Projet REV – Lot 5
« Aspects juridiques »
Livrable – L 5.1

État de l'art sur l'exploitation des vulnérabilités

Réalisé par Lila de Lattre

Encadré par Noémie Véron, responsable Lot 5

Version	Date	Auteur	Commentaires
V0.1	25 juin 2025	Lila de Lattre	Réalisation du livrable
V0.2	25 juin 2025	Noémie Véron	Mise en forme et relecture
V1.1	30 juin 2025	Lila de Lattre	Bibliographie et relecture
V1. 2	1er juillet	Noémie Véron	Dernières relectures
V2.0	1er Juillet	Lila de Lattre	Modifications

Table des matières

INTRODUCTION 7

PARTIE 1 : LE CADRE JURIDIQUE DE LA VULNÉRABILITÉ EXPLOITÉE 15

1. Les exploitations strictement interdites 20

1.1 Les exploitations ayant pour finalité les atteintes aux systèmes de traitement automatisé de données 21

1.1.1 Les atteintes sanctionnées au titre d'une exploitation frauduleuse de vulnérabilités 23

1.1.1.1 L'accès ou le maintien dans tout ou partie d'un STAD 23
1.1.1.2 Le traitement de données sur tout ou partie d'un STAD 27

1.1.2 Les atteintes sanctionnées indépendamment du caractère frauduleux de l'exploitation 30

1.2 Les exploitations ayant pour finalité les atteintes à la personnalité 32

1.2.1 Les sanctions relatives aux atteintes à l'intimité de la vie privée d'autrui... 33

1.2.2 Les sanctions relatives aux atteintes au secret des correspondances 36

Conclusion 39

2. Les exploitations autorisées sous conditions 41

2.1 La captation de données informatiques par les services de police judiciaire et de renseignement 45

2.1.1 La captation opérée par les services de police judiciaire 46

2.1.1.1 Le champ matériel des infractions pouvant faire l'objet d'une technique de captation..... 47
2.1.1.2 La procédure d'autorisation 49
2.1.1.3 Les dispositions spécifiquement applicables à la technique de captation..... 51
2.1.1.4 La procédure applicable aux moyens de l'État soumis au secret de la défense nationale..... 54

2.1.2 La captation opérée par les services de renseignement 55

2.1.2.1 La procédure d'autorisation 57
2.1.2.2 Les dispositions spécifiquement applicables à la technique de captation des données informatiques 60
2.1.2.3 Les services autorisés à recourir à la technique de captation 62

Conclusion 67

2.2 L'accès aux données inaccessibles ou inintelligibles au cours de la procédure judiciaire 69

2.2.1 L'accès au support contenant des données informatiques 71

2.2.2 La mise au clair des données chiffrées nécessaires à la manifestation de la vérité 73

2.2.2.1 Les modalités encadrant les opérations techniques de mise au clair 74
2.2.2.2. Les spécificités encadrant le recours aux moyens de l'État soumis au secret de la défense nationale 77

Conclusion 80

2.3 Les incidences du droit européen 82

2.3.1 Le droit du Conseil de l'Europe 82

2.3.1.1 La Convention de Budapest sur la cybercriminalité 82
2.3.1.2 La jurisprudence de la Cour européenne des droits de l'homme en matière de captation de données informatiques 84
2.3.1.3 La jurisprudence de la Cour européenne des droits de l'homme en matière d'accès au support de données ou de mise au clair de données chiffrées 87

Conclusion 90

2.3.2 Le droit de l'Union européenne 91

2.3.2.1 La directive 2002/58 (« directive Vie Privée ») 91
2.3.2.2 La directive 2016/680 (directive « Police-Justice ») 95
2.3.2.3 La directive 2014/41 relative à la décision d'enquête européenne 100
2.3.2.4 Le règlement 2022/0722 (« règlement sur la liberté des médias ») 102

Conclusion 106

Conclusion de la Partie 1 109

PARTIE 2 : LE CADRE JURIDIQUE DE LA VULNÉRABILITÉ EXPLOITABLE 111

1. Le statut de la vulnérabilité exploitable au titre des atteintes aux STAD 116

1.1 La création d'une infraction de moyen 117

1.1.1 Le statut du chercheur contractuel 120

1.1.2 Le statut du chercheur non contractuel 121

Conclusion 125

1.2 Les aménagements relatifs à la sécurité nationale 126

1.2.1 L'irresponsabilité pénale des agents chargés de la défense des systèmes d'information : la vulnérabilité exploitable comme moyen défensif 126

1.2.2 L'irresponsabilité pénale des services de renseignement : la vulnérabilité exploitable comme moyen offensif 128

Conclusion 131

2. Les autres règles régissant le statut des vulnérabilités exploitables 133

2.1 Le cadre applicable aux dispositifs techniques de captation de données informatiques 133

2.1.1 La règlementation nationale relative à la fabrication et à l'acquisition de dispositifs techniques 134

2.1.2 La règlementation européenne applicable aux dispositifs techniques en tant que biens de cybersurveillance 138

2.1.2.1 Les biens énumérés à l'annexe I du règlement 140
2.1.2.2 Les biens non énumérés par l'annexe I du règlement 141
2.1.2.3 La procédure d'autorisation d'exportation 143

Conclusion 145

2.2 L'autonomisation du cadre juridique des vulnérabilités exploitables utiles aux services de police judiciaire et de renseignement 147

2.2.1 Le cadre juridique des vulnérabilités jour zéro en matière de police et de renseignement 148

2.2.1.1 Les obligations nationales et européennes relatives à la gestion des vulnérabilités exploitables 149
2.2.1.2 La vision européenne de la gestion des vulnérabilités jour zéro par les services judiciaires ou de renseignement 153

2.2.2 La création de vulnérabilités intrinsèques : les portes dérobées 158

Conclusion 162

Conclusion de la Partie 2 164

BIBLIOGRAPHIE 167

Liste des principales abréviations

CA	Cour d'appel
CAA	Cour d'appel administrative
C. cass	Cour de cassation
Cons. const.	Conseil constitutionnel
CE	Conseil d'Etat
Ch. crim	Chambre criminelle (Cour de cassation)
CJUE	Cour de justice de l'Union européenne
CEDH	Cour européenne des droits de l'homme
CPP	Code de procédure pénale
CSI	Code de la sécurité intérieure
JOUE	Journal officiel de l'Union européenne
JORF	Journal officiel de la République française
STAD	Système de traitement automatisé de données

Introduction

Le projet REV (Recherche et Exploitation des Vulnérabilités) a pour objectif principal, l'étude des vulnérabilités présentes dans les systèmes informatiques, tels que ceux des objets connectés et des smartphones. Pour ce faire, le projet vise à analyser les attaques possibles sur ces systèmes informatiques, dont la complexité ne cesse de croitre, à la fois au niveau matériel, logiciel et interfaces de communication (Web et IoT). Les résultats de l'étude pourront avoir de multiples finalités : forensique de systèmes complexes, extraction de données par les forces de l'ordre, renforcement de la sécurité des systèmes informatiques. Ce projet soulève également des questions éthiques et juridiques sur le traitement des vulnérabilités informatiques par les chercheurs, les services de renseignement et de police judiciaire.

