecte de renseignements ou d'entrave à des risques et menaces, notamment par le piratage informatique. Evitant jusqu'ici l'application du droit international à l'espionnage, les Etats doivent désormais envisager son application aux actions des services de renseignement dans le cyberspace, voir même l'application des règles relatives

aux agressions armées face aux conséquences possibles des cyberopérations offensives.

Prenant également conscience de l'incapacité des Etats à maintenir un contrôle ou une souveraineté pleine et entière sur les produits et les services numériques ainsi que de la vulnérabilité du cyberspace, les pouvoirs publics nationaux et instances internationales s'accordent progressivement à considérer que la numérisation du renseignement doit se conformer à des exigences de cybersécurité contribuant à sauvegarder la confiance dans l'économie numérique. On retrouve cette préoccupation dans la mise en œuvre de la cyberprotection du renseignement dont les règles s'attachent à concilier le cadre particulier et secret des activités du renseignement avec le recours croissant à l'externalisation pour satisfaire les besoins des services en recherches de technologies toujours plus performantes et efficaces. Aussi, en se positionnant comme garant de la cybersécurité de la société, les Etats semblent s'engager à ne peut pas remettre en cause la liberté de chiffrement et à rejoindre le mouvement de responsabilisation qui s'organise juridiquement sur le traitement des failles de sécurité informatique, ce qui implique alors de nouvelles limitations au renseignement numérique. On peut toutefois regretter le retard de la France dans ces domaines mais des solutions peuvent être rapidement mises en place.

De l'application des règles de cyberdéfense ou de cybersécurité au renseignement numérique, il émerge une nouvelle distinction dans la répartition des missions du renseignement qui doit être clarifiée. Les spécificités du cyber-renseignement occultent la distinction entre renseignement intérieur et renseignement extérieur pour laisser place à celle qui organise la lutte informatique soit selon le modèle américain ou britannique qui fusionne la LID et la LIO au sein d'une seule agence technique, soit selon le modèle français qui sépare la défense de l'offensif. Si le premier modèle a des avantages opérationnels, le modèle français nous semble plus cohérent avec les enjeux politiques et juridiques du cyberspace dès lors que l'on garde à l'esprit que ce modèle n'a pas vocation à se substituer à l'organisation de la communauté nationale du renseignement et que les actions de cyber-renseignement ne sont pas toutes de même nature. L'ANSSI demeure une autorité de cybersécurité dont l'activité de renseignement a pour mission d'aider les victimes de cyberattaques et d'apporter

une réponse défensive technique alors que les services de renseignement interviennent dans une perspective plus large d'aide à la décision du gouvernement en matière de sécurité nationale et de relations internationales.

Une nouvelle conciliation émerge également dans l'encadrement des services de renseignement face à la protection du cyberspace. A celle traditionnelle à opérer entre la sécurité nationale et les libertés et droits fondamentaux s'ajoute une conciliation plus subtile dans les règles à invoquer entre la sécurité nationale et la sécurité du numérique. En effet, ces deux finalités justifiant des mesures juridiques de protection peuvent être aussi bien confondues pour autoriser les services de l'Etat à recourir à des moyens de surveillance dérogatoires au respect des libertés qu'être en opposition pour, cette fois-ci, limiter les moyens de surveillance numérique et apporter des garanties spécifiques de protection de l'économie numérique et aux droits et libertés des internautes.

En plus de modifier les conditions d'activités des services de renseignement, le cyberspace et sa protection juridique bouleverse, par là même, le cadre juridique du renseignement. Bien que des réponses soient proposées pour répondre aux incertitudes de ce bouleversement, il devient ainsi nécessaire d'inscrire la régulation du renseignement numérique dans celle plus large de la technologie pour répondre à leurs enjeux communs relatifs au respect de l'Etat de droit, à la sécurité et aux libertés dans les sociétés démocratiques numérisées telles que la France. En ce sens, il est temps que les Etats, individuellement et collectivement, assument une véritable régulation démocratique de leurs outils, notamment de cybersurveillance, et de la société numérique afin d'éviter leur déclin devant la puissance mais aussi les vulnérabilités de la doctrine du « code is law » redoutée par le Professeur Lawrence Lessig¹.

¹ En ce sens, voir notamment B. Warusfel, *Technologies et sécurité : réguler pour reprendre le contrôle*, Cahiers de la sécurité et de la justice de l'INHESJ n° 50, 2021, p. 254 à 260 et M. Watin-Augouard, *La cybersécurité, enjeu de la souveraineté à l'ère numérique*, op. cit..

CONCLUSION GENERALE

RENFORCER L'ENCADREMENT DU RENSEIGNEMENT NUMERIQUE

L'utilisation des technologies du numérique par le renseignement d'Etat dans l'organisation et l'exécution ses missions n'est pas un phénomène nouveau. Cependant, les progrès de l'informatique avec le Big data et l'Intelligence artificielle ainsi que les développements du cyberspace ont démultiplié les capacités du renseignement numérique, notamment pour lutter efficacement contre le terrorisme, et renouvelé ses missions pour les besoins de la cyberdéfense.

Cette numérisation suscite des inquiétudes pour les droits et libertés face au risque d'une surveillance de masse liberticide mais aussi pour l'économie numérique qui peut être fragilisée par les capacités de cyberespionnage. Par conséquent, ces enjeux de la numérisation du renseignement n'ont pas manqué d'être appréhendée par le droit, tant au niveau international et européen qu'au niveau national.

Plus particulièrement, l'encadrement de la numérisation du renseignement fait l'objet d'une dualité entre le droit du renseignement et le droit du numérique dont l'articulation n'est pas évidente. Si un droit du renseignement numérique semble émerger pour réguler de façon autonome les moyens numériques de renseignement, force est de constater que l'application du droit du numérique au renseignement s'affirme pour appréhender l'ensemble des enjeux juridiques de la numérisation du renseignement.

Cependant, l'état actuel du droit demeure globalement favorable à une technologisation du renseignement dès lors qu'elle se justifie par les besoins de la sécurité nationale alors même qu'elle brouille les fonctions de sécurité de l'Etat, qu'elle introduit davantage de vulnérabilités pour la sécurité du cyberspace et qu'elle permettrait de faciliter les atteintes aux droits et libertés des individus. Dans ces considérations, il nous apparait désormais opportun de renforcer

l'encadrement du renseignement numérique tant dans le droit du renseignement que dans le droit du numérique, selon une articulation cohérente au service d'un Etat de droit démocratique numérisé. Deux axes de renforcement peuvent être proposés à la réflexion : un axe organisationnel qui porte sur la délimitation des acteurs du renseignement numérique (**Section I**) et un axe matériel qui invite à une plus grande vigilance dans l'encadrement des nouveaux moyens numériques de renseignement (**Section II**).

SECTION I : La délimitation du renseignement numérique

Les possibilités offertes par le numérique de mettre en place des systèmes de partages de données entre les services de renseignement et de nombreux acteurs publics ou privés ainsi que la participation du renseignement à la cyberdéfense nécessite de situer juridiquement le renseignement numérique par rapport aux autres activités qui interagissent avec lui. Plus encore, les spécificités du renseignement numérique interrogent sur son autonomie organisationnelle qui pourrait apparaître cohérente au regard d'une certaine autonomisation de son droit. Après avoir rappelé le rattachement du renseignement numérique à l'appareil de renseignement d'Etat (§1.), on soutiendra que l'organisation française du renseignement numérique, fondée sur la mutualisation des moyens, constitue un exemple de limitation soucieuse des libertés et des problématiques de cybersécurité qui n'a nullement besoin d'être réformé pour adopter un modèle similaire au renseignement numérique américain ou britannique (§2.).

§1. Le rattachement à l'appareil de renseignement d'Etat

En droit, les termes « renseignement numérique », « cyber-renseignement », « renseignement technique » ou encore « cyberespionnage » peuvent renvoyer à plusieurs activités d'acteurs publics ou privés, plus ou moins secrets, de collecte et d'exploitation de données à des fins de surveillance. Pour ce qui nous concerne, on rattachera ces termes en France à la politique publique de renseignement¹ et aux activités des services spécialisés de renseignement qui sont

¹ Article L. 811-1 du code de la sécurité intérieure.

placés sous l'autorité du Gouvernement et qui se conforment aux orientations du Conseil national du renseignement¹. Dans ces conditions, plusieurs principes organisationnels pourraient être affirmés.

Tout d'abord, seuls les services répondant aux besoins de la communauté nationale de renseignement devraient pouvoir entrer dans le champ du renseignement numérique. Autrement dit, il conviendrait d'exclure les services de l'Etat ne participant manifestement pas à la politique publique de renseignement de l'élargissement du recours aux techniques numériques de renseignement prévu à l'article L. 811-4 du code de la sécurité intérieure. Il s'agirait notamment de limiter le recours à ces techniques administratives par les services de police judiciaire qui disposent de techniques similaires selon le code de procédure pénale.

En ce qui concerne ces dernières, il serait ensuite anormal que le renseignement numérique conduise à consacrer une systématisation de partages des données dans le sens d'une judiciarisation du renseignement ayant pour conséquence, en vertu du principe de primauté de l'autorité judiciaire, l'avènement d'une police répressive prédictive bafouant la séparation des pouvoirs.

Enfin, l'organisation de la cyberdéfense française et son « mille-feuille » de cyber-renseignement ne devraient pas conduire les pouvoirs publics à envisager l'intégration de l'ANSSI dans la communauté nationale du renseignement, même si cette dernière se voit confier des mesures techniques similaires aux services de renseignement. Garante pour le compte de l'Etat de la cybersécurité de la société, l'ANSSI ne peut être rattachée au renseignement numérique au risque de briser la confiance des entreprises et des internautes. Par ailleurs, le renseignement partenarial avec des opérateurs privés détenteurs de données stratégiques qu'exige le renseignement numérique n'implique pas nécessairement une privatisation du renseignement ou l'organisation d'une économie numérique de la surveillance, à la condition qu'une séparation garante des libertés, notamment celle du commerce et de l'industrie, soit organisée. A cet égard, la collaboration entre les services de renseignement et les opérateurs du numérique organisée via

¹ Article L. 811-2 du code de la sécurité intérieure.

le Groupement interministériel de contrôle (GIC) nous apparaît un exemple à suivre et un argument non négligeable pour soutenir une consolidation du modèle français de renseignement numérique.

§2. La consolidation du modèle français de mutualisation

Les modèles de renseignement numérique américain et britannique incarnés par une agence technique autonome regroupant également les moyens de cyberdéfense, la NSA pour le premier et le GCHQ pour le second, offrent des avantages opérationnels certains, notamment pour faire innover les programmes de surveillance. Pour autant, les Crypto Wars, les révélations d'Edward Snowden ou encore les cyberattaques mondiales WannaCry et NotPetya tendent à démontrer les limites de ce type d'organisation du renseignement numérique face aux enjeux démocratiques des sociétés numérisées.

De son côté, le modèle français qui repose sur la mutualisation des moyens numériques entre les différents services de renseignement peut s'avérer être une source de confusion et d'incohérence dans la mise en œuvre et le contrôle des techniques numériques au regard d'une montée en puissance capacitaire au profit de l'ensemble de la communauté du renseignement. En outre, ce modèle combiné à celui de la cyberdéfense conduit à privilégier les moyens de la DGSE et de la DGSI et constitue un facteur d'inégalité entre les membres de la communauté nationale du renseignement. Malgré ces remarques, il nous semble néanmoins préférable de consolider le modèle actuel et de ne pas envisager la création d'une agence autonome de renseignement numérique pour trois raisons.

Premièrement, le rapprochement avec les modèles américain ou britannique pourrait avoir pour effet de mettre fin aux fonctions technico-juridiques neutres du GIC de mise en œuvre des moyens de surveillance auprès des opérateurs du numérique qui constituent une garantie contre les risques d'abus.

Deuxièmement, la création d'un nouveau service national regroupant les moyens de renseignement numérique ne serait pas sans conséquences sur le modèle de cyberdéfense. Ce nouveau service opèrerait une probable confusion entre la LID, la LIO et la L2I et entrerait alors en concurrence avec l'ANSSI, le COMCYBER et VIGINUM. A plus long terme, cette situation risquerait d'entraîner

une fusion des services au profit du renseignement pour éviter les doublons, ce qui constituerait une régression du rôle de l'Etat pour garantir la cybersécurité de la société.

Troisièmement, il deviendrait difficile en pratique de faire respecter par un service de renseignement numérique autonome les distinctions entre les renseignements intérieur et extérieur consacrées dans le droit du renseignement français ainsi qu'entre la surveillance ciblée et non ciblée des individus. C'est alors l'ensemble du cadre juridique des services de renseignement qui se verrait bouleversé et à repenser.

La délimitation actuelle de l'organisation du renseignement numérique en France nous semble donc globalement adaptée aux enjeux des démocraties numérisées. En revanche, il nous apparaît nécessaire d'être plus vigilant dans l'encadrement et le contrôle de nouveaux moyens numériques de renseignement.

SECTION II : Une plus grande vigilance dans l'encadrement de nouveaux moyens numériques de renseignement

Depuis la fin des années 1970, une dizaine de textes législatifs sont venues renforcer les moyens numériques de renseignement, c'est-à-dire les dispositifs de renseignement d'intérêt cyber (RIC) et de renseignement d'origine cyber (ROC). La grande majorité des textes concernent directement l'arsenal numérique des services de renseignement. Faiblement censurées, ces lois dérogatoires reflètent une tendance à une technologisation de la sécurité presque sans limites lorsque de nouveaux moyens sont justifiés par les besoins de la sécurité nationale. Selon nous, cette situation n'est pas tenable au regard des enjeux de la cybersécurité et de « sécurité humaine » dans la cybersurveillance. Dès lors, il conviendrait désormais d'adopter plus de rigueur dans la légalisation de nouveaux moyens (§1.) et d'étendre leur contrôle (§2.) afin d'éviter les risques de réelles dérives liberticides.

§1. Une légalisation des moyens plus rigoureuse

Bien que le législateur s'efforce d'adopter une certaine neutralité technologique dans la légalisation des moyens numériques de renseignement selon leur finalité et leur niveau d'atteinte aux libertés, il apparaît inévitable de tenir compte de la technologie elle-même pour que cette légalisation puisse trouver à s'appliquer. L'expérimentation s'est alors révélée être une solution confortable pour le législateur mais elle constitue, à nos yeux, une approche inadéquate pour répondre à des enjeux démocratiques majeurs de respect des libertés et de cybersécurité de la société. Le cyberspace et les internautes ne peuvent être placés dans une logique de « bac à sable » des services de renseignement, d'autant plus que la solution expérimentale peut dériver vers la doctrine redoutée du « code is law ».

On pourrait alors profiter de l'émergence d'un certain régime juridique de « recherche et développement », consacré en matière d'essais des techniques de renseignement et de conservation des renseignements collectés pour les besoins de l'intelligence artificielle, pour affirmer un cadre juridique dédié à l'évaluation des nouveaux moyens numériques de renseignement. Dans ce cadre séparé du droit de la surveillance, les services de renseignement seraient ainsi autorisés à éprouver de nouvelles solutions pour les adapter spécialement à leurs besoins et à leur réglementation. Davantage de rapprochements avec les entreprises du numériques et le monde académique pourraient alors être facilités pour concevoir des solutions souveraines et innovantes.

De la distinction entre un régime juridique de « recherche et développement » et un régime juridique de la surveillance, il serait alors possible de rendre la légalisation de nouveaux moyens numériques de renseignement plus rigoureuse. En effet, le premier régime aurait vocation à établir la réelle utilité, la fiabilité et la cohérence de l'introduction d'un nouveau dispositif dans le second régime, renforçant alors la clarté, l'intelligibilité et la prévisibilité de la loi.

Une telle approche permettrait d'ailleurs d'adapter le renseignement numérique aux nouveaux enjeux de la numérisation des sociétés qui mettent en concurrence les concepts de sécurité nationale, de sécurité humaine et de sécurité du numérique. Autrement dit, la cybersécurité devrait également pouvoir constituer une finalité qui limite ou interdise la légalisation de nouveaux moyens

numériques de renseignement trop intrusifs ainsi qu'un critère à prendre en compte dans le contrôle de ces moyens.

§2. Un contrôle des moyens plus étendu

On commencera par saluer l'apport de la jurisprudence de la CJUE dans le renforcement du contrôle des moyens de surveillance numérique à travers notamment l'introduction d'un contrôle de la gravité et de la réalité de la menace pour la sécurité nationale. Il est effectivement bienvenu pour l'Etat de droit et la démocratie de pouvoir mettre en débat la finalité même de sécurité nationale qui justifierait les atteintes les plus graves aux libertés. Au-delà des techniques numériques, ce nouveau contrôle trouve toute sa place dans le contrôle du renseignement. En revanche, les enjeux numériques devraient particulièrement conduire à étendre le contrôle de proportionnalité et de nécessité des moyens aux considérations nouvelles du droit de la cybersécurité¹, en plus de celles relatives aux libertés et droits fondamentaux. En ce sens, il pourrait être envisagé quelques innovations dans le contrôle :

- d'abord, en s'inspirant de la jurisprudence constitutionnelle relative au délit de consultation de sites à caractère terroriste², le Conseil constitutionnel pourrait renforcer son contrôle de proportionnalité de la légalisation d'un nouveau moyen numérique de renseignement en tenant compte de l'ensemble des moyens de surveillance déjà mis en œuvre par l'Etat dans le cyberspace, que ce soit en matière de renseignement mais aussi en matière de cyberdéfense ou de lutte contre la cybercriminalité ;
- ensuite, il serait pertinent de renforcer la responsabilisation de l'administration et des agents des services de renseignement dans l'usage des moyens numériques en permettant : d'une part, à la CNCTR d'opérer un véritable contrôle contraignant sur la centralisation des techniques et des renseignements numériques et d'élargir son contrôle aux fichiers de renseignement ; d'autre part, à la formation spécialisée du Conseil d'Etat d'exercer un contrôle entier des mesures de surveillance à l'encontre d'un

¹ Dans le sens de l'apparition d'un véritable droit de la cybersécurité, voir T. Douville, *L'émergence d'un droit commun de la cybersécurité*, Recueil Dalloz 2017, p. 2255.

² Décisions n° 2016-611 QPC du 10 février 2017 et n° 2017-682 QPC du 15 décembre 2017.

individu, d'assurer le respect du droit d'accès indirect aux données personnelles classifiées et de faciliter la transmission d'une affaire susceptible de relever de la cybercriminalité au parquet en disposant de la faculté de juger de la déclassification des informations utiles à l'enquête. On ajoutera, ici, notre souhait d'établir une commission de contrôle de la rétention des vulnérabilités informatiques pour les besoins du renseignement.

Ces considérations appellent deux dernières remarques. Elles invitent les contrôleurs à adopter une double fonction, celle de contrôler les activités des services de renseignement et celle de veiller à la cybersécurité de la société. Elles incitent les contrôleurs du renseignement mais aussi ceux de la cybergdéfense à s'organiser en une communauté d'intérêt pour répondre à l'objectif d'une régulation publique des technologies conforme aux nécessités des sociétés démocratiques numérisées.

De l'organisation du renseignement numérique et des moyens technologiques conférés aux services secrets, c'est bien le choix d'une société numérique qui peut être affirmé. On ne peut ainsi nier l'importance de l'encadrement de la numérisation du renseignement dans la gouvernance des Etats et du cyberspace, ainsi que l'eupéanisation et l'internationalisation du droit du renseignement que cet encadrement provoque.