De ce fait, le lot 5 du projet REV s'appliquera à fournir une analyse de ces enjeux éthiques et juridiques avec un premier livrable, notamment, sur l'état de l'art de l'encadrement juridique de la vulnérabilité. Cette étude ne saurait être effectuée sans aborder les composantes européennes qui influencent le cadre normatif national. En effet, la France, comme beaucoup d'États européens, fait partie de l'Union européenne et est membre du Conseil européen. À cet égard, elle doit répondre aux obligations qui lui incombent, en vertu de son appartenance à ces organisations internationales. Ces obligations, disséminées dans des domaines variés, ont une incidence sur la manière dont le cadre juridique de la vulnérabilité est construit en droit français.

Le terme « *vulnérabilité* » recoupe diverses définitions, selon les textes nationaux ou européens, strictement normatifs ou doctrinaux. Elle est également à rapprocher de la « *faille de sécurité* », la différence entre les deux n'étant pas strictement établie. Par exemple, dans le CyberDico de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), publié le 16 juillet 2024 et mis à jour le 5 décembre 2024[1], la vulnérabilité est une « *faille de sécurité pouvant affecter un logiciel, un système d'information ou encore un composant matériel. Elle peut servir de porte d'entrée pour les acteurs malveillants s'ils parviennent à l'exploiter. Les vulnérabilités sont généralement corrigées lors de mises à jour ou par des correctifs publiés par les éditeurs* ». La faille de sécurité, quant à elle, est une « *vulnérabilité dans un système*

[1] CyberDico de l'ANSSI FR/EN, publié le 16 juillet 2024, mis à jour le 05 décembre 2024.

informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient ».

Selon le CyberDico de l'ANSSI, une « *faille de sécurité* » est une « *vulnérabilité informatique* », et inversement. Cependant, il met l'accent sur le fait que la vulnérabilité peut servir de porte d'entrée si elle est exploitée, tandis que la faille de sécurité permet de porter atteinte au fonctionnement normal d'un système informatique. L'une est davantage rédigée au conditionnel, elle « *peut être exploitée* », l'autre « *permettant de porter atteinte* ». Cela étant dit, les différences sont subtiles et rendraient compliquée la lecture s'il fallait faire une stricte distinction entre les deux. De ce fait, il conviendra d'employer uniquement les termes « *vulnérabilités informatiques* ».

Par ailleurs, toute vulnérabilité exploitable n'est pas nécessairement exploitée. L'Union européenne fait cette distinction dans le règlement sur la cyberrésilience[2]. Il existe la vulnérabilité (« *une faiblesse, une susceptibilité ou une faille d'un produit comportant des éléments numériques qui peut être exploitée par une cybermenace* »)[3], la vulnérabilité exploitable (« *une vulnérabilité susceptible d'être utilisée efficacement par un adversaire en conditions de fonctionnement effectives* »)[4] et la vulnérabilité activement exploitée (« *une vulnérabilité pour laquelle il existe des preuves fiables qu'elle a été exploitée par un acteur malveillant dans un système sans l'autorisation du propriétaire du système* »)[5].

La distinction entre la vulnérabilité informatique exploitée et la vulnérabilité informatique exploitable est apparue particulièrement pertinente. En effet, selon leur statut, elles ne sont pas encadrées de la même manière. Cela est d'autant plus vrai qu'en droit, la vulnérabilité n'est pas toujours mentionnée de façon directe. Elle existe et est encadrée indirectement, par exemple, à travers les dispositifs techniques qui permettent son exploitation, ou les opérations effectuées sur ou par le biais de systèmes informatiques, où elle peut être un élément essentiel de réussite.

[2] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828, *JOUE* L, 20 novembre 2024 (Règlement sur la cyberrésilience).
[3] *Ibid*., art. 3, par. 40.
[4] *Ibid*., par. 41.
[5] I*bid*., par. 42.

Par exemple les récentes actualités, notamment les affaires Pegasus[6] et Encrochat[7], montrent que les services de renseignement ou de police judiciaire utilisent des vulnérabilités jour zéro, vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif, pour surveiller les individus ou extraire des données informatiques. Comment ces vulnérabilités jour zéro sont appréhendées par le droit ? La question se pose puisque les impératifs en matière de sécurité des systèmes d'information se font de plus en plus pressants, alors que les chercheurs en vulnérabilités ont un statut encore ambigu et que ce type de vulnérabilité demeure utile, sinon nécessaire, pour les autorités nationales.

Sur la base des considérations ci-dessus explicitées, il a été décidé que l'état de l'art du cadre juridique des vulnérabilités informatiques serait scindé en deux parties. L'une sur les vulnérabilités exploitées, et l'autre sur les vulnérabilités exploitables.

Le cadre de la vulnérabilité exploitée est découpé les utilisations frauduleuses, sans autorisations, et les utilisations autorisées de façon conditionnelle, par les autorités nationales notamment. Il convient de préciser que « *l'utilisation de vulnérabilités* » ne saurait se limiter à l'objectif de l'intrusion ou de l'extraction de données. Dans le cas du chiffrement, transformation cryptographique de données en utilisant un cryptogramme[8], la mise au clair des données, dont la lisibilité aurait été restreinte et protégée, peut bénéficier des vulnérabilités créées par défaillances cryptographiques ou présentes dans le protocole de chiffrement.

Par la suite, le cadre de la vulnérabilité exploitable traitera plus largement de l'enjeu de la sécurité informatique, la recherche sans exploitation ultérieure, mais également de la « possession » de vulnérabilités informatiques sans exploitation personnelle, de l'échange et de la commercialisation de ces dernières, en passant par la question des équipements et dispositifs techniques qui permettent l'exploitation ultérieure. Enfin, sera également abordé sous un angle plus critique, les portées dérobées ou le

[6] « L'affaire Pegasus » fait référence aux révélations du 18 juillet 2021, portant sur l'utilisation d'un logiciel espion israélien *Pegasus*, pour espionner plusieurs individus dans différents pays, la France en faisant partie. Voir aussi (Article)

[7] « L'affaire Encrochat » fait référence aux opérations menées par les autorités françaises, pour démanteler les réseaux criminels qui utilisaient EncroChat, service de télécommunication chiffrée néerlandaise, et qui ont débouché sur des poursuites judiciaires dans plusieurs pays, dont l'Allemagne. Voir aussi (Article)

[8] CyberDico de l'ANSSI FR/EN, mis à jour le 5 décembre 2024, *op. cit.*

signalement des vulnérabilités découvertes par les autorités nationales, lorsque celles-ci sont utiles à l'exercice de leurs missions.

Enfin, les différents cadres juridiques abordés par ce livrable recoupent plusieurs sources du droit, nationale comme européenne. Ce sont principalement le droit de l'Union européenne et le droit du Conseil de l'Europe qui, du point de vue européen, apportent des contraintes supplémentaires à la latitude des autorités publiques pour exercer leurs missions. Cependant la structure même de ces organisations influence les capacités dont elles disposent pour réguler ce champ.

Le Conseil de l'Europe :

Organisation internationale fondée en 1949 par divers pays européens, dont la France[9], le Conseil de l'Europe a pour mission la défense des droits humains par l'adoption d'instruments contraignants, tels que des conventions, et par la création d'un corpus juridique de référence, avec des recommandations, des lignes directrices. Tous les membres du Conseil de l'Europe doivent être partis à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CSDHLF), autrement appelée Convention européenne des droits de l'Homme. Ils doivent de plus avoir reconnu la compétence de la Cour européenne des droits de l'Homme pour le respect de sa mise en œuvre. Selon les termes de l'article 34 de la Convention, *« la Cour peut être saisie d'une requête par toute personne physique, toute organisation non gouvernementale ou tout groupe de particuliers qui se prétend victime d'une violation par l'une des hautes parties contractantes des droits reconnus dans la Convention ou ses protocoles* ».

Les jurisprudences rendues par la Cour ont une portée diffuse. Bien qu'elles aient pour objet d'aboutir ou non à la condamnation d'une haute partie contractante, elles forment ensemble un référentiel cohérent pour expliciter la portée des droits garantis, et les conditions des limitations autorisées.

En outre, certaines conventions sont également ouvertes à signature à des États non-membres du Conseil de l'Europe. Ces textes posent généralement des exigences minimales sur un sujet donné, afin que les États adoptent les mesures législatives pour les incorporer en droit interne. Elles doivent être « transposées » au niveau national, et ne s'appliquent pas telles quelles. Les principes jurisprudentiels dégagés par la CEDH, en revanche, s'appliquent directement aux États.

[9] La Belgique, le Danemark, la France, l'Irlande, l'Italie, le Luxembourg, les Pays-Bas, la Norvège, la Suède et le Royaume-Uni. En 2025, 46 États européens sont membres du Conseil de l'Europe.

L'Union européenne :

L'Union européenne est constituée de plusieurs organes et entités, dont les compétences et les capacités à régir le droit national varient.

Ces variations sont notamment structurées conformément au principe de répartition des compétences. Selon l'article 2 du traité sur le fonctionnement de l'Union européenne, il existe des compétences exclusives au bénéfice de l'Union. Dans ce cas, les États ne peuvent prendre des actes juridiquement contraignants que s'ils y sont directement habilités. Il existe aussi des compétences partagées, les États exercent leur compétence dans la mesure où l'Union n'a pas exercé la sienne, et des compétences d'appui, où l'Union peut soutenir les États sans remplacer leur compétence[10].

Les États bénéficient également de domaines réservés, notamment la sécurité nationale, pour lesquels l'Union ne peut légiférer. En effet, selon les termes de l'article 4 du traité sur l'Union européenne, « *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* »[11]. Ce domaine réservé influence nécessairement l'applicabilité et l'application du droit de l'Union en ce qui concerne les activités des services de renseignement.

Aux fins de ses missions, l'Union européenne peut adopter, entre autres, des directives et des règlements. La directive ne s'applique pas telle quelle, les États doivent adopter des actes de transpositions. Cet instrument à l'avantage d'être relativement souple tout en amorçant l'harmonisation des systèmes juridiques des États membres. Le règlement est un instrument bien plus rigide, qui s'applique directement sans nécessiter de transposition.

[10] Art. 2, Traité sur le fonctionnement de l'Union européenne (TFUE) (version consolidée) du 25 mars 1957, *JOUE* 7 juin 2016.
[11] Art. 4, Traité sur l'Union européenne (TUE) (version consolidée) du 13 décembre 2007, *JOUE,* 26 octobre 2012.

Lorsqu'ils mettent en œuvre le droit de l'Union, les États membres doivent respecter la Charte des droits fondamentaux de l'Union européenne[12], dont la portée et la valeur juridique ont été renforcées par le traité de Lisbonne en 2009[13]. En cas de non-respect de ces droits par un texte européen ou un texte national mettant en œuvre ces textes, une personne peut se prévaloir de la Charte, pour modifier ou faire annuler celui-ci. Certaines conditions doivent être remplies pour ce faire.

Enfin, dernière spécificité pertinente pour l'analyse ci-dessous, il existe différentes procédures devant la CJUE, dont l'issue a participé à créer le corpus juridique applicable en matière de vulnérabilités exploitées par les services de police judiciaire et de renseignement. Selon la procédure engagée, la CJUE ne dispose pas de la même marge de manœuvre, son appréciation n'a pas les mêmes conséquences. Ces procédures sont :

- **Le renvoi préjudiciel**, procédure par laquelle une juridiction nationale au cours d'une procédure interne, sous l'impulsion d'une partie au procès ou du magistrat, demande à la CJUE l'interprétation d'un acte de l'Union, souvent, vis-à-vis d'une disposition nationale contestée. L'interprétation de la CJUE lie la juridiction nationale, mais elle ne détermine pas l'issue de la procédure interne. L'interprétation lie également les juridictions nationales des autres États membres.
- **Le recours en annulation**, procédure par laquelle un requérant demande l'annulation d'un acte de l'Union. L'acte annulé n'est plus opposable aux États membres et aux destinataires de celui-ci. Ce recours peut être initié par un particulier ou par un État membre.
- **Le recours en manquement**, procédure qui permet de contrôler le respect par les États membres, des obligations qui leur incombent en vertu du droit de l'Union. Il peut être initié par la Commission européenne, ou par un autre État membre.

Ainsi, contrairement à la jurisprudence de la Cour européenne des droits de l'homme, celle de la Cour de justice est généralement circonscrite à la fois au contexte de la procédure nationale en cours et à la fois à l'objet de la norme européenne que la juridiction nationale souhaite expliciter. L'analyse qui sera faite du droit de l'Union dans ce livrable portera autant sur les textes que les interprétations jurisprudentielles qui ont été délivrées.

[12] Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000, *JOCE* C 364/01, (Charte DFUE).

[13] La valeur juridique de la Charte DFUE est égale à celle des traités, depuis le 1er décembre 2009.

Après ces quelques précisions structurelles pour faciliter la compréhension des sources européennes, il conviendra d'analyser dans une première partie le cadre juridique des vulnérabilités exploitées (**Partie 1**) puis, dans une deuxième, le cadre juridique des vulnérabilités exploitables (**Partie 2**).

PARTIE 1 : Le cadre juridique de la vulnérabilité exploitée

La vulnérabilité pour laquelle il existe des preuves qu'elle est activement exploitée n'est pas directement encadrée par le droit. Elle n'est appréhendée qu'à travers les différents actes pouvant résulter de cette exploitation : intrusion dans un système d'information, entrave à son bon fonctionnement, altération des données contenues dans celui-ci (de leur disponibilité, de leur fiabilité, de leur intégrité, de leur confidentialité) ; effectués par différents acteurs : services de renseignement ou de police judiciaire, cyberattaquants, particuliers ; poursuivant différentes finalités : surveillance des individus (dans le cadre d'enquêtes ou de renseignement, dans le cadre privé, dans le cadre professionnel), contre-espionnages, investigations numériques, gains financiers ou personnels[14].

La légalité de l'exploitation dépend davantage de la légitimité des finalités poursuivies, la qualité de l'exploitant ayant par ailleurs des incidences fondamentales sur celle-ci, que de l'outil utilisé pour l'exploitation. Ainsi, l'analyse du cadre juridique de la vulnérabilité exploitée distingue structurellement les exploitations strictement interdites, celles dont la qualité de l'acteur et les finalités poursuivies placent l'exploitation en dehors du cadre légal, des exploitations autorisées sous conditions, celles qui bénéficient d'aménagements juridiques en raison de la qualité de l'acteur et des finalités poursuivies.