Aujourd'hui, il n'est plus question de se laisser porter par l'innovation technologique pour répondre aux inquiétudes sécuritaires des pouvoirs publics mais de s'investir dans la protection des sociétés numérisées dont l'exploitation des vulnérabilités, au sens le plus large, n'aboutira qu'à un plus grand désordre. L'heure est à l'élaboration d'un cadre juridique de la numérisation du renseignement soucieux du rôle de l'Etat comme garant de la cybersécurité de la société, rappelant par là même la légitimité des forces de sécurité lorsqu'elles agissent dans le respect des libertés et droits fondamentaux. Cette perspective protectrice des principes de la démocratie ne peut se concevoir que si le renseignement numérique est mieux encadré, ses effets délétères mieux contrôlés et ses dérives véritablement sanctionnées.

BIBLIOGRAPHIE

I. OUVRAGES

Classement thématique par ordres chronologiques

A. Ouvrages sur le renseignement et la sécurité

WARUSFEL, Bertrand. *Le renseignement contemporain – Aspects politiques et juridiques*, Éditions L'Harmattan, 2003

BAUER, Alain et SOULLEZ, Christophe. *Les fichiers de police et de gendarmerie*. Presses Universitaires de France, 2011

LAFOUASSE, Fabien. *L'espionnage dans le droit international*, Editions Nouveau Monde, 2012

VALLAR, Christian et LATOUR, Xavier. *Le droit de la sécurité et de la défense en 2013*. Presses Universitaires d'Aix-Marseille. 30 avril 2014

COUSSERAN, Jean-Claude. HAYEZ, Philippe. *Renseigner les démocraties, renseigner en démocratie*. Odile Jacob, 2015

MARTIN, David. *Les fichiers de police*. Presse universitaire de France. Que sais-je ? n° 3461, 9 octobre 2015

LAURENT Sébastien et WARUSFEL Bertrand, *Transformations et réformes de la sécurité et du renseignement en Europe*, Presses Universitaires de Bordeaux, 2016

CONSEIL DE L'EUROPE. *Partie 1. Les opérations de surveillance massive, Surveillance de masse*, 2016

DE MAISON ROUGE, Olivier. *Le droit du renseignement*. LexisNexis, 2016

COUSSERAN, Jean-Claude et HAVEZ, Philippe. *Leçon sur le Renseignement*, Odile Jacob, septembre 2017

COTTERET, Jean-Marie et DENECE, Éric, *Le renseignement au service de la démocratie*. Fauves Editions, 2018

DELESSE, Claude. *NSA, Histoire de la plus secrète des agences de renseignement*, collection Texto, Editions Tallandier, 2018

MOUTOUH, Hugues et POIROT, Jérôme. *Dictionnaire du renseignement*. Perrin, 2018

WARUSFEL, Bertrand et BAUDE, Florent. *Annuaire 2018 du droit de la sécurité et de la défense*, Mare et Martin, 2018

CHOPIN, Olivier et OUDET, Benjamin. *Renseignement et sécurité*. Armand Colin, 2019

AFROUKH, Mustapha, MAUBERNARD, Christophe et VAL, Claire. *La sécurité : mutations et incertitudes*, Institut universitaire Varenne, 2019

FORCADE, Olivier et WARUSFEL, Bertrand. *Le droit du renseignement*, Actes du colloque organisé par l'Académie du renseignement à l'Ecole militaire, le 8 février 2019

BUCHAN, Russel. *Cyber Espionage and International Law*. Bloomsbury Publishing, 25 février 2021

MOULIN, Thibault. *Le cyber espionnage en droit international*, Editions Pedone, septembre 2021

CUMIN, David et MESZAROS, Thomas. *Annuaire 2021 du droit de la sécurité et de la défense*, Mare & Martin, 2021

VERON, Noémie. *Protection des données personnelles et renseignement : contribution à l'identification d'un régime juridique autonome*, Institut Francophone Justice et Démocratie – Theses N° 217, 20 décembre 2022

GUILLAUMAIN, Béatrice. *L'appareil français de renseignement. Une administration ordinaire aux attributs extraordinaires*, Mare & Martin, Bibliothèque des thèses, 25 avril 2024

LAURENT, Sébastien-Yves. *Etat secret, Etat clandestin : essai sur la transparence démocratique*, Editions Gallimard, 2024

B. Ouvrages sur le numérique et autres

GENY, François. *Des droits sur les lettres missives*. Sirey, 1911

STERN, Jacques. *La Science du secret*. Odile Jacob, 1998

SINGH, Simon. *Histoire de codes secrets*. Lattès, 1999

MORANGE, Jean. *La Déclaration des Droits de l'Homme et du Citoyen (26 août 1789)*. Presses Universitaires de France, 2002

HARBULOT, Christian. *Manuel d'intelligence économique*. Presses Universitaires de France, 2012

CARMES, Maryse et NOYER, Jean-Max. *Les débats du numérique*. Presse des Mines, 2013

- GUILLLOT, Philippe. *La cryptologie, l'art des codes secrets*, EDP Sciences, 2013
- CRYNBAUM, Luc. LE GOFFIC, Caroline et MORIET-HAIDARA, Lydia. *Droit des activités numériques*, Précis, juin 2014
- CHEVALLIER-GEYERS, Constance. *L'échange de données dans l'Espace de liberté, de sécurité et de justice de l'Union européenne*. Mare & Martin, 2017
- SCHMITT, Michael N. *Manuel de Tallinn 2.0 sur le droit international applicable aux cyberopérations*, Cambridge University Press, 2017
- EUROPEAN DATA PROTECTION SUPERVISOR. *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*. 11 avril 2017
- TAILLAT, Stéphane. *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin. 2018
- AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE. *Manuel de droit européen en matière de protection des données*. Edition 2018
- VAN ENIS, Quentin et DE TERWANGNE, Cécile, *L'Europe des droits de l'homme à l'heure d'Internet*. Bruxelles, Bruylant, inPress, 2019
- SNOWDEN, Edward. *Mémoires vives*, Editions du Seuil, 19 septembre 2019
- GRANGE, Maryline et NORODOM, Anne-Thida. *Cyberattaque et droit international. Problèmes choisis*, Paris, Pedone, 2019
- FERAL-SCHUHL, christiane. *Cyberdroit*, Praxis Dalloz, 2020
- CASTETS-RENARD, Céline, NDIOR, Valère et RASS-MASSON, Lukas. *Enjeux Internationaux Des Activités Numériques*, Bruxelles, Larcier, 2020
- STERN, Jacques. *La cryptologie au cœur du numérique*. Les Grandes Voix de la Recherche, CNRS éditions, 2021
- LAURENT, Sébastien-Yves. *Conflits, crimes et régulations dans le cyberspace*, vol. 4, ISTE, 2021
- TAILLAT, Stéphane, CATTARUZZA, Amaël et DANET, Didier. *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, 2023
- LATIL, Arnaud. *Le droit du numérique. Une approche par les risques*, Hors collection Dalloz, mars 2023
- QUEMENER, Myriam. *Ecosystème numérique : défis juridiques et sociétaux*, Gualino, Hors collection, 4 avril 2023

II. ARTICLES

Classement thématique et par ordres alphabétiques

A. Droit du renseignement numérique

ALIX, Julie et CAHN, Olivier. *Mutations de l'antiterrorisme et émergence d'un droit répressif de la sécurité nationale*, Revue de Science Criminelle et de Droit Pénal Comparé, Dalloz, 2018, p. 845

BAUER, Alain et SOULLEZ, Christophe. *Des fichiers, pour quelles finalités ?*, in Alain Bauer éd., Les fichiers de police et de gendarmerie, Presses Universitaires de France, 2011

BEDARRIDES, Edouard. *Des écoutes au renseignement, un exemple de la distinction entre les polices judiciaire et administrative*, AJDA 2015, p. 2026

BOSSUROY, François. *L'accès aux fichiers des renseignements généraux*. ADJA 2002

BOULOC, Bernard. *Réglementation des écoutes téléphoniques*, RSC 1992

BRICET, Georges-Henri. *Les technologies de renseignement en France : à la recherche d'un modèle de développement*. Revue Défense Nationale, vol. 825, no. 10, 2019, pp. 83-89

BRUN, Olivier. *Secret de la défense nationale*. in Dictionnaire du renseignement. Perrin, 2018, pp. 707-710

CAPRIOLI, Eric A. *Interception légale de sécurité*. Communication Commerce électronique n° 10, Octobre 2016, comm. 87

CAPRIOLI, Eric A. *Lutte contre le terrorisme – Les technologies de l'information et la lutte anti-terroriste*. Communication Commerce électronique n° 5, Mai 2006

CARAYON, Lisa. *Quelle folie !*. La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés, mis en ligne le 11 juin 2020

CATELAN, Nicolas. *Les nouveaux textes relatifs au renseignement : un moindre mal*. RSC 2015

CHAMBON, Pierre. *Analyse et commentaire de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications*. Recueil Dalloz 1991

CHAUVIN, Edouard et VADILLO, Florian. *La loi n° 2015-912 du 24 juillet 2015 « relative au renseignement » au secours de la protection pénale des systèmes de données*. Revue Lamy Droit de l'Immatériel, 1^{er} janvier 2016, 122

CHAVENT-LECLERE, Anne-Sophie. *La surveillance : une pratique encadrée ? renseignement, écoute, vidéo-protection...*, Procédures n°1, Janvier 2016

CHOPIN, Olivier. *Renseignement, sécurité et libertés fondamentales*, in *Le droit du renseignement*. 8 février 2019

CLEMENT, Eloi. *Le juge et l'espion*, AJ Pénal 2021

COEURET, Alain, *Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications*, RTD Civ, 1991

COTTEREAU, Marc. *Le « super fichier » des enquêtes administratives passe le contrôle de proportionnalité du Conseil d'Etat*. AJDA 2019

COTTERET, Jean-Marie. *Les fichiers de police et de renseignement en France*, Rapport de recherche 21, CF2R, octobre 2017

DE GUBERNATIS, Jean-Baptiste et MARTIN, Mathilde. *La loi relative au renseignement : la victoire de la peur sur l'idéal de protection des droits et libertés ?*, Les Cahiers Portalis, vol. 3, n° 1, 2016, p. 75 à 85

DEBET, Anne. *Croisement d'Hopsyweb et du FSPRT : l'interconnexion réalisée entre les deux traitements est un traitement intéressant la sûreté de l'Etat*. Communication Commerce électronique n° 6, Juin 2020, comm. 51

DELABIE, Lucie. *CRISTINA sous l'œil du Conseil d'Etat : les fichiers classés secret défense sont sous contrôle*, AJDA 2010

DELARUE, Jean-Marie. *Le renseignement pénitentiaire*. *Après-demain*, 2018/1 (n° 45, NF), p. 7 à 9

DELARUE, Jean-Marie. *Renseignement et sphère privée*, Archives de politique criminelle 2021/1 (n° 43), p 73 à 89

DELON, Francis. *La Commission nationale de contrôle des techniques de renseignement*, in *Actes du colloque organisé par l'Académie du renseignement à l'Ecole militaire*. 8 février 2019

DEPRAU, Alexis, *FPR et FSPRT : quel fichier pertinent pour le suivi des radicalisés ?*, CF2R, Tribune libre n° 86, Janvier 2020

DESAULNAY, Olivier. *Le renseignement français n'est plus hors-la-loi – Commentaire de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement*. Droit pénal n° 9, Septembre 2015

DOUAD, Emmanuel. *Décrets en matière de renseignement territorial*, Dalloz IP/IT 2021

DRM. *Intelligence artificielle et renseignement militaire*, Revue Défense Nationale, 2019/5 (N° 820)

DUMENIL, Gabriel. *La nécessité urgente d'encadrer procéduralement la mesure de cyber-infiltration*. Droit pénal n° 9, Septembre 2018, étude 22

EDDAZI, Fouad. *La responsabilité de l'Etat en matière de renseignement : affirmation et construction d'un régime*. Droit Administratif n° 11, novembre 2017, étude 16

FAUVARQUE-COSSON, Bénédicte. *Les données et la loi française*, in CNCIS, 23^{ème} rapport d'activité 2014-2015

FORCADE, Olivier. *Retour historique sur les institutions et les pratiques du renseignement français de 1991 à 2015*. in Le droit du renseignement, Actes du colloque organisé par l'Académie du renseignement à l'Ecole militaire, le 8 février 2019

FRAYSSINET, Jean. *L'accès aux données nominatives des fichiers des renseignements généraux*, Communication Commercer électronique n° 10, Octobre 2002, chron. 23

FRAYSSINET, Jean. *Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux*, Recueil Dalloz 1992

FRIEDRICH, Clemmy, *Compétence du Conseil d'Etat en matière de renseignement : une délimitation restrictive*, La Semaine Juridique Administrations et Collectivités territoriales n° 46, 20 novembre 2017

GAUTRON, Virginie. et MONNIAUX, David. *De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme*, Archives de politique criminelle, vol 38, n° 1, 2016

GAUTRON, Virginie. *Une mémoire policière hypertrophiée : la fin du droit à l'oubli ?*. Les Cahiers de la Justice, vol 4, n° 4, 2016, pp. 607-617

GAUTRON, Virginie. *Usages et mésusages des fichiers de police : la sécurité contre la sûreté ?*. AJ Pénal 2010, p.266

GONOD, Pascale. *Loi du 24 juillet 2015 relative au renseignement : quels contrôles ?*. Procédures n° 11, novembre 2015, étude 10

GOTTOT, Salomé. *Renseignement : premières décisions de la formation spécialisée du Conseil d'Etat*. AJDA 2017. 581

GOZZI, Marie-Hélène. *Sed quis custodiet ipsos custodes ? A propos de la loi du 24 juillet 2015 relative au renseignement*, La Semaine Juridique Edition Générale n° 38, 14 septembre 2015

GUERRIER, Claudine. *La CNCTR, une rupture ou une continuité avec la CNCIS ?*, Revue Le Lamy Droit de l'immatériel, n° 117, 1er juillet 2015

GUERRIER, Claudine. *Les interceptions et la loi de programmation militaire*. Revue Le Lamy Droit de l'immatériel, n° 104, 1^{er} mai 2014

GUERRIER, Claudine. *PRISM est-il conforme au droit ?*. Revue Lamy Droit de l'immatériel, n° 97, 1^{er} octobre 2013

HENRARD, Olivier. *Accès aux données de connexion, blocage et déréférencement des sites : l'administration pourra agir sans recourir au juge. Observations sous Conseil d'État*, 12 février 2016, n° 388134 et n° 388255, Association French Data Network et autres et Conseil d'État, 15 février 2016, n° 389140 et n° 389896, Association French Data Network et autres, Dalloz IP/IT 2016

KOUBI, Geneviève. *Cadences sécuritaires : des fichiers de renseignements extensibles*, La Semaine Juridique Administrations et Collectivités territoriales n° 3, 18 janvier 2021, act. 33

KOUBI, Geneviève. *Décret PASP, GI-PASP. Précisions sur la donnée « origine géographique »*, site internet Droit cri-TIC, 11 mai 2013

KOUBI, Geneviève. *Le « méga-fichier » des titres électroniques sécurisés*, La Semaine Juridique Administrations et Collectivités territoriales n° 47, 28 novembre 2016

KOUBI, Geneviève. *Les données à caractère personnel, outil des services de renseignement*. La Semaine Juridique Administrations et Collectivités territoriales n° 46, 9 novembre 2009

LAFOUASSE, Fabien. *Fasc. 1210 : Droit du renseignement numérique*, JurisClasseur Communication. 1^{er} janvier 2022

LATOUR, Xavier. *La première injonction d'effacement de données dans un fichier intéressant la sûreté de l'État : une victoire à la Pyrrhus ?*, La Semaine Juridique Edition Générale n° 23, 5 Juin 2017

LATOUR, Xavier. *La loi relative au renseignement : un Etat de surveillance ?*. La Semaine Juridique Administrations et Collectivités territoriales n° 40, 5 octobre 2015

LATOUR, Xavier. *Les fichiers PNR et les transporteurs aériens internationaux*, Annuaire 2018 du droit de la sécurité et de la défense. Mare et Martin, 2018

LATOUR, Xavier. *Premiers enseignements sur le contrôle juridictionnel des activités de renseignement*, La Semaine Juridique Edition Générale n° 46, 14 novembre 2016, 1199

LATOUR, Xavier. *Sécurité intérieure : un droit « augmenté » ?*. AJDA 2018. 431

LAZERGES, Christine et HENRION-STOFFEL, Hervé. *Politique criminelle, renseignement et droits de l'homme*, RSC, 2015, p. 761

LE BOT, Olivier. *Chronique de contentieux administratif. Décisions d'avril à juin 2021*. La Semaine Juridique Administrations et Collectivités territoriales n° 36, 6 septembre 2021, 2260

LE BOT, Olivier. *Le contentieux du renseignement devant la formation spécialisée du Conseil d'Etat*, RDFA 2017

LEFEBVRE Paul, *Officier*. in Dictionnaire du renseignement. Perrin, 2018, pp. 569 à 571

- LEPRI, Charlotte. *Les services de renseignement en quête d'identité : quel rôle dans un monde globalisé ?*. Géoéconomie, vol. 45, no. 2, 2008, pp. 33-53
- MAFART, Jean, *Agent*, in Dictionnaire du renseignement. Perrin, 2018, pp. 37 à 40
- MAFART, Jean, *Espionnage*, in Dictionnaire du renseignement. Perrin, 2018, pp. 348-359
- MAFART, Jean. *EDVIGE*, in Dictionnaire du renseignement, Paris, Perrin, 2018
- MAFART, Jean. *Fichier*, in Dictionnaire du renseignement. Perrin, 2018
- MARINO, Laure. *Surveillance du net : un Patriot Act à la française ?* Recueil Dalloz 2014
- MARTHINET, Laurent. *Contentieux de l'accès indirect aux fichiers : sortie de l'impasse ?*, AJDA 2016
- MASTOR, Wanda. *La France, Etat de surveillance ?*. AJDA 2015
- MAUGUE, Christine. *Communication des fichiers des renseignements généraux*, AJDA 2003
- MAUPIN, Emmanuelle. *Censure partielle de l'article L. 863-2 du code de la sécurité intérieure*. AJDA 2021
- MEILLAN, Eric. *Le renseignement intérieur : pour l'efficacité dans la démocratie*. Droit pénal n° 7-8, juillet 2016, étude 15
- MICHALON, Barthélémy, et PUYBAREAU, Benjamin. *Secret d'État et secret des sources : comment des journalistes enquêtent-ils sur le renseignement en France ? : Entretiens avec Jean Guisnel et Jacques Follorou*. Cultures & Conflits, vol. 114-115, no. 2-3, 2019, pp. 227-262
- MILANO, Laure. *Surveillance sur le net : du nouveau avec le décret du 24 décembre 2014*. Recueil Dalloz 2015
- MINET, Charles-Edouard. *La responsabilité de l'Etat envers les victimes d'actes de terrorisme à raison des carences des services de renseignement n'est engagée qu'en cas de faute lourde*. La Semaine Juridique Administrations et Collectivités territoriales n° 51-52, 26 décembre 2018, 2347
- MONTECLER, Marie-Christine de. *Techniques de renseignement : quand le Conseil d'Etat invite la CJUE à revoir sa jurisprudence*, Dalloz actualité. 7 septembre 2018, p. 1586
- PARIZOT, Raphaële. *Surveiller et prévenir... à quel prix ?*. La Semaine Juridique Edition Générale n° 41, 5 octobre 2015
- PETIT-PREVOST-WEYGAND, Eloïse. *L'activité extraterritoriale des services de renseignement numérique : recherche de solutions technico-juridiques de protection des données*, Journal du droit international (Clunet) n° 3, juillet 2021, var. 7

PETTITI, Louis-Edmond., *A propos de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications*, AJDA 1992

POIROT Jérôme, *ROSO*, in Dictionnaire du renseignement. Perrin, 2018, pp. 677-681

POIROT Jérôme. *Biométrie*, in Dictionnaire du renseignement. Perrin, 2018

POIROT Jérôme. *Intelligence artificielle*, in Dictionnaire du renseignement, Perrin, 2018

PRADA-BORDENAVE, Emmanuelle. *Le contrôle juridictionnel : un contrôle précisément défini par le législateur et confié à une formation spécialisée du Conseil d'Etat*, in Le droit du renseignement, Actes du colloque organisé par l'Académie du renseignement à l'Ecole militaire, 8 février 2019

PRADEL, Jean. *Un exemple de restauration de la légalité criminelle : le régime des interceptions de correspondances émises par la voie des télécommunications*. Recueil Dalloz 1992

QUEMENER, Myriam. *Les dispositions en lien avec le numérique de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme*. Dalloz IP/IT 2017

RAPAILLE, Guy. *Approche comparée des droits du renseignement (Belgique/Europe)*, in Le droit du renseignement, Actes du colloque organisé par l'Académie du renseignement à l'Ecole militaire, le 8 février 2019, p. 47 et suivantes

REES, Marc. *La loi sur le renseignement ou le grand méchant flou*. Revue Le Lamy Droit de l'immatériel, n° 118, 1^{er} août 2015

ROUSSEAU, Pierre et ROUSSEAU, François. *Prévention d'actes de terrorisme et renseignement. Commentaire de la loi n° 2021-998 du 30 juillet 2021*, Droit pénal n° 10, octobre 2021, étude 18

SAFI, Farah. *La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Entre pérennisation et extension de l'exception...*, La Semaine Juridique Edition Générale n° 40, 4 octobre 2021, 1012

SCHMITZ, Julia. *Le juge administratif et le contentieux du droit d'accès indirect aux fichiers de renseignement*. AJDA 2018

THOMAS-TAILLANDIER, Delphine. *Le nouveau fichier national des auteurs d'infractions terroristes*. AJ Pénal 2015

TIBERE, Clément. *Enigma*, in Dictionnaire du renseignement. Perrin, 2018

TOUILLIER, Marc. *La loi sur le renseignement traduit-elle l'émergence d'une procédure « para-pénal » ?*, in *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*. Janvier 2016, Nanterre, France, p. 159 à 176

URVOAS, Jean-Jacques. *Était-il tolérable que la France soit le seul État européen où les services de renseignement agissaient en dehors de tout cadre juridique ?*, La Semaine Juridique Administrations et Collectivités territoriales n° 40, 5 Octobre 2015, 2285

VADILLO, Florian. *Quand l'Etat de droit rencontre l'Etat secret : cadre et garanties du recours aux techniques de recueil de renseignement*, in Le droit du renseignement, 8 février 2019

VADILLO, Florian. *Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?*, Les Cahiers de la sécurité, n° 47, février 2020

VADILLO, Florian. *Une seconde loi renseignement ? Pour une main tremblante mais des idées claires*, Livret n° 12, L'Hétairie, 9 mars 2020

VEDEL Renaud. *Les contrôles internes*, in Le droit du renseignement, Actes du colloque organisé par l'Académie du renseignement à l'Ecole militaire, 8 février 2019

VEDEL, Renaud. *Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure*, AJ Pénal 2007

VERPEAUX, Michel. *La loi sur le renseignement, entre sécurité et libertés, à propos de la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015*. La Semaine Juridique Edition Générale n° 38, 14 septembre 2015, doct. 981

WARUSFEL, Bertrand. *La légalisation du renseignement en France (1991-2015)*, in Laurent Sébastien & Warusfel Bertrand, Transformations et réformes de la sécurité et du renseignement en Europe, Presses Universitaires de Bordeaux, 2016

WARUSFEL, Bertrand. *Contraintes juridiques et culture du secret, comme freins à l'échange de données de sécurité en Europe*, Intervention au colloque sur l'échange de données dans l'espace de liberté, de sécurité et de justice de l'Union européenne (CESICE, Université Grenoble-Alpes, 18 novembre 2016)

WARUSFEL, Bertrand. *Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement*, in Le droit du renseignement, 8 février 2019, p. 75 et suivantes

WARUSFEL, Bertrand. *Justice et renseignement dans la lutte contre la radicalisation violente*, AJ Pénal 2018

WARUSFEL, Bertrand. *Le cadre juridique incertain des actions spéciales*, publication sur le blog Hestia.hypothèses.org, 9 mars 2016

WARUSFEL, Bertrand. *Le renforcement du cadre juridique des services de renseignement*, L'ENA hors les murs, juin 2014

WARUSFEL, Bertrand. *Le renseignement, dimension majeure de l'action publique dans une société d'information*, in Le renseignement contemporain – Aspects politiques et juridiques, Éditions L'Harmattan, 2003

WARUSFEL, Bertrand. *Les enjeux du nouveau cadre juridique du renseignement*, 3^{ème} colloque annuel de l'Association française de droit de la sécurité et de la défense (AFDSD), septembre 2015

WARUSFEL, Bertrand. *Quelles réformes pour le droit du renseignement ?*, in Annuaire 2021 du droit de la sécurité et de la défense, Mare & Martin, 2021

B. Droit international et européen et surveillance numérique

ALLAND, Denis. *Les 100 mots du droit international*, points 50. *Ingérence (non-ingérence)* et 53. *Intervention*. Presses Universitaires de France, 2021, p 65 et 66 et p. 69 et 70

ANDRIANTSIMBAZOVINA, Joël. *La conception des libertés par le Conseil constitutionnel et par la Cour européenne des droits de l'homme*. Les nouveaux cahiers du Conseil constitutionnel n° 32, juillet 2011

AZOULAI, Loïc et RITLENG, Dominique. *L'État, c'est moi. Le Conseil d'État, la sécurité et la conservation des données*, RTD Eur., 2021, p.349

BARTOLUCCI, Mattéo. *Le Conseil d'État acte la conservation générale et indifférenciée des données de connexion*. La Semaine Juridique Administrations et Collectivités territoriales n° 28, 12 juillet 2021, 2223

BENLOLO-CARABOT, Myriam. *Chronique Droit pénal de l'Union européenne - Protection des données personnelles, lutte contre le terrorisme. La CJUE confrontée à la surveillance de masse*, RTD Eur. 2017, p.884

BERTRAND, Brunessen. *Chronique Droit européen du numérique : Les enjeux de la surveillance numérique*. RTD Eur. 2021, p.175

BERTRAND, Brunessen. *Chronique Droit européen du numérique, Les précisions sur l'interprétation et l'application du régime de l'e-privacy*, RTD Eur. 2022, p.481

BERTRAND, Brunessen. et SIRINELLI, Jean. *Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle*, Dalloz IP/IT, 2021, p.408

BERTRAND, Brunessen. *La souveraineté numérique européenne : une « pensée en acte » ?*, RTD Eur. 2021 p.249

BERTRAND, Brunessen. *L'audace sans le tact : jusqu'où la Cour de justice peut-elle aller trop loin ?*, Dalloz IP/IT 2021, p.468

BONNEVILLE, Philippe. GANSER, Christian. MARKARIAN, Sophie et ILJIC, Anne. *Chronique de jurisprudence de la CJUE*, AJDA 2021, p. 387

BONNEVILLE, Philippe. GANSER, Christian. MARKARIAN, Sophie et ILJIC, Anne. *Chronique de jurisprudence de la CJUE*, AJDA 2022, p.1675

BRUN Olivier, *Union européenne*, in Dictionnaire du renseignement. Perrin, 2018, pp. 801-804

BUISSON, Jacques. *Données de connexion, conservation et accès : la primauté du droit de l'Union réaffirmée*, Procédures n° 10, Octobre 2022, étude 11

CAPRIOLI, Eric A. *La CEDH invalide partiellement l'ancien système britannique de surveillance électronique*. Communication Commerce électronique n° 1, Janvier 2019, comm. 5

CAPRIOLI, Eric A. *La CEDH valide le contrôle des messages professionnels*. Communication Commerce électronique n° 4, Avril 2016, comm. 37

CASSIA, Paul, *Le Frexit sécuritaire du Conseil d'Etat*, billet de blog, Le Club Mediapart, 23 avril 2021

CHEVALLIER-GEYERS, Constance. in *L'échange de données dans l'Espace de liberté, de sécurité et de justice de l'Union européenne*. Mare & Martin, 2017

CORREIA, Vincent. *A propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens*. Communication Commerce électronique n° 6, Juin 2018, étude 10

DANIS-FATÔME, Anne. *Arrêt Schrems II : sauvetage de façade des « clauses contractuelles types » mais invalidation du bouclier de protection des données*. Communication Commerce électronique n° 11, Novembre 2020, comm. 83

DANIS-FATÔME, Anne. *Dispositif de surveillance des personnes versus droit à la protection des données à caractère personnel*, Communication Commerce électronique n° 7-8, Juillet 2022, comm. 52

DANIS-FATÔME, Anne. *Surveillance de masse – Sécurité nationale et protection des données : quelle articulation ?*, Communication Commerce électronique n° 9, Septembre 2021, comm. 66

DE TERWANGNE, Cécile. *L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt La Quadrature du Net de la Cour de justice de l'Union Européenne*. Revue trimestrielle des droits de l'Homme, vol. 129, no. 1, 2022, pp. 3-27

DELCHER, Emilie. *La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ?*. RDP, mai 2022, p. 845

DERIEUX, Emmanuel. *Internet et protection des données personnelles*, Revue Le Lamy Droit de l'immatériel. N° 38, 1er mai 2008

DEROUDILLE, Alexis. *L'exploitation généralisée et indifférenciée des données de connexion en question*. Revue de l'Union européenne, 2022, p.332

DOUVILLE, Thibault et GAUDIN, Hélène. *Un arrêt sous le signe de l'exceptionnel*, Recueil Dalloz, 2021, p. 1268

DUBUISSON, François. *La Cour européenne des droits de l'homme face à la surveillance de masse*. Revue trimestrielle des droits de l'homme, 2022/1 (N° 129), p. 123 à 141

DUPONT-LASSALLE, Julie. *La subsidiarité juridictionnelle, instrument de l'intégration communautaire ?*. Droit et société, vol. 80, no. 1, 2012, pp. 47-71

GROSSHOLZ, Caroline. *L'avenir incertain d'un instrument de lutte contre le terrorisme : l'exploitation des données de connexion*, La Semaine Juridique Administrations et Collectivités territoriales n° 27, 10 juillet 2017, 2177

GUILLAUMIN, Béatrice. « *Étude comparée des jurisprudences de la CEDH et de la CJUE : vers la consécration d'un jus commune européen du renseignement ?* », Études françaises de renseignement et de cyber, vol. 1, no. 1, 2023, pp. 23-37

HAFTTEL, Bernard. *Transferts transatlantiques de données personnelles : la Cour de justice invalide le Safe Harbour et consacre un principe de défiance mutuelle*. Recueil Dalloz 2016 p.111

HOURSON, Sébastien. « *Données passagers* » : le contrôle de la machine, Droit administratif n° 8-9, Août 2022, alerte 105

ILIOPOULOU-PENOT, Anastasia. *La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué*. La Semaine Juridique Edition Générale n° 24, 14 juin 2021, 659

KELLER, Jonathan. *L'exportation de systèmes de surveillance informatique par les sociétés privées européennes vers les pays tiers*. La Revue des droits de l'homme [En ligne], 11 | 2017, mis en ligne le 16 janvier 2017

LAFOUASSE, Fabien. *Droit international du renseignement*. JurisClasseur Communication, Fascicule 1200, 2018

LAFOUASSE, Fabien. *Le droit du renseignement : un droit conforme aux traités internationaux*, in *Le droit du renseignement*. Actes du colloque organisé par l'Académie du renseignement à l'Ecole militaire, 8 février 2019, p. 187 à 199

LAURENT, Sébastien. Et KHELOUFI, Maxime. *Les normes juridiques internationales applicables aux communications individuelles : les enjeux du « secret des correspondances » et des « données personnelles »*, Programme « UTIC France-Europe », IRM, Université de Bordeaux, Livrable n° 7 v. 10, 28 février 2018

LE BONNIEC, Nina. *La Cour européenne des droits de l'homme face aux nouvelles technologies de l'information et de communication numériques*. RDLF 2018, chron. n° 5

LE BONNIEC, Nina. *L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne : une délicate conciliation entre sécurité nationale et sécurité numérique*. RTD Eur. 2018, p.617

LEVADE, Anne. *Le Conseil constitutionnel et l'Union européenne*, Cahiers du Conseil constitutionnel. Hors série – colloque du cinquantenaire, 3 novembre 2009

MALVERTI, Clément et BEAUFILS, Cyrille. *L'instinct de conservation*. AJDA, 2021, p. 1194

MATTATIA, Fabrice. *Données personnelles : la CJUE invalide le Privacy Shield*, La Semaine Juridique Administrations et Collectivités territoriales n° 36, 7 septembre 2020, act. 491

MAUBERNARD, Christophe. *Données personnelles et sécurité nationale : Big Brother can watch everybody, Les juridictions de l'Union européenne et les droits fondamentaux ; Chronique de jurisprudence (2020)*. Revue trimestrielle des droits de l'Homme 2021/3 (N° 127), p. 573 à 620

MAUBERNARD, Christophe. *Droits fondamentaux, Annuaire de droit de l'Union européenne*. 2021, p. 403 à 461

MAXWELL, Winston. *La CJUE dessine le noyau dur d'une future régulation des algorithmes*. Légipresse #388, décembre 2020, p.671

MEDHI, Rostane et BROSSET, Estelle. *De quoi le droit de l'Union est-il le nom ? À propos du droit de l'Union entendu comme le droit commun des Etats membres*. in B. Bonnet. *Traité des rapports entre ordres juridiques*, LGDJ, pp. 669-695, 2016

MONTECLER, Marie-Christine de. *Conservation des données : la guerre des juges n'aura pas lieu*, AJDA 2021, p.828

MONTECLER, Marie-Christine de. *La CEDH admet le principe de la surveillance électronique de masse*. AJDA 2021, p. 1060

MONTECLER, Marie-Christine de. *Publication des nouveaux décrets sur la conservation des données*, AJDA 2021, p.2133

MORENO, Carlos et MEDJAOUI, Khadija. *Dissension among the Courts : France and EU Personal Data Retention Standards*. Revue Internationale de la Compliance et de l'Éthique des Affaires n° 4, Août 2022, comm. 200

NAVARETTE, Inaki. *L'espionnage en temps de paix en droit international public*, in Canadian Yearbook of International Law/Annuaire Canadien De Droit International, 53, 1-65, 2016

PADOVA, Yann. *Le Safe Harbor est mort, vive le Privacy Shield ?*. Revue Lamy Droit de l'Immatériel, N° 127, 1er juin 2016

PELTIER, Frédéric et WIERRE, Clément., *L'acharnement thérapeutique de la justice sur les données de connexion des opérateurs de téléphonie*. La Semaine Juridique Edition Générale n° 17, 2 mai 2022, 544

SANTULLI, Carlo. *Droit administratif et droit international*, RFDA 2018

SAUVE, Jean-Marc. *L'autorité du droit de l'Union européenne : le point de vue des juridictions constitutionnelles et suprême*. Congrès du 25ème anniversaire de l'Académie de droit européen (ERA) à Trèves le 19 octobre 2017

SIMON, Denys. *Coup de tonnerre dans le monde du numérique. La Cour de justice prononce l'invalidité du « bouclier de protection de la vie privée » à propos des transferts de données personnelles vers les États-Unis*. Europe n° 8-9, Août 2020, étude 8

SIMON, Denys. *Protection des données*. Europe n° 8-9, Août 2022, comm. 265

SIMON, Denys. *Quadrature du Net. Des données juridiques complexes sur la conservation des données numériques*, La Semaine Juridique Edition Générale n° 21, 25 Mai 2021, doctr. 561

SIMON, Denys. *Retour des monologues juridictionnels croisés ? À propos de l'arrêt du Conseil d'État dans l'affaire « French Data »*. Europe n° 6, Juin 2021, étude 3

SVENDSEN, Adam D.M. *The globalization of intelligence since 9/11 : Frameworks and operational parameters*. Cambridge Review of International Affairs, mars 2008

TAMBOU, Olivia. *La condamnation relative des mesures de surveillances massives étatiques : une occasion manquée par la Cour européenne des droits de l'homme*. Blogdroiteuropéen, 2021

TINIERE, Romain. *Le contenu essentiel des droits fondamentaux dans la jurisprudence de la Cour de justice de l'Union européenne*. Cahiers de droit européen- CDE, Bruxelles : Larcier, 2020, pp.417

VERON, Noémie. *Le Conseil constitutionnel et la conservation des données de connexion : entre apaisement et perturbation du dialogue des juges*. Communication Commerce électronique n° 10, Octobre 2022, étude 18

VIANGALLI, François. *De la conservation des données de communication électronique aux fins de politique pénale ou de sécurité nationale au regard du droit européen*. Revue Lamy Droit de l'Immatériel, N° 192, 1er mai 2022

WARUSFEL, Bertrand. *Conservation des données et sécurité nationale au regard du droit de l'Union européenne*, in Annuaire 2022 du droit de la sécurité et de la défense, mare et martin, 2022, pp. 161-173.