Le cadre juridique des exploitations interdites est, en droit interne, fixé par les dispositions du code pénal.

Il s'agit d'un cadre qui se construit tout d'abord, au travers des articles 323-1 à 323-3, relatifs aux atteintes aux systèmes de traitement automatisé de données, présents dans un chapitre éponyme au sein du code pénal. Le chapitre est constitué de plusieurs articles, cependant, seuls les articles 323-1 à 323-3 intéressent spécifiquement le cadre juridique des infractions susceptibles d'être le fait d'une vulnérabilité exploitée.

Ensuite, les articles 226-1 et 226-15, traitant respectivement des atteintes à l'intimité d'autrui et des atteintes au secret des correspondances, sont également pertinents en ce que les infractions qui y sont inscrites peuvent être réalisées par le biais de l'exploitation effective de vulnérabilités informatiques. Ces deux infractions sont inscrites au sein du code pénal également, dans le chapitre relatif aux atteintes à la personnalité.

[14] Liste non exhaustive.

Il faudra ainsi distinguer l'encadrement juridique de la vulnérabilité informatique exploitée, par le biais des atteintes aux systèmes de traitement automatisé de données, de celui par le biais des atteintes à la personnalité.

De plus, le droit pertinent en la matière se nourrit du corpus normatif européen. Au niveau du Conseil de l'Europe, l'essentiel de l'apport provient de la Convention sur la cybercriminalité du 23 novembre 2001[15].

Entrée en vigueur le 1er juillet 2004, cette Convention est « *le premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques, traitant en particulier des infractions portant atteinte aux droits d'auteurs, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Il contient également une série de pouvoirs et de procédures, telle que la perquisition de réseaux informatiques et l'interception* »[16]. Son objectif est de « *poursuivre une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale* »[17]. La Convention est un instrument global, permettant de recouper différentes recommandations qui avaient été déjà publiées par le Conseil de l'Europe[18], et élargissant par ailleurs sa signature aux États non-membres de l'organisation.

Au niveau de l'Union européenne, la directive 2013/40 du 12 août 2013 relative aux attaques contre les systèmes d'information[19] fixe « *des règles minimales concernant la définition des infractions pénales et les sanctions en matière d'attaques contre les systèmes d'information. Elle vise également à faciliter la prévention de ces infractions et à améliorer la coopération entre les autorités judiciaires et les autres autorités*

[15] Convention STE n° 185 du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité, (Convention sur la cybercriminalité).
[16] *Ibid*., détails du traité n° 195.
[17] *Ibidem.*
[18] Conseil de l'Europe, Recommandation n°R(89)9 du Comité des Ministres aux États membres sur la criminalité en relation avec l'ordinateur (Adoptée par le Comité des Ministres le 13 septembre 1989 lors de la 428e réunion des Délégués des Ministres ; Recommandation n°R(95)13 du Comité des Ministres aux États membres relative aux problèmes de procédure pénale liées à la technologie de l'information (Adoptée par le Comité des Ministres le 11 septembre 1995 lors de la 543e réunion des Délégués des Ministres).
[19] 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, *JOUE L 218/8*, 14 août 2013 (Directive 2013/40).

compétentes »[20]. Par ailleurs, ce texte étant une directive, son contenu n'est pas opposable tel quel à l'instar d'un règlement, aux États membres de l'Union européenne. Il a été transposé par divers décrets, lois et arrêtés[21].

Enfin, il convient de mentionner la Convention de lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, de l'Organisation des Nations unies, adoptée le 27 novembre 2024[22]. Il s'agit du premier instrument adopté par cette organisation. Les dispositions de celui-ci reprennent en partie la Convention sur la cybercriminalité, bien qu'il laisse une importante marge de manœuvre aux États parties. Puisqu'il est moins contraignant, et qu'il est similaire dans sa composition à la Convention du Conseil de l'Europe, il conviendra de se pencher sur cette dernière uniquement. Ce parti pris est également tiré du fait que la Convention onusienne n'est pas encore ouverte à la signature, son entrée en vigueur nécessitant une ratification par 40 États minimum.

Le cadre juridique des exploitations autorisées sous conditions dispose également d'une composante nationale et européenne.

En droit national, les recherches se concentrent notamment sur la captation de données informatiques, autorisée par le biais de deux articles. Dans le code de procédure pénale (ci-après, « CPP »), l'article 706-102-1 (Livre IV « *De quelques procédures particulières* », Titre XXV « *De la procédure applicable à la criminalité et à la délinquance organisées et aux crimes* », Chapitre II « *Procédure* », Section 6 « *Des autres techniques spéciales d'enquête* », Paragraphe 4 « *De la captation des données informatiques* ») et au sein du code de la sécurité intérieure (ci-après, « CSI »), l'article L.853-2 (Livre III « *Du renseignement* », Titre V « *Des techniques de recueil de renseignement soumises à autorisation* », Chapitre III « *De la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques* »).

Les articles 230-1 à 230-5 du CPP relatifs à la mise au clair de données chiffrées (Livre Ier « *De la conduite de la politique pénale, de l'exercice de l'action publique et de l'instruction* », Titre IV « *Dispositions communes* », Chapitre Ier « *De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité* ») seront aussi abordés, puisque certaines techniques peuvent nécessiter l'exploitation de vulnérabilités informatiques. Un raisonnement similaire est appliqué pour l'accès au support de

[20] *Ibid*., art. 1er.

[21] Voir notamment la page dédiée aux transpositions nationales de la directive.

[22] Nations Unies, Convention A/79/460 de l'Assemblée générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, du 27 novembre 2024.

données informatiques, consacré à l'article 60-3 du CPP (Livre Ier « *De la conduite de la politique pénale, de l'exercice de l'action publique et de l'instruction* », Titre II « *Des enquêtes et des contrôles d'identité »,* Chapitre Ier « *Des crimes et des délits flagrants* »).

En droit européen la Convention sur la cybercriminalité sera également pertinente, de même que les jurisprudences de la CEDH, concernant le droit au respect de la vie privée et familiale inscrit à l'article 8 de la Convention européenne des droits de l'homme.

Plusieurs textes de l'Union européenne devront faire l'objet d'une analyse approfondie, notamment la directive 2002/58 (directive Vie Privée)[23], la directive 2016/680 (directive Police-Justice)[24], la directive 2014/41 (relative à la décision d'enquête européenne)[25], et le règlement 2022/0277 (règlement sur la liberté des médias)[26]. Les développements jurisprudentiels de la Cour de justice de l'Union européenne (ci-après « CJUE ») à l'égard de ces textes viendront compléter l'analyse de la portée de ceux-ci.

Puisque le droit pose une interdiction de principe, les autorisations demeurant des exceptions, il conviendra d'aborder les exploitations interdites (**1**), avant les exploitations autorisées sous conditions (**2**).

1. Les exploitations strictement interdites

Les exploitations interdites sont associées à différentes infractions, qui appartiennent, selon le code pénal, à deux catégories. Celles ayant pour finalité les atteintes aux biens, précisément aux systèmes de traitement automatisé de données (**1.1**), et celles ayant pour

[23] 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), *JOUE* L 201, 31 juillet 2002 (directive Vie-Privée).

[24] 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, *JOUE* L 119, 4 mai 2016 (Directive Police-Justice).

[25] Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, *JOUE* L 130, 1 mai 2014 (Directive 2014/41).

[26] Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement sur la liberté des médias), *JOUE* L, 17 avril 2024 (Règlement sur la liberté des médias).

finalité les atteintes à la personnalité, notamment à l'intimité d'autrui et au secret des correspondances (**1.2**).

1.1 Les exploitations ayant pour finalité les atteintes aux systèmes de traitement automatisé de données

L'exploitation de vulnérabilités peut être réprimée au titre des atteintes aux systèmes d'information.

En droit national, les infractions qui en découlent ont été créées par la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique[27], dite « *loi Godfrain* » du nom du député qui a déposé le projet de loi à l'Assemblée nationale. La loi portant réforme des dispositions du code pénal relatives à la répression des crimes et des délits contre les biens de 1992,[28] a par la suite repris la loi Godfrain et crée au sein du code pénal un chapitre nommé « *Des atteintes aux systèmes de traitement automatisé de données* ». Dans ce chapitre, les articles 323-1 à 323-3 couvrent les attaques pouvant être menées contre des systèmes de traitement automatisé de données. Avant tout développement deux points doivent être explicités.

Tout d'abord, ces trois articles ne traitent pas directement et uniquement de l'exploitation de vulnérabilités. Les infractions qui y sont consacrées ne spécifient pas d'éléments matériels relatifs à un moyen précis pour leur caractérisation.

Ensuite, il n'existe aucune définition stricte de l'expression « s*ystèmes de traitement automatisés de données* » dans les textes législatifs ou dans la jurisprudence. Certains juges du fond se basent sur une définition élaborée lors des travaux parlementaires. Absente de la version définitive pour son caractère restrictif et pour le risque d'obsolescence prématurée qu'elle faisait peser sur la Loi, la définition qualifiait de STAD « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes entrées-sorties et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* »[29].

[27] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, *JORF* n° 4 du 6 janvier 1988.
[28] Loi n° 92-685 du 22 juillet 1992 portant réforme des dispositions du Code pénal relatives à la répression des crimes et de délits contre les biens, *JORF* n° 169 du 23 juillet 1992.
[29] Rapport fait au nom de la commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale (1) sur la proposition de loi adoptée par l'Assemblée nationale, relative à la fraude informatique, 2 oct. 1987, p. 52

Ainsi, a été admis comme étant un « *système de traitement automatisé de données* » (ci-après « STAD ») par la jurisprudence [30]: le disque dur d'un ordinateur contenant le logiciel de comptabilité et les données d'un cabinet d'expertise comptable[31], le radiotéléphone, des systèmes d'exploitation de données au sein d'entreprises[32], un service télématique[33], l'annuaire électronique de France Télécom[34], le réseau de cartes France Télécom[35], le réseau Carte bancaire[36], un boitier composé d'une partie logicielle et d'une partie électronique à destination des engins agricoles[37], un logiciel[38] et bien entendu les systèmes d'information[39]. Au regard de ces exemples de qualifications jurisprudentielles, il est raisonnable de considérer que les téléphones portables, les tablettes et les objets connectés puissent être entendus comme étant des STAD.

En dehors des dispositions tirées de la loi Godfrain, leurs modifications successives et interprétations jurisprudentielles, la Convention sur la cybercriminalité du Conseil de l'Europe ainsi que la directive 2013/40 de l'Union européenne doivent également être prises en compte. Elles portent en effet, au moins en partie, sur les atteintes aux systèmes informatiques. Cependant la directive, arrivant après la loi Godfrain, n'a pas affecté le droit français qui était déjà plus protecteur que celle-ci. Elle est tout de même opposable aux États membres et c'est en cela qu'il est nécessaire de l'étudier.

Au regard des spécificités du champ européen, il convient de rappeler que les termes de « systèmes informatiques » ou de « systèmes d'information » ont une définition autonome, qui englobe les STAD au sens du droit national.

En effet, la Convention sur la cybercriminalité définit un système d'information, comme « *tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données* »[40]. La directive 2013/40 quant à elle, reprend exactement la

[30] Proposition de loi pour renforcer l'efficience de la lutte contre les attaques informatiques pour un monde numérique plus civilisé et donc plus fort, 11 mai 2011, n° 3412, p. 2.
[31] CA Douai, 7 octobre 1992, cité par Proposition de loi pour renforcer l'efficience de la lutte contre les attaques informatiques pour un monde numérique plus civilisé et donc plus fort, préc.
[32] CA Paris, 5 octobre 1994 ; TGI Paris, 1er juin 2007, *ibid.*
[33] CA Paris, 5 avril 1994, *ibid.*
[34] TC Brest, 14 mars 1995, *ibid.*
[35] TC Paris, 26 juin 1995, *ibid.*
[36] TC Paris, 25 février 2000
[37] CA Douai, 11 mai 2023, n° 15-06278.
[38] C.cass., ch. crim., 7 janvier 2020, n° 18-84.755
[39] C.cass., ch. crim., 16 janvier 2018, n° 16-87.168
[40] Art. 1, a), Convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185).

même tournure que la Convention pour définir le système d'information, en ajoutant également « *les données stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci* »[41].

Dans la mesure où le fait d'assurer un traitement automatisé de données est un critère obligatoire de qualification d'un système d'information, le système chargé de cette opération peut être considéré comme une composante indissociable de celui-ci. Sur la base de ce constat, l'étude des deux textes précités semble justifiée.

Enfin, il est important de noter que le droit national en vigueur comporte des différences majeures au niveau de la rédaction des articles qui encadrent les infractions. Parmi ces différences, le caractère « frauduleux » ou non, de l'acte réprimé. Une telle distinction n'est pas strictement présente dans les textes européens. Le choix a été fait, de traiter distinctement, les infractions nécessitant un aspect frauduleux (**1.1.1**), de celles ne l'imposant pas (**1.1.2**). Elles ont systématiquement une composante nationale (**a**), et européenne (**b**).

1.1.1 Les atteintes sanctionnées au titre d'une exploitation frauduleuse de vulnérabilités

Les infractions pour lesquelles le caractère frauduleux de la commission est nécessaire sont visées par les articles 323-1 (**1.1.1.1**) et 323-3 (**1.1.1.2**) du code pénal.

1.1.1.1 L'accès ou le maintien dans tout ou partie d'un STAD

a) Dispositions en droit national

L'article 323-1 du code pénal, dans sa version en vigueur depuis le 26 janvier 2023, tel que modifié par l'article 6 de la loi d'orientation et de programmation du ministère de l'Intérieur de 2023[42], punit de trois ans d'emprisonnement et de 100 000 euros d'amende, « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie*

[41] Art. 2, par a), directive 2013/40.
[42] Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur (1), *JORF* n° 21 du 25 janvier 2023.

d'un système de traitement automatisé de données »[43]. L'article distingue l'infraction de l'accès de celle du maintien, tout en instaurant une peine commune. Le champ matériel de ces infractions a été principalement explicité par la jurisprudence.