C. Droit pénal, cybercriminalité et renseignement

AUDIBERT, Matthieu. *La pénétration du droit pénal dans l'espace privé. La captation de données informatiques*. Archives de politique criminelle, vol. 43, no. 1, 2021, pp. 91-103

BEAUSSONIE, Guillaume. *La dématérialisation de l'abus de confiance*. AJ Pénal 2017 p.215

BEAUSSONIE, Guillaume. *La place du droit pénal dans la lutte contre la cybercriminalité*. La Semaine Juridique Edition Générale n° 21, 25 Mai 2021, 538

BELLOIR, Philippe. *Le délit de collecte déloyale de données à caractère personnel à l'épreuve d'internet*. Revue Lamy Droit de l'Immatériel, N° 17, 1er juin 2006

CAPRIOLI, Eric A. *Atteinte à la e-réputation de l'entreprise et de ses salariés*. Communication Commerce électronique n° 10, Octobre 2015, comm. 85

CAPRIOLI, Eric A. *Collecte de données personnelles non protégées et extraction frauduleuse*. Communication Commerce électronique n° 2, Février 2018, comm. 16

CAPRIOLI, Eric A. *Condamnation pour abus de confiance d'un salarié ayant détourné des données professionnelles à des fins personnelles*. Communication Commerce électronique n° 2, Février 2015, comm. 17

CAPRIOLI, Eric A. *Condamnation pour maintien dans le STAD et vol de fichiers informatiques*. Communication Commerce électronique n° 9, Septembre 2015, comm. 74

CAPRIOLI, Eric A. *Le « recel » d'informations et des correspondances sanctionné*. Communication Commerce électronique n° 3, Mars 2008, comm. 46

CAPRIOLI, Eric A. *Le phishing saisi par le droit*. Communication Commerce électronique n° 2, Février 2006, comm. 37

CAPRIOLI, Eric A. *Licéité de la preuve d'une publication Facebook privée*. Communication Commerce électronique n° 12, Décembre 2020, comm. 94

CAPRIOLI, Eric A. *Sécurité des systèmes d'information et espionnage informatique*. Communication Commerce électronique n° 5, Mai 2012, comm. 58

CAPRIOLI, Eric A. *Usage frauduleux d'un logiciel keylogger*. Communication Commerce électronique n° 4, Avril 2018, comm. 30

CAPRIOLI, Eric A. *Usurpation d'identité par création d'adresses mails et de faux profils Facebook*. Communication Commerce électronique n° 1, Janvier 2015, comm. 9

CAPRIOLI, Eric A. *Validité du contrôle du contenu de messages envoyés depuis une messagerie personnelle*. Communication Commerce électronique n° 10, Octobre 2013, comm. 110

CAPRIOLI, Eric A., *L'aspiration d'un site sanctionnée sur le fondement de la fraude informatique*. Communication Commerce électronique n° 1, Janvier 2009, comm. 10

CHOPIN, Frédérique. *Les politiques publiques de lutte contre la cybercriminalité*. AJ Pénal, 2009, p. 101

CONTE, Philippe. *Atteinte à l'intimité de la vie privée. Notion d'intimité*, Droit pénal n° 7-8, Juillet 2020, comm. 130

DARSONVILLE, Audrey. *Le motif légitime dans l'infraction de trafic de moyens destinés à commettre des infractions en matière informatique*. Dalloz actualité, 14 décembre 2009

DAURY-FAUVEAU, Morgane. *Fasc. 20 : ATTEINTES AUX SYSTÈMES DE TRAITEMENT AUTOMATISÉ DE DONNÉES – C. pén., art. 323-1 à 323-8*, JurisClasseur Pénal Code, 22 octobre 2019

DE MAISON ROUGE, Olivier. *La longue reconnaissance juridique du vol de données*. Sécurité globale, vol. 12, no. 4, 2017, pp. 45-54

DETRAZ, Stéphane. *Application de l'abus de confiance à des informations*. La Semaine Juridique Edition Générale n° 11-12, 12 mars 2012, act. 322

DONNAT, Francis. *Contrôle des fichiers contenant des informations pénales ou civiles individuelles*. AJDA 2004 p.2228

DREYER, Emmanuel. *Accès frauduleux, indirect, mais certain, dans un STAD et détention du matériel le permettant*. RSC 2018, p.701

DREYER, Emmanuel. *Diversité des atteintes aux « STAD »*, Le Lamy droit pénal des affaires. 11/2020

DREYER, Emmanuel. *Infractions relevant du droit de l'information et de la communication*. Revue de science criminelle et de droit pénal comparé, vol. 3, no. 3, 2018, pp. 701-720

DREYER, Emmanuel. *Infractions relevant du droit de l'information et de la communication*. Revue de science criminelle et de droit pénal comparé, vol. 3, no. 3, 2020, pp. 641-662

FRANCILLON, Jacques. *De diverses variétés de piratages*. RSC 1998, p. 138

FRANCILLON, Jacques. *Fraudes informatiques. Introductions frauduleuses de données et intrusions illégales dans un système informatique (piratage de Greenpeace)*. RSC 2013 p.559

FRANCILLON, Jacques. *Infractions relevant du droit de l'information et de la communication*. Revue de science criminelle et de droit pénal comparé, vol. 4, no. 4, 2015, pp. 877-888

FRANCILLON, Jacques. *Infractions relevant du droit de l'informatique. La loi Informatique*. Fichiers et libertés du 6 janvier 1978 à l'épreuve de la jurisprudence pénale, RSC 1996 p.676

FRANCILLON, Jacques. *L'affaire du « faux site officiel » de Rachida Dati : une étape dans la lutte contre la cyberdélinquance*. RSC 2015 p.101

FRANCILLON, Jacques. *Piratage informatique. Révélation de failles de sécurité informatique*, « *Infractions relevant du droit de l'information et de la communication* ». Revue de science criminelle et de droit pénal comparé, vol. 1, no. 1, 2010, pp. 170-181

FRAYSSINET, Jean. *La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois*. LEGICOM, vol. 42, no. 1, 2009, pp. 23-33

GRIGUER, Merav. *Le point sur la lutte contre l'usurpation d'identité numérique*. Cahiers de droit de l'entreprise n° 4, Juillet 2011, prat. 20

HAAS, Gérard et DUBARY, Amanda. *Cybercriminalité : mais que fait la justice ?*. Revue Lamy droit des affaires, n° 168, 1er mars 2021

HARBULOT, Christian. *Étude de cas : L'affaire Michelin*. in Manuel d'intelligence économique. Presses Universitaires de France, 2012, pp. 319-326

LAVRIC, Sabrina. *Fadettes du Monde : condamnation pour collecte illicite de données personnelles*, Dalloz actualité, 17 avril 2014

LE CLAINCHE, Julien. *La Cour de cassation clarifie le régime des pourriels*, Revue Lamy Droit de l'Immatériel, N° 16, 1er mai 2006

LE CLAINCHE, Julien., *Liste noire de notaires : dernier acte ?*. Revue Lamy Droit de l'Immatériel, N° 30, 1er août 2007

LEGIPRESSE, *L'infraction d'usurpation d'identité numérique prévue par l'article 226-4-1 du code pénal s'applique aux personnes morales*, Légipresse N° 402, 13 avril 2022, p. 209

LEGRIS-DUPEUX, Chloé et RENAUD-CHOURAQUI, Eve. *Quelle réponse juridique face à l'augmentation exponentielle du développement des faux sites administratifs ?*, Revue Lamy Droit de l'Immatériel, N° 158, 1er avril 2019

LEPAGE, Agathe. *Affaire Bettencourt c/ Mediapart : suite et fin ?*. Communication Commerce électronique n° 3, Mars 2015, comm. 23

LEPAGE, Agathe. *Collecte déloyale de données personnelles sur Internet*. Communication Commerce électronique n° 9, Septembre 2006, comm. 131

LEPAGE, Agathe. *Déclaration d'inconstitutionnalité de l'article 421-2-5-2 du Code pénal*. Communication Commerce électronique n° 4, Avril 2017, comm. 35

LEPAGE, Agathe. *Fin de partie pour la répression du recel de fichiers provenant d'un site d'apologie d'actes de terrorisme*. Communication Commerce électronique n° 10, Octobre 2020, comm. 73

LEPAGE, Agathe. *Interprétation pas tout à fait stricte de l'article 226-1 du Code pénal*. Communication Commerce électronique n° 6, Juin 2010, comm. 66

LEPAGE, Agathe. *Le faux-jumeau de l'arrêt Nikon*. Communication Commerce électronique n° 7, Juillet 2005, comm. 121

LEPAGE, Agathe. *Par-delà le prosélytisme, la pénalisation des influences*. Essai d'une typologie des influences. Société, droit et religion 2017/1 (Numéro 7), p. 15 à 34

LEPAGE, Agathe. *Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel*. Droit pénal n° 3, mars 2005, étude 5

LEPAGE, Agathe. *Un an de droit pénal du numérique (oct. 2016 – sept. 2017)*. Droit pénal n° 12, décembre 2017, chron. 11

MALAUURIE-VIGNAL, Marie. *Réflexions sur la protection du patrimoine informationnel de l'entreprise contre le piratage économique*. Recueil Dalloz 2012 p.1415

MARINO, Laure. *Le secret des correspondances, tel un satellite...*, La Semaine Juridique Edition Générale n° 6, 4 Février 2009, II 10022

MARINO, Laure. *Protection pénale de la vie privée du salarié espionné par son employeur*. Recueil Dalloz 2003, p. 1533

MATTATIA, Fabrice. *Faut-il dépénaliser les hackers blancs ?*, Revue de science criminelle et de droit pénal comparé. vol. 4, no. 4, 2015, pp. 837-846

MATTATIA, Fabrice. *L'usurpation d'identité sur internet dans tous ses états*, Revue de science criminelle et de droit pénal comparé. vol. 2, no. 2, 2014, pp. 331-337.

MENDOZA-CAMINADE, Alexandra. *La protection pénale des biens incorporels de l'entreprise : vers l'achèvement de la dématérialisation du délit ?*. Recueil Dalloz 2015 p.415

MISTRETTA, Patrick. *Droit pénal médical*, Revue de science criminelle et de droit pénal comparé, vol. 2, no. 2, 2018, pp. 473-485

MISTRETTA, Patrick. *Le secret des correspondances, Molière et la tartufferies médicales*, RSC 2018 p.480

PERE, David. *L'arsenal répressif du phishing*. Recueil Dalloz 2006 p.2666

PEREIRA, Brigitte. *La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité*. Revue internationale de droit économique, vol. xxx, no. 3, 2016, pp. 387-409

QUEMENER, Myriam. *Cyberattaque : le point de vue du magistrat sur les actions en justice*, Dalloz IP/IT 2021 p.389

QUEMENER, Myriam. *Enquête dans le Darkweb*. Dalloz IP/IT 2017

QUEMENER, Myriam. *Fake news, infox, quelles réponses juridiques ?*, Dalloz IP/IT 2019 p.178

QUEMENER, Myriam. *La consultation de sites à caractère terroriste à l'épreuve de la liberté d'expression*, Dalloz IP/IT 2017 p.289

QUEMENER, Myriam. *Le terrorisme face au cyberspace*. AJ Pénal 2013

QUEMENER, Myriam. *Les données personnelles à l'ère du numérique, Quelle protection sur le plan pénal ?*, RDP 2016, p. 71

QUEMENER, Myriam. *Les techniques spéciales d'enquête en matière de lutte contre la cybercriminalité*. AJ Pénal 2015

QUEMENER, Myriam. *Radicalisation : quelles réponses juridiques ?*. Sécurité et stratégie, vol. 24, no. 4, 2016, pp. 41-45

RASCHEL, Evan. *Réflexion sur la pénalisation de la violation du secret des affaires*. Dalloz IP/IT 2018 p.675

ROUJOU DE BOUBÉE, Gabriel. CARE, Thierry et MIRABAIL, Solange. *Droit pénal*. Recueil Dalloz 2007 p.399

ROUSSEL, Bruno. *Droit de se taire et investigations numériques : l'accès aux ressources numériques d'une personne visée par une enquête*, Revue Lamy Droit de l'Immatériel, N° 176, 1er décembre 2020

ROUSSEL, Gildas. *Déloyauté du recueil d'adresses électroniques sur Internet par l'utilisation d'un logiciel*. AJ Pénal 2006 p.260

SAINT-PAU, Jean-Christophe. *L'enregistrement clandestin d'une conversation*. Droit pénal n° 9, Septembre 2008, étude 17

SAINT-PAU, Jean-Christophe. *Vie privée : du lien entre délit principal et délit de conséquence*, La Semaine Juridique Edition Générale n° 23, 6 juin 2016, act. 658

SEUVIC, Jean-François. *Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques*. Articles 226-16 à 226-24 du code pénal, RSC 2004 p.916

VIANO, Emilio. C. *Section II - Droit pénal. Partie spéciale - Société de l'information et droit pénal. Rapport général* », Revue internationale de droit pénal, vol. 84, no. 3-4, 2013, pp. 311-334

WARUSFEL, Bertrand. *Procédure pénale et technologies de l'information : de la Convention sur la Cybercriminalité à la Loi sur la sécurité quotidienne*, Droit et Défense, 2002/

D. Cyberdéfense, cybersécurité, économie numérique et renseignement

ACHILLEAS, Philippe et BINET, Laurent Idest, *Un an de régulation du marché des communications électroniques*. Communication Commerce électronique n° 5, mai 2016, chron. 7

ACHILLEAS, Philippe. *La sécurité des réseaux 5G : un enjeu de souveraineté pour l'Europe et la France*, Communication Commerce électronique n° 12, Décembre 2020, étude 21

ARRIGO, Pascal. BLIN, Donatienne. *Publier les moyens d'exploiter la vulnérabilité d'un système informatique constitue un délit*. Gazette du Palais, n° 37, 6 février 2010, p. 32

BANNELIER, Karine. CHRITAKIS, Theodore. *Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la Revue Stratégique de cyberdéfense de la France et le projet de loi ACDC aux États-Unis*. Stratégique, vol. 117, no. 4, 2017, pp. 99-118

BERTRAND, Brunessen. *Chronique Droit européen du numérique - La nouvelle approche de la cybersécurité européenne*. RTD Eur., 2021, p. 155

BLISSON, Laurence. *Petits vices et grandes vertus du chiffrement*, Délibérée, vol. 7, no. 2, 2019, pp. 56-59

BOMBAL, Sébastien. LE BIHAN, Victor. *Planifier et conduire les opérations numériques*. in La Cyberdéfense. Politique de l'espace numérique. Armand Colin, 2018, pp. 218-232

BOMONT, Clotilde. *Maîtriser le cloud computing pour assurer sa souveraineté*. in La Cyberdéfense. Politique de l'espace numérique. Armand Colin, 2018, pp. 91-97

BOULOC, Bernard. *Communication d'une faille dans un système informatique*. RTD Com. 2010, p. 441

BROMLEY, Mark. *Export controls, human security and cyber-surveillance technology: examining the proposed changes to the EU dual-use regulation*, Stockholm International Peace Research Institute, December 2017

C MURPHY, Cian. *The Crypto-Wars myth : The reality of state access to encrypted communications*. Common Law World Review, 49(3-4), 2020, 245-261

CAMMILLERI-SUBRENAT, Anne. *Téléservices et confidentialités en matière de défense*. Revue française d'administration publique, vol. 146, no. 2, 2013, pp. 325-337

CAPRIOLI, Éric A. *Les notifications de violation de données à caractère personnel et le droit : des questions en suspens*, Communication Commerce électronique n° 5, Mai 2010, comm. 54

CAPRIOLI, Éric A. *La loi de programmation militaire et sécurité de l'information*, Communication Commerce électronique n° 5, Mai 2014, comm. 50

CAPRIOLI, Éric A. *La nouvelle réglementation sur la cryptologie : un cadre juridique enfin complet*. Communication Commerce électronique n° 10, Octobre 2007, comm. 128

CATTARUZZA, Amaël. *Chapitre 4. Les enjeux de souveraineté de l'espace numérique. Quelle souveraineté pour l'espace numérique ?* », in La Cyberdéfense. Politique de l'espace numérique. Armand Colin, 2018, pp. 83-91

CATTARUZZA, Amaël. DANET, Didier. TAILLAT, Stéphane. « *Introduction* », in *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, 2018, pp. 4-13

CENTER FOR CYBER AND HOMELAND SECURITY. *Into the gray zone, the private sector and active defense against cyber threats*, The George Washington University, October 2016

CHAUVEL, Louis-Marie. *Chronique Action extérieure de l'UE : La refonte en demi-teinte du règlement relatif aux biens à double usage*. RTD Eur. 2021, p.705

CHAUVEL, Louis-Marie. HAMONIC, Anne. *Chronique Action extérieure de l'UE - La diversification des régimes thématiques de mesures restrictives*. RTD Eur., 2019, p.746

CHOPIN Olivier et OUDET Benjamin. « *Chapitre 6. Sources ouvertes, cyber, data : le renseignement et la révolution de l'information* », in *Renseignement et sécurité*, Armand Colin, 2019, pp. 169-194

DELERUE, François, GÉRY, Aude. *Chapitre 3. Les aspects juridique et stratégique de la cyberdéfense*. in *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, 2018, pp. 61-70

DELERUE, François, GÉRY, Aude. *Le droit international et la cyberdéfense*. in *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, 2023, pp. 93-104

DELERUE, François. DOUZET, Frédéric. GÉRY, Aude. *Les représentations géopolitiques du droit international dans les négociations internationales sur la sécurité et la stabilité du cyberspace*. Étude n° 75, IRSEM/EU Cyber Direct, novembre 2020

DELERUE, François. *Internationally Wrongful Cyber Acts : Cyber Operations Breaching Norms of International Law*, In *Cyber Operations and International Law*. Cambridge University Press, 2020

DELESSE, Claude. *La NSA, « mauvais génie » du cybermonde ?*, *Sécurité globale*, vol. 8, no. 4, 2016, pp. 67-104

DESFORGES, Alix. « *Souveraineté numérique et autonomie stratégique : la nécessaire clarification pour une ambition européenne.* » In *L'Europe de La Cybersécurité, Pour Une Liberté Sécurisée*, TransEuropeExperts pour le FIC 2020, p. 34 et 35

DESFORGES, Alix. *Séparation des fonctions offensive et défensive : l'originalité du modèle de cyberdéfense française remis en cause ?*. Chapitre 3, in *Conflits, crimes et régulations dans le cyberspace*, Volume 4. Série Cybersécurité, ISTE, 2021, p. 65 à 87

DOUZET, Frédéric. SAMAAAN, Jean-Loup. DESFORGES, Alix. *Les pirates du cyberspace*. Hérodote, vol. 134, no. 3, 2009, pp. 176-193

DOUZET, Frédérick. TAILLAT, Stéphane. « *Chapitre 6. Les enjeux de politique internationale. L'affirmation du leadership américain* », in *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, 2018, pp. 111-122

FERAL-SCHUHL, Christiane. *Vers un renforcement de l'obligation de déchiffrement ?* Section 5 - Déchiffrement des moyens de cryptologie (532.81 - 532.84). Chapitre 532 - Régime actuel de la cryptologie. in *Praxis Cyberdroit*, 2020-2021

FITZJEAN OCOBHTHAIGHT, Alexis. *Le cloud et la souveraineté numérique dans le nouveau monde*. *Revue pratique de la prospective et de l'innovation* n° 1, Avril 2021, dossier 2

FREDERICK.T, Davis et GUNKA, Charlotte. *Perquisitionner les nuages - CLOUD Act, souveraineté européenne et accès à la preuve dans l'espace pénal numérique*. *Revue critique de droit international privé*, vol. 1, no. 1, 2021, pp. 43-66

GAUDION, Amy C. *It's time to reform the U.S. Vulnerabilities Equities Process*. U.S. Army War College, September 2, 2021

GAUTIER, Louis. *Cyber : les enjeux pour la défense et la sécurité des Français*. *Politique étrangère*, vol., no. 2, 2018, pp. 29-42

GEORGELIN, Estéban. HOLEINDRE, Jean-Vincent. *Des ruses de guerre numériques ? Le hacking comme ressource stratégique dans les conflits contemporains*. *Quaderni*, vol. 103, no. 2, 2021, pp. 89-104

GERY, Aude. *Droit international et prolifération des cyberarmes*. *Politique étrangère*, vol., no. 2, 2018, pp. 43-54

GERY, Aude. *La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense*. *Les Champs de Mars*, vol. 30+s, no. 1, 2018, pp. 307-316

GÉRY, Aude. NOËL, Esther. *La recherche de son autonomie stratégique numérique par l'Union européenne*. *Revue de l'Union européenne*, 2023, p. 152

GOLIARD, François. *Télécommunications et réglementation française du cryptage*. *Recueil Dalloz* 1998, p. 120

GOUPY, Marie. *La bienveillante neutralité des technologies d'espionnage des communications : le cas tunisien*. *Cultures & Conflits*, 93 | 2014, 109-124

GUIFFARD, Jonathan. « *Sur les rives du Potomac, le centre du système de renseignement et de cyberdéfense des États-Unis* », *Études françaises de renseignement et de cyber*, (N° 2), 1, 2024, pp.43-57

HILARY, Gilles. *WannaCry and the Diffusion of Zero Day Exploits*. CREOGEN Research Note no. 25, 2017

HOURSON, Sébastien. *La lutte administrative contre la menace informationnelle*. *Droit Administratif* n° 10, Octobre 2021, alerte 146

HUREL, Benoit. LEMONIER, Vincent. *L'enquête pénale à l'épreuve du chiffrement*. Délibérée, vol. 4, no. 2, 2018, pp. 53-57

JARVIS, Craig. *Crypto Wars : The fight for privacy in the digital age : a political history of digital encryption*. CRC Press, 2021

JOMNI, Adel. *Le RGPD : un atout ou un frein pour la cybersécurité ?*, Dalloz IP/IT, 2019, p. 352

KANETAKE, Machiko. *The EU's dual-use export control and human rights risks : the case of cyber surveillance technology*. Eur. World. 2019. Vol. 3(1)

KLEIN, Roland. *Trimming Pegasus' Wings*. International Export Control Law and « Cyberweapons », Völkerrechtsblog, 27.10.2021

LAFOUASSE, Fabien. *L'enjeu des données personnelles et souveraines à l'aune d'un « droit international du renseignement » en formation*, Chapitre 7, in Conflits, crimes et régulations dans le cyberspace, Volume 4. Série Cybersécurité, ISTE, 2021, p. 145 à 165

LASCONIARIAS, Guillaume. TAILLAT, Stéphanne. *L'Otan et le domaine opérationnel cyber*. in La Cyberdéfense. Politique de l'espace numérique. Armand Colin, 2018, pp. 150-156

LATIL, Arnaud. *Les « portes dérobées » incompatibles avec le droit à la vie privée des utilisateurs de messageries cryptées*, Communication Commerce électronique n° 5, Mai 2024, comm. 5.