Les deux infractions ne sont pas liées et peuvent être caractérisées de façon dissociée. Dès lors, trois cas hypothétiques sont envisagés. Le premier est l'accès frauduleux ainsi que le maintien frauduleux. Le deuxième est l'accès frauduleux sans maintien frauduleux, en raison du retrait direct de la personne, du STAD auquel il avait préalablement accédé frauduleusement. Dans ce cas, l'infraction de l'accès frauduleux est caractérisée, mais pas celle du maintien. Enfin, troisième cas, le maintien frauduleux résultant de l'accès non frauduleux. Cette hypothèse, ayant déjà fait l'objet d'une jurisprudence[44], est également juridiquement valable. Dans cette affaire, l'individu avait accédé au STAD de l'ANSES[45] par erreur, en exploitant une vulnérabilité qui résultait d'une défaillance technique concernant les certificats existants dans le système. La Cour de cassation a estimé, que l'accès par erreur n'entrainait pas une impossibilité de caractériser l'infraction du maintien frauduleux, dès l'instant où l'individu, constatant par les suites de sa navigation sur le STAD la présence d'un contrôle d'accès ou de signes d'un accès restreint, acquérant conscience de son accès frauduleux, se maintenait sur le STAD.

Le caractère frauduleux de l'acte devient l'élément moral de l'infraction, l'intention coupable. Une intention coupable est caractérisée chez la personne qui *« sachant qu'elle n'y est pas autorisée, accède (se maintien) frauduleusement par quelque moyen que ce soit à ce système* »[46]. La simple exploitation d'une vulnérabilité, comme explicitée ci-dessus, n'est pas suffisante à déceler l'élément moral. En effet, en 2002, la Cour d'appel de Paris avait estimé qu'il ne pouvait être reproché à un internaute « *d'accéder aux, ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès »*[47]. En l'espèce, cet internaute avait utilisé les fonctionnalités du navigateur web NETSCAPE, pour pénétrer sur le site Internet de la société TATI,

[43] Art. 323-1, al. 1er, code pénal (CP).
[44] C.cass., ch. crim., 20 mai 2015, n° 14-81.336.
[45] Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail.
[46] C.cass., ch. crim., 5 avril 2022, n° 21-83.590.
[47] CA Paris, 12e ch., 30 octobre 2002, n° 02/04867, *Tati c. Kitetoa.*

suffisamment profondément pour parvenir au répertoire des fichiers de données nominatives et à ces fichiers eux-mêmes.

Une charge pèse alors sur les propriétaires et hébergeurs de STAD, de mettre en place des obstacles à l'accès, traduits en procédés de sécurisation, et des indications aptes à aiguiller l'individu sur les autorisations d'accès et de maintien sur le STAD.

L'alinéa 2 de l'article 323-1 est rédigé ainsi « *lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 euros d'amende* ». Au titre de cet alinéa, la suppression, la modification ou l'altération des données ne nécessite pas d'avoir été effectuée avec une intention délictueuse. Ces conséquences, même accidentelles, sont une circonstance aggravante devant être appréciée en combinaison avec l'alinéa 1er lorsque l'accès ou le maintien frauduleux ont été caractérisés.

Enfin, l'article 9 de la loi relative à la protection de l'identité de 2012[48] a introduit une autre infraction au sein de l'article, à l'alinéa 3, qui porte les peines à sept ans d'emprisonnement et 300 000 euros d'amende « *lorsque les infractions ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État* ». Ces STAD peuvent être, à titre d'exemple, la base centrale de titres sécurisés[49], le fichier des empreintes génétiques (FNAEG)[50].

b) Dispositions en droit européen

La Convention sur la cybercriminalité du Conseil de l'Europe, ratifiée par la France en 2005,[51] impose aux Parties, des mesures à prendre au niveau national. En plus de l'implémentation des dispositions de la Convention en droit interne et l'opposabilité de celle-ci, le traité sert de fondement juridique pour la coopération internationale : il

[48] Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, *JORF* n° 75 du 28 mars 2012.
[49] Proposition de loi relative à la protection de l'identité (n° 682), enregistrée à la Présidence du Sénat le 27 juillet 2010, p. 6.
[50] Rapport fait au nom de la Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République sur la proposition de Loi (n° 3471), adoptée par le Sénat, relative à la protection de l'identité, enregistrée à la Présidence de l'Assemblée nationale le 29 juin 2011, p. 35.
[51] Loi n° 2005-493 du 19 mai 2005 autorisation l'approbation de la Convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (1), *JORF* n° 116 du 20 mai 2005.

permet aux Parties de mettre un commun leurs expériences, de nouer des relations spécifiques, notamment pour répondre aux situations d'urgence[52].

Cela étant dit, les obligations qui traitent de l'intrusion sur un système d'information, sont au chapitre II (« *Mesures à prendre au niveau national* »), Section 1 (« *Droit pénal matériel* »), Titre 1 : « *Infraction contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques* ».

L'article 2, sur l'accès illégal, dispose notamment que « *chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique* ». Le terme de deux systèmes interconnectés fait référence à la mise en réseau informatique. L'accès illégal, résultant de l'exploitation d'une vulnérabilité, rentre dans le champ de la violation des mesures de sécurité.

La Convention laisse une certaine marge de manœuvre aux États pour décider de la portée de l'élément d'intentionnalité. En effet, contrairement à la notion « d'accès frauduleux » qui implique nécessairement que l'individu ait eu connaissance de l'absence de droit de son accès, les termes « l'accès intentionnel et sans droit » peuvent être entendus différemment. L'accès doit certes être intentionnel, mais la circonstance qu'il fut sans droit semble être caractérisable indépendamment de la connaissance pour l'individu, de cette absence d'autorisations.

Par ailleurs, la Convention ne traite pas du maintien dans le STAD. Celui est seulement sous-entendu par la référence aux vols de données.

La directive 2013/40/UE relative aux attaques contre les systèmes d'information traite de l'intrusion dans un STAD par le biais de son article 3, qui dispose que les États prennent *« les mesures nécessaires pour ériger en infraction pénale punissable l'accès sans droit, lorsqu'il est intentionnel, à tout ou partie d'un système d'information, lorsque l'acte est commis en violation de mesure de sécurité ou du moins lorsqu'il ne s'agit pas de cas mineurs* ». Ici, la rédaction de l'article clarifie la relation entre

[52] Comité de la Convention sur la cybercriminalité (T-CY), *La Convention de Budapest sur la cybercriminalité : avantages et impacts concrets*, T-CY (2020)16, Strasbourg, 13 juillet 2020, p. 3.

l'élément intentionnel et l'absence de droit. L'accès sans droit doit être intentionnel, ce qui implique la connaissance et la pleine conscience de l'illégalité de l'accès.

De plus, la directive précise la notion « *sans droit* », ce qui n'est pas le cas de la Convention. Il s'agit d'un « *comportement (...), y compris un accès, une atteinte à l'intégrité ou une interception, qui n'est pas autorisé par le propriétaire du système ou d'une partie du système ou un autre titulaire de droits sur celui-ci ou une partie de celui-ci, ou n'est pas permis par le droit national* »[53]. Théoriquement, la mention « *qui n'est pas permis par le droit* » allège la charge aux responsables du système, de devoir rendre explicite aux potentiels intrus, l'aspect illégal de leur acte. Cependant, l'intentionnalité de l'accès illégal implique que l'individu ait eu la connaissance et la pleine conscience de cette absence d'autorisations, ce qui implique, normalement, des obstacles matériels (procédés de sécurisation), ou/et des indications explicites. Par exemple, une mention visible à tout individu accédant, du statut requis pour bénéficier d'une autorisation d'accès.

Enfin, la directive pose un seuil de risque minimal au-delà duquel l'infraction visée à l'article 3 doit être transposée en droit interne. Il s'agit des cas mineurs, des faits où « *les dommages causés par l'infraction et/ou le risque pour les intérêts publics ou privés, tels que le risque pour l'intégrité d'un système informatique ou de données informatiques, ou pour l'intégrité, les droits ou les autres intérêts d'une personne, sont peu importants ou de nature telle qu'il n'est pas nécessaire d'appliquer une sanction pénale dans les limites du seuil légal ou que la responsabilité pénale soit engagée* »[54]. Il convient de rappeler que le droit français ne fait pas de distinction entre les cas mineurs et les cas majeurs. Ce seuil est un moyen pour l'Union européenne, de s'assurer que les États mettront en place en droit interne, au moins des règles minimales harmonisées[55].

1.1.1.2 Le traitement de données sur tout ou partie d'un STAD

a) Disposition en droit national

En droit national, l'exploitation d'une vulnérabilité est également réprimée lorsqu'elle a pour conséquence ou intention d'opérer un traitement illicite sur tout ou partie d'un STAD. En effet, l'article 323-3 du code pénal explicite que « *le fait d'introduire*

[53] *Ibid*., art. 2, sous d).
[54] Directive 2013/40, préc., § 11.
[55] *Ibid*., §1.

frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende ». Tout comme l'article 323-1 du code pénal, les peines sont portées à sept ans d'emprisonnement et 300 000 euros d'amende lorsque les infractions ont été commises à l'encontre d'un STAD à caractère personnel, mis en œuvre par l'État[56].

La différence principale de l'infraction posée à cet article de celle posée à l'article 323-1 alinéa 2, et qu'il n'est pas nécessaire que l'accès ou le maintien dans le STAD ait été frauduleux. Cette différence permet d'englober plus largement les individus dont la profession ou la circonstance particulière, leur accorde des droits d'accès au STAD, lequel ne serait alors pas frauduleux. Ce serait le cas du logiciel dont il aurait été accordé aux professionnels, une licence d'exploitation.

Ainsi, dans le cadre de l'exploitation d'une vulnérabilité aboutissant sur la caractérisation de l'infraction visée par l'article 323-3, les droits accordés aux individus ne peuvent avoir pour objet la possibilité d'effectuer l'extraction, la détention (…) de données dans le STAD en question[57]. Ainsi, il ne suffit pas que l'altération soit faite dans un but frauduleux. L'aspect frauduleux doit être celui de l'altération en elle-même. Par exemple, la Cour de cassation a estimé dans un arrêt du 7 janvier 2020[58], que l'utilisation d'un logiciel qui facilitait la fraude fiscale, en raison de sa fonctionnalité qui permettait de faire disparaître des lignes d'écritures relatives à des ventes payées en espèce (selon certaines conditions), ne suffisait pas à caractériser une infraction au titre de l'article 323-3.

Dans cet arrêt, la Cour a retenu une applicabilité très restrictive de l'article en disant « *que les atteintes aux STADS prévues (à l'article 323-3), ne sauraient être reprochées à la personne qui, bénéficiant des droits d'accès et de modification des données, procède à des suppressions de données, sans les dissimuler à d'éventuels autres utilisateurs du système* ». Il ressort à la lecture de cette phrase, que l'altération doit être sans droit, intentionnelle et irréversible.

[56] Art. 323-3 CP, al. 2.
[57] Voir en ce sens, C. cass., ch. crim., 8 décembre 1999, n° 98-84.752.
[58] Voir en ce sens, C. cass., ch. crim., 7 janvier 2020, n° 18-84.755.

b) Disposition en droit européen

La Convention sur la cybercriminalité du Conseil de l'Europe traite de ce cas dans son article 4 « Atteinte à l'intégrité des données » qui dispose que « *chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. Une Partie peut se réserver le droit d'exiger que le comportement décrit entraîne des dommages sérieux* ».

Cet article ne couvre pas, contrairement au droit national, la détention, la transmission et la reproduction de données informatiques. Il concède au surplus, la possibilité d'un seuil minimal de dommages sérieux.

L'article 7 de la Convention sur la falsification informatique élargit les actes réprimés en matière d'altération des données. Rédigé ainsi, « *(…) pour ériger en infraction pénale (…), l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles* », l'article inclut les altérations de données effectuées dans un but précis. Une formulation reprise par l'article 8, paragraphe a), qui vise les altérations de données dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou autrui. Il peut s'agir des rançongiciels, des cyberattaques à but pécuniaire.

Les dispositions de la Convention confèrent une protection en dessous des standards français, qui couvrent plus largement les types d'altération réprimés, et qui n'imposent pas d'objectifs précis aux actions effectuées.

Il en va de même pour la directive 2013/40/UE, dont l'article 5 sur les atteintes illégales à l'intégrité des données, vise le fait « *d'effacer, d'endommager, de détériorer, d'altérer, de supprimer ou de rendre inaccessibles des données informatiques d'un système d'information lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs* ». Toutefois, le droit européen impose pareillement pour les infractions ci-dessus traitées en droit français, un caractère frauduleux à l'acte. Tel n'est pas le cas de l'infraction relative aux entraves au bon fonctionnement d'un STAD.

1.1.2 Les atteintes sanctionnées indépendamment du caractère frauduleux de l'exploitation

a) Disposition en droit national

En droit français, le caractère frauduleux de l'exploitation d'une vulnérabilité n'est pas requis lorsqu'il est question d'entrave ou de faussement d'un STAD. L'article 323-2 du code pénal, qui traite de ce cas, permet de punir de cinq ans d'emprisonnement et de 150 000 euros d'amende « *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données* ». L'article distingue l'entrave, le fait de paralyser ou de ralentir sensiblement le fonctionnement, de l'action qui tend à fausser, faire aboutir le STAD à un résultat différent de celui attendu. Sont visés par cet article, les attaques par déni de service[59], mais également l'envoi de messages massifs[60]. L'absence de mention du caractère frauduleux que doivent revêtir les actes permet d'englober également les erreurs ou négligences.

Par ailleurs, tout comme les articles 323-1 et 323-3 du code pénal, les peines sont majorées lorsqu'il est question d'un STAD à caractère personnel, mis en œuvre par l'État.

b) Disposition en droit européen

Au sein de la Convention sur la cybercriminalité, l'article 5 sur les atteintes à l'intégrité du système, dispose que « *chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques* ». La Convention pose un seuil de gravité au-delà duquel les Parties doivent adopter des mesures législatives, en plus des critères également présents dans les articles susmentionnés, de l'intentionnalité et de l'absence d'autorisation légale. Seule l'entrave est directement visée par l'article de la Convention, puisque le fait de fausser le fonctionnement du

[59] TGI Paris, 19 mai 2006.
[60] TGI Le Mans, 7 novembre 2003.

système est indirectement réprimé par l'article 8, paragraphe b) sur la fraude informatique.