LAURENT, Sébastien-Yves. *Les Etats-Unis, les Etats et les faux semblants de la fin de l'internet mondial*, Chapitre 1, in Conflits, crimes et régulations dans le cyberspace, Volume 4, Série Cybersécurité, ISTE, 2021, p. 5 à 43

LAURENT, Sébastien-Yves. *Liberté et sécurité dans un monde anomique de données*, 22^{ème} rapport d'activité de la CNCIS, 2013-2014, p. 11 à 18

LEGRIS, Chloé. *Le lanceur d'alerte informatique, ce hacker incompris*. Revue Lamy Droit de l'Immatériel, N° 145, 1er février 2018

LEPAGE, Agathe. *La volonté d'information ne constitue pas, en soi, un motif légitime en matière de publication des vulnérabilités*. La Semaine Juridique Edition Générale n° 1-2, 11 janvier 2010, act. 19

LUZEAUX, Dominique. *Cloud souverain : souveraineté et résilience, ou confiance ?*. Revue Défense Nationale, vol. 855, no. 10, 2022, pp. 14-21

MACNISH, Kévin. *An End to Encryption ? Surveillance and Proportionality in the Crypto-Wars*, In : Henschke, Adam., Reed, Alastair. Robbins, Scott., Miller, Seumas. (eds) Counter-Terrorism, Ethics and Technology. Advanced Sciences and Technologies for Security Applications, 2021

MASSIT-FOLLEA, Françoise. *La « sécurité offensive », La régulation de l'internet : fictions et frictions*. In : Les débats du numérique, Paris : Presse des Mines, 2013

NORODOM, Anne-Thida. « *Souveraineté, Cybersécurité et Union Européenne.* » In *L'Europe de La Cybersécurité, Pour Une Liberté Sécurisée*, TransEuropeExperts pour le FIC 2020, p. 32 et 33

OBERDORFF, Henri. *La transformation numérique de l'administration publique*. RDP, septembre 2020, p. 1173

OBSERVATOIRE DU MONDE CYBERNETIQUE. *La révision de l'Arrangement de Wassenaar dans le domaine des logiciels d'intrusion et ses conséquences*. Lettre n° 70, Janvier 2018

OBSERVATOIRE DU MONDE CYBERNETIQUE. *Point juridique sur la publication de failles de sécurité*. Lettre n° 7 – juillet 2012, p. 11 à 13

PELLEGRINI, François et CANEVET, Sébastien. *Le droit du numérique : une histoire à préserver. Vers un Musée de l'Informatique et de la Société Numérique en France ?*, Conservatoire National des Arts et Métiers, Nov 2012, Paris, France. pp.61-76

PELLEGRINI, François. *Sécurité et numérique : Entre fantasmes d'efficacité et violations avérées des droits fondamentaux*. in *La sécurité : mutations et incertitudes*, Collection Colloques & Essais, Institut universitaire Varenne, 2019, pp.89-100

PERARNAUD, Clément. *Les contrôles aux exportations comme instruments de pouvoir dans la gouvernance de l'Internet*. Terminal [En ligne], 132-133 | 2022, mis en ligne le 28 février 2022

PERRAY, Romain. FERRANDO, Laetitia. *Les failles de sécurité : la CNIL met sa politique de sanction en ordre de marche*. Communication Commerce électronique n° 12, Décembre 2017, étude 20

POUPARD, Guillaume. *De la cryptographie à la sécurité numérique : une décennie et la suite*. Sécurité globale, vol. 19, no. 3, 2019, pp. 5-10

QUEMENER, Myriam. *Revue stratégique de cyberdéfense: cyberdéfense, cybersécurité, cybercriminalité, même combat*. Dalloz IP/IT 2018, p. 176

SCHMITT, Michael N. *Grey Zones in the International Law of Cyberspace*. 42:2 Yale Journal of International Law Online 1. October 18, 2017

SCHMITZ-BERNDT, Sandra. SCHIFFNER, Stefan. *Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR*. International Review of Law, Computers & Technology, 2021, vol. 35, N° 2, p. 101-115

SCHULZE Matthias. *Quo Vadis Cyber Arms Control ? A Sketch of an International Vulnerability Equities Process and a 0-Day Emissions Trading Regime*, Science Peace Security '19. *Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research* REUTER, Christian. ALTMAN, Jürgen. GOTTSCHKE, Malte. and HIMMEL, Mirko. (Editors). TUprints, Darmstadt, 2019

SCHULZE, Matthias. *Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016*. Media and Communication, 2017, Volume 5, Issue 1, Pages 54–62

SIBONY, Eric. *Qu'est ce que l'intelligence artificielle ?, Intelligence artificielle, un nouvel horizon : pourquoi la France a besoin d'une culture numérique ? Comprendre et débattre ses enjeux technologiques, économiques, légaux et éthiques*. Les Cahiers Lysias, juillet 2017

SIRVENT, Thomas. *La cryptographie, socle de la souveraineté numérique*, Revue Défense Nationale, vol. 855, no. 10, 2022, pp. 59-66

SUDRES, Arnaud. *Cyberespace et dimension stratégique de la force informatique*. Stratégique, vol. 117, no. 4, 2017, pp. 65-82

TAILLAT, Stéphane. *Un mode de guerre hybride dissymétrique ? Le cyberespace*. Stratégique, vol. 111, no. 1, 2016, pp. 89-106

TORRES, Chloé. *3 questions. Les failles de sécurité : quel régime juridique ?*, La Semaine Juridique Entreprise et Affaires n° 4, 22 Janvier 2015, 63

TREGUER, Félix. *De la dépêche secrète aux Crypto Wars (brève histoire politique du chiffrement)*. 2017, halshs-01649969

TREGUER, Félix. *Anonymat et chiffrement, composantes essentielles de la liberté de communication*, in VAN ENIS, Quentin. DE TERWANGNE, Cécile, *L'Europe des droits de l'homme à l'heure d'Internet*. Bruxelles, Bruylant, inPress, 2019

TRICAUD, Anne. *Vers une co-souveraineté nationale et européenne en matière de cybersécurité*. Revue Défense Nationale, vol. 855, no. 10, 2022, pp. 22-28.

TURK, Pauline. *La conservation des données, quels enjeux pour la souveraineté numérique ?*, La Semaine Juridique Administrations et Collectivités territoriales n° 50, 19 décembre 2022, 2348

TURK, Pauline. *Définition et enjeux de la souveraineté numérique*, Parole d'expert, Vie publique, 14 septembre 2020

URBAN, Lisa. *La vie privée révélée et la vulnérabilité exploitée – une approche comparée du piratage informatique en tant que méthode occulte d'enquête policière*. Archives de politique criminelle, vol. 43, no. 1, 2021, pp. 207-219

VAN DAALEN, O.L. VAN HOBOKEN, Joris. RUCK, Melinda. *Export control of cybersurveillance items in the new dual-use regulation : The challenges of applying human rights logic to export control*, Computer Law & Security Review. The International Journal of Technology Law and Practice, April 2023

VERDIER, Henri et ROLLAND, Léoanard. « *L'usage responsable des capacités commerciales de cyber-intrusion : une perspective diplomatique* », in CNCTR, 8^{ème} Rapport d'activité (2023), pages 175 à 179

VERON, Michel. *La diffusion d'informations présentant un risque d'utilisation à des fins de piratage*. Droit pénal n° 1, janvier 2010, comm. 3

WARUSFEL, Bertrand, *Dix ans de réglementation de la cryptologie en France : du contrôle étatique à la liberté concédée*. in Annuaire français de relations internationales, n° 1, 2000, pp. 657-661

WARUSFEL, Bertrand. *La cryptologie au cœur de la cybersécurité : enjeux et choix*. Revue de la Gendarmerie Nationale, 4ème trimestre 2015, p. 107 à 114

WARUSFEL, Bertrand. *La cyberdéfense, dimension numérique de la sécurité nationale*, Chapitre 5, in Conflits, crimes et régulations dans le cyberspace, Volume 4, Série Cybersécurité, ISTE, 2021, p. 106

WARUSFEL, Bertrand. *La transversalité du droit du numérique*, Études en l'honneur du Professeur Jérôme Huet, LGDJ, pp.412-423, 2017

WARUSFEL, Bertrand. *Technologies et sécurité : réguler pour reprendre le contrôle*, Cahiers de la sécurité et de la justice de l'INHESJ n° 50, 2021, p. 254 à 260

WATIN-AUGOUARD, Marc. *Cybermenaces et sécurité nationale*, in Le droit de la sécurité et de la défense en 2013. Presses Universitaires d'Aix-Marseille, 30 avril 2014, p. 297 à 312

WATIN-AUGOUARD, Marc. *La cybersécurité, enjeu de la souveraineté à l'ère numérique*. Dalloz IP/IT, 2021, p. 130

WATIN-AUGOUART, Marc *Entre sécurité et liberté, quel équilibre pour la défense et la sécurité de l'espace numérique ?*. in Annuaire 2018 du droit de la sécurité et de la défense, mare & martin, 2018, p. 115 à 140

WILSON THOMPSON, Andi, *Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter*, Lawfare blog, Wednesday, January 13, 2021

E. Autres

ALIX, Julie. *Chronique de politique criminelle*, Revue de science criminelle et de droit pénal comparé. vol. 2, no. 2, 2019, pp. 505-521

ALT, Eric. *De nouvelles protections pour les lanceurs d'alerte*, La Semaine Juridique Edition Générale n° 4, 23 janvier 2017, doct. 90

BENABOU, Valérie-Laure. *L'extension du domaine de la donnée*. LEGICOM, vol. 59, no. 2, 2017, pp. 3-17

BONNET, Julien et ROBLOT-TROIZIER, Agnès. *Chronique de droits fondamentaux et libertés publiques*. Les Nouveaux Cahiers du Conseil constitutionnel, vol. 55-56, no. 2-3, 2017, pp. 117-149

BOUCHET, Hubert. *La surveillance numérique au travail*. Hermès, La Revue, vol. 53, no. 1, 2009, pp. 85-90

BOURGEOIS, Matthieu et MOINE, Marion. *Réécriture de la loi informatique et libertés : encore des nouveautés*, Cahiers de droit de l'entreprise, janvier 2019, dossier 4

BRUN, Olivier. MOUTOUH, Hugues. *Désinformation*. in Dictionnaire du renseignement. Perrin, 2018, pp. 250-253

CANAS. Sophie. *L'influence de la fondamentalisation du droit au respect de la vie privée sur la mise en œuvre de l'article 9 du code civil*, Nouveaux Cahiers du Conseil constitutionnel n°48, Dossier : Vie privée, Juin 2015, p. 47 à 58.

CAPRIOLI, Eric A. *Contrôle par l'employeur des fichiers stockés sur l'ordinateur professionnel d'un salarié en son absence*. Communication Commerce électronique n° 5, Mai 2018, comm. 40

CAPRIOLI, Eric A. *Le régime des lanceurs d'alertes de sécurité dans la loi pour une République numérique*. Communication Commerce électronique n° 1, Janvier 2017, comm. 9

CARRIGOS-KERJAN, Mariel. *La tendance sécuritaire de la lutte contre le terrorisme*, Archives de politique criminelle. 2006/1 (n° 28)

CASAUX-LABRUNEE, Lise. *Vie privée des salariés et vie de l'entreprise*. Droit social n° 4, avril 2012

CASTEX, Lucien. *Le secret de la correspondance en ligne : dans le sillon des lettres missives*. Revue Lamy Droit de l'Immatériel, N° 137, 1er mai 2017

COUDERC, Agathe. *Renseignement technique et secret militaire : le Chiffre français pendant les premiers mois de la Grande Guerre*. Stratégique, vol. 105, no. 1, 2014, pp. 57-72

DAOUD, Emmanuel. MERCINIER, Emmanuel et NEIMAN, Juliette. *Loi du 30 juillet 2018 relative à la protection du secret des affaires : un apport utile mais insuffisant*. Revue Lamy droit des affaires, N° 147, 1er avril 2019

DE MAISON ROUGE, Olivier. *La surveillance et le contrôle au sein de l'entreprise : les limites de l'exercice posées par le Droit*. Sécurité et stratégie, vol. 21, no. 1, 2016, pp. 12-17

DE MAISON ROUGE, Olivier. *Le secret des affaires : la reconnaissance juridique d'un droit de l'information protégée*. Dalloz IP/IT 2018 p.659

DE MONTALIVET, Pierre. *Les objectifs de valeur constitutionnelle*, Cahiers du Conseil constitutionnel n° 20, juin 2006

DEBET, Anne. *Constitutionnalité des listes noires des supporters*. Communication Commerce électronique n° 9, Septembre 2017, comm. 75

DELPUECH, Michel. *Le rôle de l'Etat en matière de sécurité*. Revues des Juristes de Sciences Po n° 19, octobre 2020

DUBOUT, Edouard. *Le Conseil d'Etat, gardien de la sécurité*. RDLF, 2021, chron. n° 18

FRAYSSINET, Jean. *La loi relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ?*. Revue Le Lamy Droit de l'immatériel, N° 9, 1er octobre 2005

FRAYSSINET, Jean., *Les sites de notation (Note2be...) face au droit*. LEGICOM, vol. 43, no. 2, 2009, pp. 83-87

GARDIN, Alexia, *Géolocalisation du véhicule du salarié : quand finalité, proportionnalité et fiabilité font loi*. Revue de droit du travail 2015, p. 544

HARBULOT, Christian. *L'intelligence juridique et le droit des secrets d'affaires*. Manuel d'intelligence économique, Presses Universitaires de France, 2012, pp. 305-318

HERRAN, Thomas. *L'impact de la loi relative à la sécurité publique sur la distinction entre la police judiciaire et la police administrative*. AJ Pénal 2017

KALDOR, Mary. *La sécurité humaine : un concept pertinent ?*. Politique étrangère, vol., no. 4, 2006, pp. 901-914

LATOUR, Xavier. *La lutte contre les sites djihadistes et la liberté de communication*. La Semaine Juridique Administrations et Collectivités territoriales n° 7, 19 février 2018, 2056

LATOUR, Xavier. *La participation des personnes privées au contrôle des migrations en France*, AJDA 2019

LE CLAINCHE, Julien et LE METAYER, Daniel. *Données personnelles, vie privée et non-discrimination : des protections complémentaires, une convergence nécessaire*. Revue Lamy Droit de l'Immatériel, N° 90, 1er février 2013

MALLET-POUJOL, Nathalie. *La liberté d'expression sur l'internet : aspects de droit interne*. Recueil Dalloz 2007 p.591

MAYAUD, Yves. *Consultation de site internet : seconde censure*. Recueil Dalloz 2018 p. 97

MELIN, Matthieu et MELISON, David. *Salarié, employeur et données informatiques : brefs regards croisés sur une pièce à succès*. Revue Le Lamy Droit de l'immatériel, N° 23, 1er janvier 2007

MORANGE, Jean. *La Déclaration et la proclamation des droits de l'homme*. in Jean Morange éd., *La Déclaration des Droits de l'Homme et du Citoyen*. (26 août 1789). Presses Universitaires de France, 2002, pp. 11-54

OBSERVATOIRE DU MONDE CYBERNETIQUE. *Le New Space et la course à l'Internet spatial*, 7 septembre 2020

OBSERVATOIRE DU MONDE CYBERNETIQUE. *Nouvelles techniques de géolocalisation et risques cyber*, Lettre n°67, octobre 2017

QUEMENER, Myriam. *La géolocalisation : un outil de protection ou de surveillance ?*, Sécurité et stratégie, vol. 15, no. 4, 2013, pp. 11-17

QUEMENER, Myriam. *Présentation du décret du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (TES)*. Dalloz IP/IT 2017

SUTTER, Gérald. *Utilité et limites des objectifs de valeur constitutionnelle sur le plan contentieux*, Titre VII [en ligne], n° 8, Les catégories de normes constitutionnelles. avril 2022

TRUCHET, Didier. *Correspondance et communication*. Recueil Dalloz 2014 p. 2353

VIDAL NAQUET, Ariane. *La sécurité en droit constitutionnel : non-dit ou non-être ?*, *La sécurité en droit public*. Institut Universitaire Varenne, Colloques & Essais, 2018

WARUSFEL, Bertrand. « *Enjeux et limites de l'ouverture des données en matière de sécurité et de défense* », *Revue française d'administration publique*, vol. 167, no. 3, 2018, pp. 551-564

WARUSFEL, Bertrand. *Le contentieux de la sécurité nationale*, *Annuaire du droit de la sécurité et de la défense* 2018, mare & martin, p. 203 à 218

III. DOCUMENTATION INSTITUTIONNELLE

Classement par institutions et par ordres chronologiques

A. Institutions internationales et européennes

PNUD, *Rapport sur le développement humain de 1994*, Paris, Economica, 1994

PARLEMENT EUROPEEN. *Etude sur les programmes de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE*, septembre 2013

COMMISSAIRE AUX DROITS DE L'HOMME DU CONSEIL DE L'EUROPE, *La prééminence du droit sur l'internet et dans le monde numérique en général*, 2014

OMTZIGT, Pieter. *Les opérations de surveillance massive*, Rapport de la Commission des questions juridiques et des droits de l'homme, Assemblée parlementaire du Conseil de l'Europe, 18 mars 2015

KAYE, David. *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*. Conseil des droits de l'homme, 22 mai 2015

ENISA, *Good Practice Guide on Vulnerability Disclosure*, novembre 2015

CONSEIL DE L'EUROPE, *Surveillance de masse. Quel contrôle démocratique ?*, Conseil de l'Europe, « Hors collection », 2016

ENISA, *On the free use of cryptographic tools for (self) protection of EU citizens*, January 20, 2016

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update*, 20 octobre 2017

Déclaration conjointe par A. Pierucci, Présidente du Comité de la Convention 108 et J. -P. Walter, Commissaire à la protection des données du Conseil de l'Europe, « *Mieux protéger les personnes dans un contexte de flux international de données : la nécessité d'une supervision démocratique et effective des services de renseignement* », Strasbourg, 7 septembre 2020

UNODA. *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States*, UNODA, A/76/136, August 2021

B. Parlement national

• Délégation parlementaire au renseignement

URVOAS, Jean-Jacques. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, DPR, 18 décembre 2014

RAFFARIN, Jean-Pierre. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*. DPR, 25 février 2016

ADAM, Patricia et BAS, Philippe. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, DPR, 2 mars 2017

BAS, Philippe. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour 2017*, DPR, 12 avril 2018

BRAUN-PIVET, Yaël. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018*. Tome 1, DPR, 11 avril 2019

CAMBON, Christian. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, 11 juin 2020

DUMAS, Françoise et BUFFET, François-Noël. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021*. DPR, 1^{er} juillet 2021

BUFFET, François-Noël. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2021-2022*, DPR, 24 février 2022

- **Assemblée nationale**

GEST, Alain. *Rapport fait au nom de la commission d'enquête sur les sectes*, Assemblée nationale, 22 décembre 1995

GOUZES, Gérard. *Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Assemblée nationale, 9 janvier 2002

DIONIS DU SEJOUR, Jean. *Rapport sur le projet de loi (n° 528) pour la confiance dans l'économie numérique*. 1^{ère} partie, Assemblée nationale, 12 février 2003

NESME, Jean-Marc. *Rapport sur le projet de loi n° 905 autorisant l'approbation de la convention sur la cybercriminalité*, Assemblée nationale, 8 décembre 2004

MARSAUD, Alain. *Rapport fait au nom de la commission des Lois de l'Assemblée nationale sur le projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, 16 novembre 2005

DIARD, Éric, Rapporteur, et DRAY, Julien, corapporteur. *Rapport d'information sur la mise en application de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôle frontaliers*, Assemblée nationale, 5 février 2008

BATHO, Delphine et BENISTI, Jacques Alain. *Rapport d'information sur les fichiers de police*, Assemblée nationale, 24 mars 2009

BATHO, Delphine et BENISTI, Jacques Alain. *Rapport d'information sur les fichiers de police*, Assemblée nationale, 21 décembre 2011

URVOAS, Jean-Jacques et VERCHERE, Patrice. *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*. Assemblée nationale, 14 mai 2013

CAVARD, Christophe, président, et URVOAS, Jean-Jacques, rapporteur. *Rapport fait au nom de la commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés*. Assemblée nationale, 24 mai 2013

ADAM, Patricia et GROSSELIN-FLEURY, Geneviève, *Rapport sur le projet de LPM 2014-2019*, Tome 1, Assemblée nationale, 14 novembre 2013

URVOAS, Jean-Jacques. *Rapport sur le projet de loi relatif au renseignement*. Assemblée nationale, 2 avril 2015

ADAM, Patricia et NAUCHE, Philippe. *Proposition de loi relative aux mesures de surveillance des communications électroniques internationales*, Assemblée nationale, 9 septembre 2015

ADAM, Patricia. *Rapport sur la proposition de loi, après engagement de la procédure accélérée, relative aux mesures de surveillance des communications électroniques internationales*. Assemblée nationale, 16 septembre 2015

FENECH, Georges. *Rapport d'enquête relative aux moyens mis en œuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015*. Assemblée nationale, 5 juillet 2016

GAUVAIN, Raphaël. *Rapport sur le projet de loi, adopté par le Sénat après engagement de la procédure accélérée, renforçant la sécurité intérieure et la lutte contre le terrorisme*. Assemblée nationale, 14 septembre 2017

FORTEZA, Paula. *Rapport sur le projet de loi relatif à la protection des données personnelles*, Assemblée nationale. 25 janvier 2018

GAUVAIN, Raphaël. *Rapport sur la proposition de loi portant transposition de la directive du Parlement et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués contre l'obtention, l'utilisation et la divulgation illicites*, Assemblée nationale, 21 mars 2018

BECHT, Olivier et GASSILLOUD, Thomas. *Rapport d'information en conclusion des travaux d'une mission d'information sur les enjeux de la numérisation des armées*, 30 mai 2018

LACHAUD, Bastien. VALETTA-ARDISSON, Alexandra. *Rapport d'information sur la cyberdéfense*. Assemblée nationale, 4 juillet 2018

PARIS, Didier et MOREL-A-L'HUISSIER, Pierre. *Rapport d'information sur les fichiers mis à disposition des forces de sécurité*, Assemblée nationale, 17 octobre 2018

LARRIVE, Guillaume, président, et KERVRAN, Loïc et MIS, Jean-Michel, rapporteurs. *Rapport d'information sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement*, Assemblée nationale, 10 juin 2020

GAUVAIN, Raphaël et KERVRAN, Loïc. *Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*, Assemblée nationale, 20 mai 2021

WARASMANN, Jean-Luc. LATOMBE, Philippe. *Rapport d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne. Tome I*, Assemblée nationale, 29 juin 2021

- **Sénat**

MARCILHACY, Pierre. *Rapport fait au nom de la Commission de contrôle des services administratifs procédant aux écoutes téléphoniques*, Sénat, 23 octobre 1973

THYRAUD, Jacques. *Rapport sur la proposition de loi adoptée par l'Assemblée nationale relative à la fraude informatique*, Sénat, 2 octobre 1987

RUDLOFF, Marcel. *Rapport relatif au secret des correspondances émises par la voie des télécommunications*, Sénat, 19 juin 1991

TÜRK, Alex. *Rapport sur le projet de loi, adopté par l'Assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Sénat, 19 mars 2003

TÜRK, Alex. *Rapport sur le projet de loi, adopté avec modification par l'Assemblée nationale en deuxième lecture, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Sénat, 23 juin 2004

BOCKEL, Jean-Marie. *Rapport d'information sur la cyberdéfense*, Sénat, 18 juillet 2012

CARRERE, Jean-Louis. *Rapport sur le projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*. Sénat, 8 octobre 2013

CARRERE, Jean-Louis. *Rapport sur le projet de loi, modifié par l'Assemblée nationale, relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, Sénat, 4 décembre 2013

SUEUR, Jean-Pierre. *Rapport d'information sur le numérique, le renseignement et la vie privée : de nouveaux défis pour le droit*, 27 juin 2014

GOULET, Nathalie et REICHARDT, André, co-présidents, et SUEUR, Jean-Pierre, rapporteur, *Rapport fait au nom de la commission d'enquête sur l'organisation et les moyens de la lutte contre les réseaux djihadistes en France et en Europe*, Sénat, 1^{er} avril 2015

RAFFARIN, Jean-Pierre. *Avis sur le projet de loi relatif au renseignement*, Sénat, 13 mai 2015

BAS, Philippe. *Rapport sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif au renseignement et sur la proposition de la loi organique présentée par MM. J. -P. Raffarin et P. Bas, relative à la nomination du président de la CNCTR*, Sénat, 20 mai 2015

BAS, Philippe. *Proposition de loi relative aux mesures de surveillance des communications électroniques internationales*. Sénat, 21 septembre 2015

BAS, Philippe. *Rapport sur la proposition de loi, adoptée par l'Assemblée nationale après engagement de la procédure accélérée, relative aux mesures de surveillance des communications électroniques internationales*. Sénat, 21 octobre 2015

FRASSA, Christophe-André. *Rapport sur le projet de loi pour une République numérique*, Tome 1, Sénat, 6 avril 2016

BOUTANT, Michel. *Avis sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*. Sénat, 12 juillet 2017

CAMBON, Christian. *Rapport relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*. Sénat, 16 mai 2018

BUFFET, François-Noël et DETRAIGNE, Yves. *Rapport sur le projet de loi de programmation 2018-2022 et de réforme pour la justice et sur le projet de loi organique relatif au renforcement de l'organisation des juridictions*, Sénat, 3 octobre 2018

PERRIN, Cédric. GUERINI, Jean-Noël. *Rapport d'information sur l'innovation et la défense*. Sénat, 10 juillet 2019

MONTAUGE, Franck. LONGUET, Gérard. *Rapport de la commission d'enquête sur la souveraineté numérique*. Tome 1, Sénat, 1er octobre 2019

JOISSAINS, Sophie et BIGOT, Jacques. *Rapport d'information sur la lutte contre la cybercriminalité*, Sénat, 9 juillet 2020

MEURANT, Sébastien. CARDON, Rémi. *Rapport d'information relatif à la cybersécurité des entreprises*. Sénat, 10 juin 2021

CADIC, Olivier et VALLET, Mickaël. *Rapport d'information pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024-2030*, Sénat, 24 mai 2023

C. Gouvernement

BRAIBANT, Guy. *Données personnelles et société de l'information*, Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46, 3 mars 1998

Déclaration de M. Lionel Jospin, Premier ministre, *sur la mise en œuvre et les orientations de développement du Programme d'action gouvernementale pour la société de l'information (PAGSI)*, Hourtin le 26 août 1999

DANIEL, Michael, *Heartbleed : Understanding When We Disclose Cyber Vulnerabilities*. White House, avril 28, 2014

Joint Statement by Attorney General Loretta Elizabeth. LYNCH and Secretary of Homeland Security Jeh JOHNSON, Friday, September 25, 2015

Livre blanc de la défense et de la sécurité nationale de 2013

ETUDE D'IMPACT, *Projet de LPM 2014-2019*, 29 juillet 2013

ETUDE D'IMPACT, *Projet de loi relatif au renseignement*, 18 mars 2015

SGDSN. *Revue stratégique de cyberdéfense*. 12 février 2018

JEANGENE VILMER, Jean-Baptiste. ESCORCIA, Alexandre. GUILLAUME, Marine. HERRERA, Janaina. *Les Manipulations de l'information : un défi pour nos démocraties*. Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018

Rapport du ministère des Armées sur *le Droit international appliqué aux opérations dans le cyberspace*, 9 septembre 2019

ANSSI, *Algorythmes de cryptographie post-quantique, Papiers numériques*. Edition 2020, p. 47

ANSSI, *Etat de la menace rançongiciel à l'encontre des entreprises et institutions*, 5 février 2020

SGDSN, *Rapport d'activité 2019-2020*

SGDSN, *Rapport d'activité 2021*

COMCYBER. *Eléments publics de doctrine militaire de lutte informatique d'influence (L2I)*, 2021

ETUDE D'IMPACT, *Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative*, 11 mai 2021

COMMISSION BRONNER, *Les Lumières à l'ère numérique*, Présidence de la République, 11 janvier 2022

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Senior Advisory Group, Panel on Commercially Available Information, Report the Director of National Intelligence*, 27 january 2022

MINISTERE DE L'ECONOMIE. *Rapport au Parlement sur les exportations des biens à double usage de la France*. Direction générale des Entreprises, juillet 2022

D. Autorités administratives indépendantes

- **Commission nationale de contrôle des interceptions de sécurité**

CNCIS, *1er rapport d'activité (1991-1992)*

CNCIS, *19^{ème} rapport d'activité (2010)*

CNCIS, *20^{ème} rapport d'activité (2011-2012)*

CNCIS, *22^{ème} rapport d'activité années (2013-2014)*

CNCIS, *23^{ème} rapport d'activité (2014-2015)*

- **Commission nationale de contrôle des techniques de renseignement**

CNCTR, *1^{er} rapport d'activité (2015-2016)*

CNCTR, *2^{ème} Rapport d'activité (2017)*

CNCTR, *3^{ème} rapport d'activité (2018)*

CNCTR, *4^{ème} rapport d'activité (2019)*

CNCTR, *5^{ème} rapport d'activité (2020)*

CNCTR, *6^{ème} rapport d'activité (2021)*

CNCTR, *7^{ème} rapport d'activité (2022)*

CNCTR, *8^{ème} rapport d'activité (2023)*

- **Commission nationale de l'information et des libertés**

BOUCHET, Hubert., *La cybersurveillance sur les lieux de travail*, rapport adopté par la CNIL le 5 février 2002

CNIL, *Rapport d'activité 2013*

CNIL, *36^{ème} rapport d'activité (2015)*

CNIL, *38^{ème} rapport d'activité (2017)*

CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Décembre 2017

CNIL, *Reconnaissance faciale : pour un débat à la hauteur des enjeux*, 15 novembre 2019

CNIL, *Publication des décrets relatifs aux fichiers PASP, GIPASP et EASP : la CNIL précise sa mission d'accompagnement*, 11 décembre 2020

E. Autres

CONSEIL D'ETAT. *Le numérique et les droits fondamentaux*, étude annuelle 2014

LE DAIN, Anne-Yvonne. SIDO, Bruno. *Rapport sur la sécurité numérique et risques : enjeux et chances pour les entreprises*. Office parlementaire d'évaluation des choix scientifiques et technologiques, Tome 1, 2 février 2015

CNCDH, ass. plén., *avis sur le projet de loi relatif au renseignement dans sa version enregistrée le 1er avril 2015 à la Présidence de l'Assemblée nationale*, 16 avril 2015

INRIA. *Eléments d'analyse technique du projet de loi relatif au renseignement*, Note interne, 30 avril 2015

DEFENSEUR DES DROITS. *Les droits fondamentaux des étrangers en France*. mai 2016

OBSERVATOIRE DES LIBERTES ET DU NUMERIQUE, *Chiffrement, sécurité et libertés*. Janvier 2017

VILLANI, Cédric. *Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne*, Rapport de la mission parlementaire du 8 septembre 2017 au 8 mars 2018

SCHAAKE, Marietje. PUPILLO, Lorenzo. FERREIRA, Afonso. VARISCO, Gianluca. *Software Vulnerability Disclosure in Europe, Technology, Policies and Legal Challenges*. Report of a CEPS Task Force, June 2018

INHESJ, *Groupe de diagnostic stratégique (GDS) n°8, Reconnaissance faciale : entre exigence de contrôle et respect de la vie privée Quels outils, quels enjeux, quelles garanties ?*, Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ), 30ème session nationale « Sécurité et Justice » 2018 – 2019

CLUB DES JURISTES, « *Le droit pénal à l'épreuve des cyberattaques* », rapport d'avril 2021

DEFENSEUR DES DROITS. *Rapport Technologies biométriques : l'impératif respect des droits fondamentaux*. Juillet 2021

IV. PRESSE ET MEDIA

Classement par ordre chronologique

BOUCHER, Philippe, « *Safari* » ou la chasse aux français, Le Monde, 21 mars 1974

GREENWALD, Glenn, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, Friday 7 jun 2013

BERTHEMET, Tanguy, *Edward Snowden, l'homme qui fait trembler le gouvernement américain*, Le Figaro, 10 juin 2013

FOLLOROU, Jacques et JOHANNES, Franck. *Révélation sur le Big Brother français*, Le Monde, 4 juillet 2013

RAULINE, Nicolas. *Bullrun, l'autre programme de la NSA qui ébranle la high-tech*, Les Echos, 6 septembre 2013

GIRARD, Quentin., *Vos mails, SMS, connexions internet, légalement surveillés ?*. Libération, 10 décembre 2013

FOLLOROU, Jacques. *Espionnage : comment Orange et les services secrets coopèrent*, Le Monde, 20 mars 2014

GRIFFIN, Andrew. *WhatsApp and iMessage could be banned under new surveillance plans*. The Independent, 12 January 2015

BOY, Louis. *« Boîte noire » et surveillance du web : le projet de loi sur le renseignement est-il liberticide ?*, Franceinfo, 5 avril 2015

FOLLOROU, Jacques. *Ce « Big Brother » dissimulé au cœur du renseignement*, Le Monde, 10 avril 2015

MANACH, Jean-Marc. *Une fois de plus, j'ai cherché le « Big Brother » du Monde, en vain !*, Arrêt sur images, 20 avril 2015

MERCHET, Jean-Dominique. *Ce que l'on sait du Pôle national de cryptanalyse et de décryptement*, L'Opinion, 20 avril 2015

ISAAK, Mike. *Explaining Apple's fight with the FBI*. The New York Times, feb. 17, 2016

YADRON, Danny. *San Bernardino iPhone : US ends Apple case after accessing data without assistance*. The Guardian, 29 mars 2016

SMITH, Brad. *The need for a Digital Geneva Convention*, Microsoft On the Issues, february 14, 2017

UNTERSINGER, Martin. *Le rançongiciel WannaCry ravive le débat sur les failles de sécurité*, Le Monde, 16 mai 2017

TH. B. *Cyberattaque mondiale : le parquet de Paris ouvre une enquête en France*, Le Parisien, 28 juin 2017

FADIER, Darius. *Avis d'Experts CEIS : Convention de Genève numérique de Microsoft, une protection adaptée ?*, ITespresso, 1 décembre 2017

GUITON, Amaëlle. *Surveillance internationale : l'eurodéputée Sophie in 't Veld déboutée par le Conseil d'Etat*, Libération, 27 juin 2018

SAINT-JALM, Jérémie. FREANI, Jérôme. FIOCRE, Nicolas. *L'initiative française « Data Intelligence » : la stratégie du cluster pour s'affranchir de Palantir*. Club Cyber de l'AEGE, Portail de l'IE, 26 octobre 2018

GUIOTON, Amaëlle. *Belgacom, ou les aléas du piratage entre amis*, Libération, 2 novembre 2018

FRANCE CULTURE, *Surveiller pour punir : la notation des citoyens chinois*, 9 janvier 2019

LEGER, Alban. FIOCRE, Nicolas. *L'intelligence campus, nouveau vecteur du renseignement militaire*. Portail de l'IE, 26 février 2019

FOLLOROU, Jacques. « *L'entrepôt* », *bâtiment ultrasécurisé et outil essentiel du renseignement français*, Le Monde, 24 avril 2019

DRIF, Anne. *Big Data : faute de solution française, les services secrets signent à nouveau avec Palantir*, Les Echos, 27 novembre 2019

Grand entretien de France Inter du ministre de l'Intérieur, Gérald Darmanin, du mercredi 28 avril 2021

LAGNEAU, Laurent. *Le renseignement militaire muscle ses capacités d'analyse de l'imagerie satellitaire avec l'intelligence artificielle*, Zone Militaire (opex360.com), 8 juillet 2021

LELOUP, Damien. UNTERSINGER, Martin. « *Projet Pegasus* » : *révélations sur un système mondial d'espionnage de téléphones*, Le Monde, 18 juillet 2021

DE FALETANS Sixtine, RENARD, Simon, MOINEAU, Charlotte. *USA-Chine : accusations d'espionnage économique sur le sol américain*. Portail de l'IE, 3 novembre 2022

TV5MONDE, *L'espionnage industriel, une arme privilégiée par la Chine ?*. 5 février 2023

INDEX

A

Algorithmes, 17, 59, 60, 61, 64, 66, 70, 189, 190, 191, 192, 195, 196, 202, 203, 204, 215, 217, 223, 235, 236, 238, 249, 255, 293, 368, 376, 377, 378, 379, 380, 387, 397, 406, 470, 593, 616

ANSSI, 7, 19, 26, 87, 295, 418, 419, 420, 438, 440, 443, 454, 455, 461, 464, 466, 467, 475, 479, 481, 483, 486, 487, 488, 491, 492, 493, 524, 525, 526, 528, 535, 541, 542, 544, 548, 551, 555, 557, 560, 563, 567, 568, 570, 574, 575, 615

ARCEP, 7, 66, 280, 304, 395, 463, 492, 568

Arrangement de Wassenaar, 21, 23, 506, 509, 510, 511, 512, 514, 516, 563, 564, 604

B

Biens à double usage, 24, 512, 514, 515, 516, 517, 518, 551, 563, 601, 615

Big data, 3, 11, 12, 13, 20, 376, 441, 470, 536, 572

C

Captation de données informatiques, 53, 82, 84, 85, 86, 89, 299, 443, 460, 462, 466, 467, 482, 594

CEDH, 7, 22, 33, 34, 45, 47, 48, 99, 104, 105, 107, 112, 185, 186, 187, 212, 229, 233, 234, 238, 248, 254, 317, 328, 329, 330, 331, 332, 333, 334, 335, 337, 338, 339, 340, 342, 343, 344, 345, 346, 347, 348, 359, 367, 368, 372, 381, 382, 386, 387, 406, 409, 452, 469, 470, 503, 591, 593

Centralisation des renseignements, 246, 251, 252, 272, 276

Chiffrement, 12, 18, 26, 80, 81, 84, 86, 87, 258, 262, 525, 534, 536, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 570, 600, 603, 605

CJUE, 7, 23, 51, 52, 55, 68, 69, 70, 166, 192, 195, 234, 236, 249, 292, 302, 351, 352, 354, 355, 356, 357, 358, 359, 360, 362, 365, 367, 368, 370, 371, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 390, 391, 392, 393, 394, 396, 397, 398, 399, 400, 402, 403, 404, 405, 406, 407, 408, 409, 469, 470, 578, 587, 590, 592, 593

CNCIS, 7, 28, 34, 35, 36, 37, 38, 42, 46, 47, 52, 54, 57, 72, 74, 211, 225, 243, 297, 299, 300, 302, 304, 342, 425, 585, 603, 615, 616

CNCTR, 7, 24, 37, 57, 58, 60, 61, 62, 69, 72, 73, 74, 77, 78, 79, 80, 81, 82, 83, 86, 87, 92, 94, 97, 101, 109, 110, 111, 112, 160, 176, 177, 179, 183, 184, 185, 186, 187, 191, 193, 194, 197, 210, 212, 213, 214, 215, 216, 217, 219, 222, 223, 224, 225, 226, 227, 231, 232, 233, 236, 239, 241, 242, 243, 244, 247, 248, 249, 250, 251, 252, 253, 254, 258, 261, 263, 268, 269, 272, 273, 274, 275, 277, 283, 284, 285, 287, 289, 290, 291, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 319, 320, 333, 339, 342, 346, 347, 348, 360, 362, 365, 370, 371, 374, 383, 386, 390, 396, 399, 421, 443, 447, 464, 465, 483, 492, 524, 531, 534, 535, 568, 578, 585, 613, 616

CNIL, 7, 12, 17, 25, 43, 48, 49, 50, 65, 66, 71, 83, 115, 116, 117, 119, 121, 122, 123, 124, 125, 129, 134, 135, 137, 138, 140, 141, 149, 151, 152, 153, 154, 155, 156, 157, 158, 168, 169, 170, 171, 172, 174, 175, 179, 180, 182, 190, 191, 193, 194, 199, 200, 202, 205, 214, 217, 235, 260, 261, 285, 291, 308, 309, 310, 311, 316, 319, 348, 395, 399, 427, 428, 430, 452, 453, 469, 487, 492, 559, 560, 568, 604, 616

COMCYBER, 8, 97, 478, 479, 481, 483, 489, 491, 492, 493, 496, 499, 501, 567, 575, 615

Communications hertziennes, 25, 75, 76, 77, 85, 103, 298, 356, 444

Communications internationales, 52, 54, 75, 78, 102, 107, 108, 109, 111, 113, 204, 221, 237, 240, 244, 256, 306, 314, 356, 397, 482

Communications satellitaires, 76, 78

Conseil d'Etat, 7, 44, 50, 52, 55, 61, 68, 69, 70, 71, 73, 74, 79, 80, 97, 98, 101, 108, 109, 110, 111, 116, 117, 119, 120, 121, 122, 123, 124, 125, 127, 128, 129, 130, 131, 133, 135, 139, 140, 144, 147, 150, 152, 153, 154, 155, 157, 167, 169, 171, 172, 174, 177, 178, 180, 192, 216, 218, 222, 231, 236, 248, 250, 255, 256, 258, 262, 263, 264, 283, 291, 301, 302, 303, 304, 308, 309, 310, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 323, 346, 348, 355, 359, 360, 361, 362, 363, 364, 365, 386, 388, 389, 390, 391, 392, 393, 394, 396, 397, 398, 399, 400, 401, 403, 404, 407, 424, 430, 447, 471, 483, 539, 579, 584, 585, 586, 587, 588, 591, 608, 618

Cour de cassation, 34, 81, 90, 93, 117, 164, 265, 360, 401, 404, 417, 418, 419, 431, 432, 433, 436, 438, 442, 451, 452, 454, 561, 562, 597

Cyberarmes, 21, 507, 510, 511, 520, 569, 602

Cybercriminalité, 22, 25, 39, 87, 98, 99, 180, 267, 325, 402, 413, 414, 428, 429, 438, 440, 447, 448, 449, 451, 470, 471, 475, 479, 513, 518, 561, 578, 579, 594, 595, 598, 599, 604, 611, 614

Cyberdéfense, 3, 5, 8, 13, 14, 26, 87, 96, 97, 180, 213, 290, 292, 295, 437, 453, 454, 455, 474, 475, 477, 478, 479, 481, 482, 483, 484, 485, 486, 491, 492, 493, 495, 496, 498, 499, 500, 505, 511, 520, 531, 533, 536, 539, 540, 542, 546, 556, 558, 563, 564, 567, 568, 569, 570, 572, 573, 574, 575, 578, 579, 600, 601, 602, 604, 606, 612, 613, 615

Cyberespace, 3, 6, 12, 13, 15, 18, 19, 21, 27, 28, 87, 90, 112, 292, 325, 326, 341, 358, 434, 436, 441, 448, 456, 472, 473, 474, 475, 476, 477, 479, 481, 482, 483, 484, 485, 488, 493, 494, 495, 496, 497, 498, 500, 501, 503, 504, 505, 511, 518, 519, 545, 546, 549, 555, 558, 566, 568, 569, 570, 571, 572, 577, 578, 579, 582, 598, 601, 603, 605, 606, 615

Cyberespionnage, 3, 14, 299, 338, 420, 488, 493, 498, 499, 500, 501, 502, 503, 504, 558, 572, 573

Cyberopérations, 21, 95, 97, 450, 451, 482, 484, 485, 489, 493, 494, 496, 497, 498, 500, 501, 566, 569, 582

Cybersécurité, 3, 5, 8, 19, 23, 86, 89, 213, 281, 325, 473, 475, 478, 481, 487, 491, 495, 498, 510, 511, 515, 519, 520, 523, 528, 531, 533, 535, 538, 539, 540, 545, 546, 547, 549, 550, 551, 554, 555, 556, 557, 560, 562, 563, 564, 565, 567, 569, 570, 571, 573, 574, 576, 577, 578, 579, 599, 600, 603, 604, 605, 606, 614

D

Délégation parlementaire au renseignement, 8, 14, 16, 24, 291, 610

DGSE, 8, 11, 61, 87, 96, 105, 106, 107, 118, 125, 131, 132, 141, 143, 152, 158, 171, 180, 218, 219, 221, 222, 251, 252, 253, 254, 270, 275, 276, 305, 441, 479, 481, 482, 490, 493, 496, 499, 500, 522, 523, 567, 575

DGSI, 8, 20, 61, 87, 134, 141, 143, 148, 158, 163, 168, 180, 196, 218, 219, 221, 222, 226, 227, 251, 252, 253, 254, 269, 275, 276, 305, 318, 348, 401, 430, 466, 479, 481, 575

Données biométriques, 153, 161, 199, 200, 201

Données de connexion, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 55, 57, 58, 61, 64, 66, 67, 68, 69,

71, 79, 105, 106, 109, 110, 111, 167, 215, 223, 224, 230, 234, 235, 236, 237, 239, 244, 246, 247, 248, 249, 250, 251, 255, 256, 257, 297, 343, 345, 347, 353, 354, 356, 359, 362, 363, 364, 368, 369, 370, 372, 374, 375, 376, 377, 383, 384, 386, 388, 389, 390, 391, 393, 394, 395, 396, 397, 400, 401, 403, 404, 405, 406, 407, 408, 460, 462, 463, 556, 586, 590, 591, 592, 593, 594

Données personnelles, 23, 37, 43, 44, 51, 93, 99, 122, 128, 129, 147, 151, 157, 159, 167, 169, 178, 179, 182, 186, 187, 190, 192, 193, 194, 197, 204, 205, 210, 234, 249, 260, 261, 265, 292, 298, 302, 310, 311, 312, 316, 317, 318, 319, 323, 325, 328, 329, 333, 335, 336, 337, 340, 341, 344, 345, 348, 349, 350, 351, 353, 357, 358, 363, 366, 367, 368, 369, 377, 380, 382, 384, 385, 386, 392, 397, 402, 409, 417, 420, 426, 427, 428, 429, 430, 438, 442, 452, 467, 489, 490, 503, 505, 549, 553, 559, 560, 590, 591, 592, 594, 595, 597, 599, 603, 612

DPR, 8, 14, 16, 19, 24, 52, 53, 58, 59, 60, 61, 64, 73, 75, 78, 82, 87, 102, 105, 107, 109, 142, 147, 150, 151, 158, 165, 168, 178, 184, 186, 214, 216, 223, 227, 260, 271, 277, 278, 283, 284, 285, 288, 289, 291, 292, 293, 294, 295, 296, 305, 308, 312, 314, 315, 348, 359, 418, 420, 421, 441, 479, 483, 492, 530, 545, 610, 611

DRM, 8, 20, 74, 77, 96, 118, 125, 152, 153, 189, 190, 196, 200, 218, 219, 221, 222, 318, 441, 481, 584

Droit au respect de la vie privée, 50, 88, 93, 124, 204, 207, 210, 229, 233, 235, 238, 301, 344, 347, 349, 404, 426, 427, 470, 503, 518, 554

Droit d'accès indirect, 116, 310, 317

Droit international, 21, 23, 96, 98, 100, 103, 262, 323, 340, 347, 359, 484, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 513, 538, 569, 580, 581, 582, 587, 590, 593, 601, 602, 603

DRSD, 8, 141, 143, 152, 153, 154, 158, 218, 219, 221, 222, 318, 479, 481, 522

E

Economie numérique, 3, 6, 9, 15, 18, 20, 26, 27, 42, 45, 49, 82, 87, 358, 394, 426, 473, 508, 519, 520, 539, 546, 547, 550, 551, 553, 555, 566, 569, 570, 571, 572, 574, 575, 599, 611

F

FAI, 8, 39, 41, 42, 47, 64

Fichiers, 25, 37, 43, 44, 114, 115, 116, 117, 119, 120, 121, 122, 123, 124, 125, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 143, 145, 146, 147, 148, 149, 150, 151, 152,

153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 174, 175, 176, 177, 181, 188, 191, 192, 195, 196, 197, 200, 201, 202, 205, 246, 262, 263, 264, 285, 289, 291, 307, 308, 309, 310, 311, 312, 313, 316, 317, 318, 319, 320, 322, 323, 342, 346, 348, 349, 356, 379, 417, 418, 421, 422, 428, 429, 430, 431, 436, 452, 534, 578, 580, 583, 584, 585, 586, 587, 588, 589, 595, 596, 597, 599, 607, 608, 611, 612, 613, 616

G

GCHQ, 8, 13, 18, 99, 184, 278, 322, 485, 566, 575

Géolocalisation, 41, 45, 47, 48, 52, 59, 63, 64, 70, 223, 224, 239, 343, 353, 356, 370, 392, 452, 517, 609

GIC, 9, 32, 34, 35, 38, 46, 47, 60, 71, 78, 79, 106, 107, 177, 192, 231, 237, 239, 251, 252, 253, 255, 260, 268, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 282, 284, 295, 305, 322, 323, 432, 531, 535, 574, 575

H

Hackers, 454, 455, 488, 491, 556, 557, 558, 559, 561, 562, 563, 564, 598

I

IMSI-catcher, 64, 65, 66, 69, 72, 79, 80, 89, 215, 223

Intelligence artificielle, 11, 17, 114, 159, 160, 164, 170, 176, 189, 190, 194, 195, 196, 205, 214, 376, 378, 441, 470, 536, 577, 589, 605, 616, 617, 619

Interconnexions, 114, 117, 126, 157, 168, 169, 170, 171, 173, 174, 175, 176, 188, 195, 196, 205, 312, 379, 523, 531, 534

J

Judiciarisation du renseignement, 163, 165, 181, 574

L

Lanceur d'alerte, 268, 281, 282, 283, 284, 562, 563, 603

Liberté d'expression, 44, 50, 51, 200, 436, 437, 553, 554

Lutte informatique défensive, 475, 483, 565

Lutte informatique offensive, 475, 483

N

NSA, 9, 13, 15, 16, 18, 19, 49, 54, 55, 99, 107, 184, 278, 281, 322, 351, 440, 456, 485, 520, 549, 558, 565, 568, 569, 575, 580, 601, 617, 618

O

Opérateurs du numérique, 16, 18, 167, 205, 268, 279, 285, 300, 323, 353, 366, 369, 370, 377, 383, 392, 393, 395, 405, 406, 449, 486, 487, 491, 492, 559, 561, 574, 575

P

Partage d'informations, 114, 177, 178, 180, 182, 557, 560, 561, 563, 564

Proportionnalité, 107, 171, 174, 209, 228, 229, 230, 231, 232, 236, 238, 242, 245, 254, 256, 262, 300, 311, 317, 330, 332, 336, 344, 366, 368, 369, 370, 371, 380, 381, 393, 408, 420, 444, 452, 490, 497, 541, 554, 566, 568, 578, 584, 608

R

Reconnaissance faciale, 199, 200, 201, 202, 490, 517

Responsabilité, 19, 32, 60, 70, 95, 97, 100, 173, 254, 262, 263, 264, 265, 266, 269, 309, 322, 340, 352, 372, 384, 413, 434, 457, 477, 478, 481, 483, 485, 501, 523, 528, 532, 559, 568, 585, 587

RGPD, 9, 128, 173, 260, 262, 351, 356, 387, 533, 553, 554, 559, 603

RIC, 9, 213, 214, 290, 322, 453, 454, 456, 482, 576

ROC, 9, 213, 322, 453, 478, 482, 576

ROSO, 9, 441, 443, 588

S

Secret de la défense nationale, 8, 19, 26, 64, 114, 116, 130, 150, 154, 197, 220, 245, 279, 280, 281, 282, 283, 284, 285, 288, 300, 304, 310, 312, 315, 317, 318, 398, 422, 447, 451, 453, 457, 466, 467, 471, 479, 521, 522, 523, 528, 529, 532, 544, 545

Secret des correspondances électroniques, 34, 204, 325, 342, 424, 425, 427, 432, 467, 549

Sécurité humaine, 506, 512, 515, 516, 518, 519, 576, 577, 608

Sécurité nationale, 3, 14, 17, 25, 29, 35, 45, 46, 70, 129, 139, 150, 161, 165, 168, 183, 192, 197, 210, 211, 219, 220, 226, 234, 236, 286, 329, 330, 331,

333, 338, 339, 345, 352, 355, 356, 359, 367, 368, 371, 372, 373, 374, 375, 376, 378, 379, 380, 381, 384, 388, 389, 390, 391, 392, 393, 394, 395, 396, 398, 399, 400, 401, 402, 403, 406, 408, 414, 422, 434, 454, 461, 470, 474, 475, 476, 477, 488, 513, 521, 536, 539, 541, 544, 545, 547, 550, 553, 555, 565, 568, 571, 572, 576, 577, 578, 583, 592, 593, 594, 606, 609, 613, 615

Sécurité publique, 8, 9, 10, 116, 117, 118, 120, 129, 131, 133, 135, 136, 138, 144, 145, 146, 147, 148, 149, 156, 171, 181, 197, 201, 213, 224, 234, 279, 353, 360, 371, 372, 373, 374, 375, 388, 398, 400, 401, 408, 541, 608

SGDSN, 10, 48, 272, 276, 277, 287, 295, 461, 465, 484, 485, 488, 489, 496, 511, 524, 525, 526, 528, 532, 535, 615

Souveraineté numérique, 14, 20, 440, 494, 503, 536, 538, 539, 540, 541, 545, 548, 590, 602, 605, 612, 614

STAD, 10, 97, 415, 417, 418, 419, 421, 424, 429, 443, 450, 452, 453, 467, 595, 596

Surveillance ciblée, 15, 16, 200, 225, 232, 233, 234, 236, 238, 576

Surveillance de masse, 3, 15, 16, 17, 19, 20, 54, 55, 59, 67, 99, 129, 164, 205, 212, 233, 235, 236, 237, 238, 281, 331, 333, 339, 348, 351, 375, 376, 377, 390, 409, 547, 549, 572, 590, 591, 592

T

Tiers service, 175, 182, 184, 187, 307, 311

Traçabilité des renseignements, 251, 252, 253, 302

U

URL, 10, 62, 249, 257, 296, 362

V

VEP, 10, 565, 566, 567, 606

VIGINUM, 10, 489, 490, 491, 492, 575

Vulnérabilités, 454, 456, 488, 510, 526, 531, 546, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 567, 568, 571, 572, 579, 603

TABLE DES MATIERES

LISTE DES PRINCIPALES ABREVIATIONS	7
INTRODUCTION	11
<i>SECTION I : Les développements de la numérisation du renseignement</i>	<i>12</i>
<i>SECTION II : Une numérisation controversée</i>	<i>15</i>
§1. Surveillance de masse et libertés	15
§2. Cyber-renseignement et économie numérique	18
<i>SECTION III : Une numérisation appréhendée par le droit</i>	<i>21</i>
§1. Le droit international et européen	21
§2. Le droit national	24
§3. Une dualité droit du renseignement/droit du numérique	26
PREMIERE PARTIE UNE AUTONOMISATION DU DROIT DU RENSEIGNEMENT NUMERIQUE	29
TITRE I LE RENFORCEMENT DES MOYENS NUMERIQUES DE RENSEIGNEMENT	30
CHAPITRE I LA RECHERCHE NUMERIQUE DES RENSEIGNEMENTS	31
<i>SECTION I : L'insuffisant dispositif antérieur à 2015</i>	<i>31</i>
§1. L'adaptation de la loi du 10 juillet 1991 aux développements des communications électroniques	32
A – La légalisation incontournable des « interceptions de sécurité »	32
B – L'application des dispositions de la loi de 1991 aux évolutions technologiques	36
C – Les limites de la loi du 10 juillet 1991 face à la numérisation	39
§2. La remise en cause progressive du dispositif antérieur à 2015	40
A – Les dispositions complémentaires au dispositif de 1991	40
1. La loi du 15 novembre 2001 relative à la sécurité quotidienne	40
2. La loi du 23 janvier 2006 relative à la lutte contre le terrorisme	40
3. La loi de programmation militaire du 18 décembre 2013	45
B – La nécessité d'une loi relative au renseignement	52
<i>SECTION II : L'exorbitant dispositif postérieur à 2015</i>	<i>57</i>
§1. L'extension des techniques numériques déjà consacrées	57
A- Les accès administratifs aux données de connexion	57
1. Les « sondes » mises en œuvre sur les réseaux	58
2. Les algorithmes de détection d'une menace terroriste	59
3. La géolocalisation en temps réel et le balisage	63
4. L'utilisation d'un « dispositif technique de proximité »	64
5. La validité des nouveaux accès aux données de connexion	66
B - Les interceptions de communications	71
1. L'élargissement des interceptions de sécurité	71
2. La réorganisation de la surveillance des communications hertziennes	73
3. La consécration d'une surveillance des communications satellitaires	78
C - Les réquisitions des conventions de déchiffrement des données	80
§2. La transposition de certaines techniques de police judiciaire	82
A - La sonorisation et la captation d'images	83
B - La captation de données informatiques	84
C - Les « cyber-patrouilles »	90
§3. L'affirmation de mesures numériques de renseignement extérieur	95
A - Les mesures mises en œuvre portant atteintes aux systèmes d'information à l'étranger	95
B - Les mesures de surveillance des communications électroniques internationales	101

CHAPITRE II L'EXPLOITATION NUMERIQUE DES RENSEIGNEMENTS 114

SECTION I : Les traitements de données..... 114

§1. Les fichiers de renseignement.....	114
A - Le cadre juridique général, de la loi « Informatique et libertés » à la loi relative au renseignement.....	116
1. La loi informatique et libertés et ses évolutions.....	116
2. Les apports de la loi relative au renseignement de 2015	130
B - Les règles spécifiques aux fichiers de renseignement	134
1. Les fichiers du renseignement intérieur	134
2. Les fichiers du renseignement extérieur et militaire	152
3. Les fichiers du renseignement économique et financier	155
4. Le fichier CAR du renseignement pénitentiaire	156
§2. Les accès aux fichiers et le rapprochement d'informations	157
A - Au sein de la communauté du renseignement.....	158
B - En dehors de la communauté du renseignement.....	160
1. L'accès à des fichiers administratifs.....	160
2. L'accès à des fichiers judiciaires	161
3. L'accès à des données d'acteurs privés	165
§3. Les interconnexions entre les fichiers	169
§4. Le partage d'informations	177
A - Les transmissions inter-services et avec d'autres administrations.....	177
B - La transmission d'informations par l'autorité judiciaire.....	180
C - Le partage international des données de renseignement	183

SECTION II : Les innovations numériques sur les données..... 189

§1. L'utilisation de l'intelligence artificielle	189
A - Un outil indispensable pour le renseignement qui suscite des craintes.....	189
B - Les mesures adoptées en droit du renseignement.....	191
C - Les perspectives juridiques de l'intelligence artificielle en renseignement.....	194
§2. La technologie biométrique	199

CONCLUSION DU TITRE 204

TITRE II L'ADAPTATION DES GARANTIES AUX MOYENS NUMERIQUES DE RENSEIGNEMENT 207

CHAPITRE I L'AMBIVALENCE DU REGIME DE MISE EN ŒUVRE DES MOYENS NUMERIQUES..... 208

SECTION I : Le régime préventif, une surveillance numérique soumise à autorisation préalable 208

§1. Les garanties relatives aux missions des services de renseignement.....	210
A - Les finalités invocables par les services de renseignement	210
1. L'élargissement du périmètre des finalités et cyberdimension	210
2. L'application des finalités dans la mise en œuvre des techniques de renseignement	215
B - Les missions des services et leurs compétences en matière de renseignement numérique..	218
1. La montée en puissance du renseignement numérique des services du premier cercle ...	218
2. L'élargissement des services du second cercle.....	222
§2. Les garanties intrinsèques aux techniques numériques de renseignement	228
A - Les principes de proportionnalité et de subsidiarité	229
B - Le principe d'individualisation ou la surveillance ciblée des individus	233
1. La reconnaissance de la surveillance ciblée et non ciblée en droit européen	233
2. L'affirmation d'une surveillance ciblée en droit du renseignement français.....	234
3. Les atténuations au principe d'individualisation	235
4. La portée limitée du principe d'individualisation	238
C - La centralisation de l'exécution des techniques de renseignement	239
D - Le principe de territorialité.....	240
E - Le contingentement des techniques.....	242
F - L'interdiction pour les services de réaliser les opérations matérielles de mise en œuvre des techniques chez les opérateurs	245
§3. Les garanties portant sur les renseignements collectés.....	246

A - La définition des renseignements collectés : données de connexion et données de « contenu »	246
1. La définition négative des données de connexion.....	247
2. La définition positive des données de connexion.....	249
3. Les données URL, un « brouillage » juridique.....	249
B - La centralisation et la traçabilité des renseignements collectés	251
C - La conservation limitée des renseignements collectés.....	254
1. Les délais de principe liés à la surveillance	255
2. Les délais dérogatoires non liés à la surveillance	258
D - Les restrictions d'accès aux renseignements collectés.....	259
1. La limitation du nombre d'agents susceptibles d'accéder aux données	259
2. L'exigence de mesures techniques de confidentialité applicable à certaines données	260
 <i>SECTION II : Le régime répressif, l'abus de la surveillance numérique constitutive d'une faute .</i>	<i>262</i>
§1. La responsabilité administrative de l'Etat pour faute simple du fait du renseignement numérique	262
§2. Un régime atypique de responsabilité pénale des agents	264
 CHAPITRE II LA SPECIALISATION DU CONTROLE SUR LES MOYENS NUMERIQUES.....	268
 <i>SECTION I : Les contrôles internes.....</i>	<i>268</i>
§1. La formalisation d'un contrôle hiérarchique du renseignement numérique	268
§2. Le rôle technico-juridique incontournable du Groupement interministériel de contrôle	271
A - Le contrôle de la mise en œuvre des techniques de renseignement	273
1. La correspondance entre identifiants techniques et cibles	273
2. La répartition des surveillances numériques	274
3. L'exploitation des techniques de renseignement	274
4. La difficulté du contrôle des techniques décentralisées.....	275
B - Le renforcement nécessaire des capacités de contrôle du Groupement interministériel de contrôle	275
1. Une réorganisation technologique	276
2. La question d'une délégation possible du contrôle de la Commission nationale de contrôle des techniques de renseignement	277
§3. Le contrôle du ministre chargé des communications électroniques sur les opérateurs du numérique.....	279
§4. La reconnaissance des lanceurs d'alerte de la surveillance numérique.....	281
A - Les atténuations du mécanisme de l'article L. 861-3 du code de la sécurité intérieure.....	282
1. Les personnes visées par le statut	282
2. Les faits pouvant être relevés.....	282
3. La procédure et ses effets	283
B - L'extension possible du mécanisme de l'article L. 861-3 du code de la sécurité intérieure ...	284
1. Etendre le statut à d'autres acteurs du renseignement numérique.....	284
2. Etendre le mécanisme à l'ensemble des activités de renseignement	285
§5. L'orientation et l'évaluation des moyens numériques par l'Exécutif	286
A - Le Conseil national du renseignement et le Coordonnateur national du renseignement	286
1. La Stratégie nationale du renseignement.....	287
2. Le Plan national d'orientation du renseignement	288
B - L'Inspection des services de renseignement	289
 <i>SECTION II : Les contrôles externes</i>	<i>291</i>
§1. Le contrôle politique des moyens numériques par le Parlement.....	291
A - Le cadre général du contrôle de la politique publique du renseignement	292
1. Un périmètre de contrôle couvrant le renseignement numérique	292
2. Des moyens de contrôle portant sur le renseignement numérique.....	293
B - Le cadre spécifique de l'application des techniques de renseignement	295
§2. Le renforcement nécessaire du contrôle de la Commission nationale de contrôle des techniques de renseignement	297
A - L'affirmation du contrôle sur le renseignement numérique	297
1. Des pouvoirs étendus	297
2. L'adaptation des moyens.....	304
B - Le dépassement du cadre d'intervention de la Commission nationale de contrôle des techniques de renseignement	307
1. Les limites à l'exercice du contrôle.....	307

2. Un contrôle plus large des activités du renseignement.....	308
§3. Le contrôle limité de la Commission nationale de l'informatique et des libertés	310
§4. Le contrôle juridictionnel « trop spécialisé » du Conseil d'Etat	312
A - Une formation juridictionnelle spécialisée sur les techniques et les fichiers de renseignement	313
1. Le contentieux des techniques de renseignement	313
2. Le contentieux du droit d'accès indirect.....	316
B - Sortir la formation spécialisée de la logique du cloisonnement des contentieux du renseignement.....	318
1. L'incohérence du cloisonnement.....	319
2. L'harmonisation du contentieux du renseignement numérique	319
CONCLUSION DU TITRE	322

SECONDE PARTIE L'APPLICATION DU DROIT DU NUMERIQUE AU RENSEIGNEMENT 325

TITRE I LES INTRICATIONS DU DROIT DU NUMERIQUE ET DU DROIT DU RENSEIGNEMENT 327

CHAPITRE I LA DIFFUSION DU DROIT EUROPEEN RELATIF A LA VIE PRIVEE NUMERIQUE 328

<i>SECTION I : Les prescriptions des instruments juridiques du Conseil de l'Europe.....</i>	<i>328</i>
§1. Les textes applicables à la surveillance numérique.....	328
A - L'article 8 de la Convention européenne des droits de l'homme	329
B - La Convention 108 sur la protection des données personnelles	336
§3. Un cadre européen du renseignement numérique en constante évolution	337
A - Le caractère évolutif du contrôle de la Cour européenne des droits de l'homme	338
B - L'adoption d'un nouvel instrument juridique du Conseil de l'Europe dédié au renseignement	339
§2. Des prescriptions fondamentales pour le droit du renseignement	342
A - Un droit du renseignement élaboré sur la base de la jurisprudence de la Cour européenne des droits de l'homme.....	342
B - Une conventionnalité discutable du cadre juridique interne du renseignement	346
1. La conventionnalité des techniques de renseignement	346
2. La conventionnalité des fichiers de renseignement	348
<i>SECTION II : Les exigences du droit de l'Union européenne</i>	<i>350</i>
§1. La compétence de l'Union européenne en matière de renseignement.....	352
A - Une compétence limitée à la surveillance numérique partenariale.....	353
1. L'accès aux données conservées par les opérateurs du numérique.....	353
2. L'accès aux données conservées par les acteurs des transports	356
3. L'accès aux données transférées hors de l'Union européenne	357
B - Une compétence discutable en matière de souveraineté	358
1. Une compétence critiquée	358
2. La résolution du conflit de normes	361
§2. Les « garanties essentielles européennes » dégagées par la Cour de justice de l'Union européenne.....	366
A - Des règles claires et précises	366
B - La nécessité et la proportionnalité	368
1. Le respect du contenu essentiel du droit à la vie privée numérique et les techniques de renseignement	369
2. La proportionnalité et la sécurité nationale	371
3. Les garanties spécifiques à l'utilisation d'algorithmes de surveillance.....	377
4. La stricte nécessité caractérisée par des critères objectifs.....	380
C - Un contrôle indépendant	382
D - Des voies de recours effectives	385
§3. Une conformité « augmentée » du droit du renseignement	388
A - Les finalités du renseignement numérique ou le « bloc de sécurité nationale »	388
B - Une redéfinition plus rigoureuse des données de connexion utiles au renseignement	393
C - L'extension du contrôle du renseignement numérique	396
1. Le contrôle préalable contraignant des techniques de renseignement	396
2. Le contentieux de l'évaluation de la menace contre la sécurité nationale.	398

D - Le cadre juridique du renseignement au secours des enquêtes judiciaires et de sécurité publique.....	400
1. Le renseignement et les infractions relatives aux atteintes aux intérêts fondamentaux de la Nation	400
2. Une dépendance des enquêtes judiciaires et de sécurité publique au renseignement	401
§4. Une européanisation indéniable du droit du renseignement	405
A - L'uniformisation de l'interprétation par la Cour de justice de l'Union européenne	405
1. L'autorité respectée de la Cour de justice de l'Union européenne	406
2. Les considérations technologiques, le « bug » jurisprudentiel	407
B - L'harmonisation par le législateur de l'Union européenne	408
1. Le règlement ePrivacy, un projet limité.....	408
2. Le règlement ePrivacy, un projet perfectible	409
C – Une européanisation qui réinterroge les fondements du droit du renseignement.....	410
1. La place du droit de la protection des données personnelles dans la dialectique « sécurité et liberté » en matière de renseignement	410
2. L'émergence d'un droit européen du renseignement fondé sur les garanties dégagées par les juges européens	411
CHAPITRE II L’AFFIRMATION DU DROIT PENAL DU NUMERIQUE	413
<i>SECTION I : La répression de l'abus cybercriminel du renseignement numérique</i>	<i>413</i>
§1. Des moyens numériques susceptibles de servir à commettre des infractions cybercriminelles	414
A - Les infractions cybercriminelles applicables aux moyens légalisés de renseignement numérique	415
1. Les atteintes aux systèmes de traitement automatisé de données	415
2. L'atteinte au secret des correspondances électroniques	424
3. Les atteintes aux données personnelles	427
4. Les atteintes à la vie privée par captations techniques de paroles, d'images ou de localisation.....	432
5. Renseignement numérique et contenus en ligne	434
B – Le risque pénal de moyens numériques n'entrant pas dans le champ du droit du renseignement.....	439
1. L'usage offensif de moyens de lutte informatique	439
2. Le recours à l'automatisation du renseignement d'origine sources ouvertes en ligne	440
§2. La délicate conciliation entre la lutte contre la cybercriminalité et le renseignement numérique	447
A - Les obstacles aux mécanismes de lutte contre la cybercriminalité par le droit du renseignement.....	447
1. L'usage illégal d'une technique de renseignement et le secret de la défense nationale ...	447
2. La protection du droit du renseignement contre la coopération pénale internationale	448
B – L'adaptation du droit pénal du numérique aux activités privées de cyber-renseignement ..	451
1. La reconnaissance du renseignement privé d'intérêt cyber	453
2. Un encadrement restrictif des partenariats public-privé de cyber-renseignement	455
<i>SECTION II : La détermination des appareils et dispositifs techniques de renseignement</i>	<i>459</i>
§1. La référence aux appareils ou dispositifs techniques mentionnés au 1° de l'article 226-3 du code pénal	459
A - Les techniques de renseignement concernées.....	459
1. Les techniques visées par le code de la sécurité intérieure	459
2. Les techniques visées par le code pénal	460
B - La liste des appareils ou dispositifs techniques	461
§2. Les conséquences de la référence au régime d'autorisation de l'article 226-3 du code pénal...	464
A - L'application du « régime d'autorisation 226-3 ».....	464
1. Une autorisation de plein droit	465
2. La nécessité d'un registre spécifique	465
B - Le contrôle des appareils et dispositifs techniques	466
1. L'organisation d'un contrôle interne	466
2. L'affirmation d'un contrôle externe	466
3. La sanction, le retrait d'autorisation.....	467
CONCLUSION DU TITRE	469

TITRE II LE RENSEIGNEMENT ET LA PROTECTION DU CYBERESPACE..... 473

CHAPITRE I L'ENCADREMENT DE LA MILITARISATION DU CYBERESPACE 474

SECTION I : Le droit de la cyberdéfense applicable au renseignement 474

§1. La participation du renseignement à la cyberdéfense	474
A - L'action des services de renseignement dans la cyberdéfense	478
1. Les missions des services de renseignement dans la cyberdéfense	479
2. Les moyens de renseignement et d'entrave.....	481
3. L'assouplissement du modèle français de cyberdéfense.....	483
B - La concurrence d'autres acteurs publics et privés dans le cyber-renseignement	486
1. L'enchevêtrement des moyens de cyber-renseignement dans la lutte informatique défensive	486
2. Le cyber-renseignement de lutte informatique informationnelle	488
3. Le « mille-feuille » du cyber-renseignement	491
§2. L'impact de la dimension internationale de la cyberdéfense sur le renseignement	493
A - Le droit international applicable aux cyberopérations.....	493
1. La reconnaissance de l'applicabilité du droit international au cyberspace	493
2. Des réponses juridiques limitées aux cyberopérations les plus offensives	496
B - L'intérêt renouvelé du droit international pour l'espionnage	499
1. Une stratégie d'évitement des Etats à bout de souffle	499
2. La formation d'un « droit international du renseignement »	503

SECTION II : La lutte contre la prolifération des outils numériques malveillants 506

§1. Le contrôle du commerce des outils numériques malveillants susceptibles d'intéresser le renseignement	506
A - La répression du trafic illicite d'outils numériques malveillants dans la Convention de Budapest	506
1. Les stipulations de contre-prolifération de l'article 6.....	507
2. L'exclusion de l'infraction de trafic illicite d'outils numériques malveillants pour le renseignement extérieur.....	508
B - L'introduction des logiciels intrusifs malveillants dans l'Arrangement de Wassenaar	509
1. Des adaptations particulièrement applicables au cyber-renseignement	509
2. Les limites de l'Arrangement de Wassenaar et du contrôle international des exportations	511
§2. La consécration d'un contrôle européen spécifique des biens de cybersurveillance fondé sur la « sécurité humaine ».....	512
A - Le risque du commerce des biens de cybersurveillance pour les droits de l'homme et le droit humanitaire	512
1. Le scandale des ventes de biens de cybersurveillance à des régimes autoritaires.....	513
2. La lente adoption d'une réforme jugée nécessaire du régime européen des biens à double usage	514
B - L'application du concept de « sécurité humaine » dans le contrôle des exportations des biens de cybersurveillance	516
1. Un régime d'autorisation ciblé, le contrôle « attrape-tout » des biens de cybersurveillance non répertoriés.....	516
2. Les critiques sur la cohérence du régime européen de contrôle des exportations des biens de cybersurveillance	518

CHAPITRE II LE RENSEIGNEMENT NUMERIQUE ET LA CYBERSECURITE 520

SECTION I : La cyberprotection du renseignement..... 521

§1. Les exigences du secret de la défense nationale sur la dématérialisation des informations classifiées	521
A – Les mesures spécifiques à la sécurité numérique	523
1. L'homologation des systèmes d'information classifiés	523
2. Le déploiement de dispositifs de cyberprotection	524
3. Une organisation dédiée à la cybersécurité du secret.....	528
B – L'application des mesures de sécurité numérique au renseignement	529
1. Des mesures de sécurité numérique adaptables aux besoins du renseignement	529
2. La conciliation des exigences du secret avec la numérisation du renseignement	531
§2. La contribution indirecte des droits de la cyberdéfense et du renseignement.....	532
A – Le recours au droit de la cyberdéfense.....	533

B - La sécurité des données personnelles traitées par les services de renseignement.....	533
C - La cyberprotection du renseignement dans les contrôles du renseignement numérique	534
§3. La maîtrise des technologies et services numériques nécessaires à la numérisation du renseignement.....	536
A - Un écosystème numérique problématique pour la cyberprotection du renseignement	537
1. Le recours aux industriels du numérique	537
2. Un enjeu de souveraineté numérique	538
B - Les solutions de confiance dans l'écosystème numérique	540
1. Les règles internes à l'administration de l'Etat.....	541
2. Les règles applicables aux industriels	542
 <i>SECTION II : Le respect d'exigences de la cybersécurité de la société</i>	 546
§1. L'éternel débat sur l'encadrement de la cryptologie	546
A - La perte du contrôle des Etats sur la cryptologie	548
1. L'apanage impossible des pouvoirs publics sur la cryptologie.....	548
2. Le choix de la libéralisation du chiffrement.....	550
3. Les souhaits peu convaincant d'un rétablissement du contrôle sur le chiffrement	552
B - La nécessité d'une liberté de chiffrement robuste dans les sociétés numérisées	553
1. « <i>Permis de chiffrer</i> », une garantie effective des droits et libertés à l'ère du numérique. 553	
2. « <i>Vivre et laisser chiffrer</i> », l'acceptation d'une sécurité nationale concurrencée par la sécurité du numérique	555
§2. Le nouvel enjeu de la « course aux vulnérabilités »	556
A - La responsabilisation de la divulgation des vulnérabilités pour la sécurité numérique	558
1. Les obligations de notification des failles de sécurité.....	559
2. La divulgation intentionnelle des vulnérabilités	561
B - Une rationalisation insuffisante de la rétention des vulnérabilités pour les intérêts de l'Etat	564
1. L'affirmation administrative balbutiante d'une mise en balance de la rétention des vulnérabilités	564
2. Une consécration juridique souhaitable d'un contrôle de la rétention des vulnérabilités	567
 CONCLUSION DU TITRE	 569
 CONCLUSION GENERALE RENFORCER L'ENCADREMENT DU RENSEIGNEMENT NUMERIQUE	 572
 <i>SECTION I : La délimitation du renseignement numérique</i>	 573
§1. Le rattachement à l'appareil de renseignement d'Etat.....	573
§2. La consolidation du modèle français de mutualisation	575
 <i>SECTION II : Une plus grande vigilance dans l'encadrement de nouveaux moyens numériques de renseignement</i>	 576
§1. Une légalisation des moyens plus rigoureuse	577
§2. Un contrôle des moyens plus étendu.....	578
 BIBLIOGRAPHIE	 580
INDEX.....	620
TABLE DES MATIERES	624