Un article qui invite les Parties à ériger en infraction pénale le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui[61], par toute forme d'atteinte au fonctionnement d'un système. Toutefois, le fait de fausser ne peut résulter d'une erreur, puisqu'il doit être intentionnel, et ne peut être uniquement dans le but de nuire, puisqu'il doit y avoir des avantages financiers.

La directive 2013/40/UE, quant à elle s'éloigne quelque peu de ce principe sur les atteintes à l'intégrité d'un système. L'article 4 énonce à ce propos que « *les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable le fait de provoquer une perturbation grave ou une interruption du fonctionnement d'un système d'information, en introduisant, en transmettant, en endommageant, en effaçant, en détériorant, en altérant, en supprimant ou en rendant inaccessibles des données informatiques lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs* ». Les termes de *perturbation grave* renvoient au fait de fausser le fonctionnement d'un système. La définition n'ayant pas été strictement explicitée, les États membres ont bénéficié d'une certaine marge de manœuvre dans la transposition.

Toutefois, la directive et la Convention ont été rédigées dans des termes restrictifs comparés au droit national, puisque l'entrave, la perturbation grave, l'interruption de fonctionnement doivent être le résultat d'un traitement de données informatiques frauduleux (intentionnel et sans droit).

Cette circonstance est cohérente aux objectifs de ces deux outils de poser des exigences minimales aux États en termes de cybercriminalité. En outre, la France a doté son système pénal d'un arsenal réprimant les attaques aux STAD avant la création de ces deux textes, dont la parution n'a pas rendu nécessaire une modification rédactionnelle des articles nationaux.

[61] Dommages économiques ou financiers.

1.2 Les exploitations ayant pour finalité les atteintes à la personnalité

L'exploitation de vulnérabilités est également sanctionnée par le biais des atteintes à la personnalité, car celle-ci est susceptible de porter atteinte à la vie privée d'autrui et au secret des correspondances qui est, en réalité, une composante de la vie privée. Dans ce cas, l'exploitation n'est pas réprimée en ce qu'elle constitue une atteinte aux biens, mais pour les dommages qu'elle engendre à la personne. Cette appréhension plus large des préjudices potentiellement causés par l'exploitation de vulnérabilité présente deux avantages. Tout d'abord, en s'appliquant aux victimes simplement utilisatrices qui ne nécessairement propriétaires du STAD, la protection vis-à-vis des conséquences d'une exploitation interdite de vulnérabilités se retrouve renforcée puisque le spectre des victimes potentielles est élargi. Ensuite, elle permet de majorer les peines au regard de certains profils de victimes, tels que les mineurs, ou selon certains contextes, comme le cadre conjugal.

Les atteintes à la personnalité revêtent aussi une dimension européenne, avec la Convention européenne des droits de l'homme[62]. En effet son article 8, qui traite du droit à la vie privée et familiale, du domicile et de la correspondance, a fait l'objet d'importants développements jurisprudentiels pour le rendre adéquat aux évolutions technologiques[63]. Dès 1987, la CEDH s'est prononcée sur le cas de l'applicabilité de l'article 8 aux questions de protection des données personnelles[64]. Sa jurisprudence s'est étoffée depuis, au point de consacrer un guide de jurisprudence spécifique à la protection des données[65]. Ses interprétations peuvent être pertinentes en matière d'exploitation de vulnérabilités informatiques, qui ont pour conséquences une violation de l'article 8. Elles seront analysées en plus du droit national, dans le cas des atteintes à l'intimité de la vie privée d'autrui et des atteintes au secret des correspondances.

L'étude commencera par les dispositions de l'article 226-1 du code pénal relatives à l'intimité de la vie privée d'autrui (**1.2.1**), puis traitera l'article 226-15, sur les atteintes

[62] Convention (STCE n°005) du Conseil de l'Europe du 4 novembre 1950, de sauvegarde des droits de l'homme et des libertés fondamentales, (Convention EDH).
[63] BLAY-GRABARCZYCK (K.), « Vie privée et nouvelles technologies », *RDLF*, 2011, chron. n° 7.
[64] CEDH, 26 mars 1987, *Leander c. Suède*, n° 9248/81.
[65] Guide sur la jurisprudence de la Convention européenne des droits de l'homme, mis à jour le 29 février 2024.

au secret des correspondances (**1.2.2**). La Convention sur la cybercriminalité est aussi applicable à ce dernier cas.

1.2.1 Les sanctions relatives aux atteintes à l'intimité de la vie privée d'autrui

a) Disposition en droit national

L'article 226-1 du code pénal punit 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 : en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ; en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé ; 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 celles-ci.* »

L'alinéa 2 de l'article précise que le consentement de la personne est présumé lorsque les deux premiers actes susmentionnés ont été accomplis au vu et au su des intéressés, sans opposition de leur part. Lorsque la personne visée est mineure, le consentement doit émaner des titulaires de l'autorité parentale[66]. Enfin, les peines sont portées à 2 ans d'emprisonnement et 60 000 euros d'amende, lorsque les faits sont commis par le conjoint ou le concubin[67]. Majoration similaire lorsqu'ils sont commis au préjudice d'une personne dépositaire de l'autorité publique, chargée d'une mission de service public, titulaire d'un mandat électif public ou candidate à un tel mandat ou d'un membre de sa famille[68].

La mention de « procédé quelconque » est bien susceptible de couvrir l'exploitation d'une vulnérabilité informatique, si celle-ci a permis l'activation de la webcam ou du micro à distance, par exemple, ou si elle a permis d'accéder aux données de géolocalisation. Il n'est pas obligatoire que les données aient été enregistrées ou transmises par ailleurs, la simple captation, et, par extension, le simple fait d'accéder, est susceptible de caractériser l'infraction.

[66] Art. 226-1 CP, al. 3.
[67] *Ibid*., al. 4 (inclus les partenaires au sens du pacte civil de solidarité).
[68] *Ibid*., al. 5.

Puisque l'article impose que l'individu ait volontairement souhaité porter atteinte à la vie privée de la personne visée, le cas de l'exploitation de vulnérabilités par erreur ou par négligence lorsqu'elle a pour conséquence une atteinte, ne rentre pas dans le champ d'application de l'article. Toutefois, l'exploitation par erreur ou par négligence semble dans ce cas précis marginal au regard de la technicité requise pour, par exemple, activer une webcam ou un micro à distance.

Enfin, tel qu'énoncé par l'alinéa 1er de l'article 226-1, l'absence de consentement de la personne est un critère décisif. Ce critère permet notamment d'exclure du champ d'application de l'article certaines prestations de services qui impliquent parfois l'accès aux fonctionnalités d'un système d'information ou aux périphériques d'entrée. Par exemple, en cas de dépannage informatique.

Il est nécessaire de préciser qu'en outre de la responsabilité pénale au titre de l'article 226-1, l'exploitation d'une vulnérabilité attentant à la vie privée d'autrui peut également entraîner la responsabilité civile sur le fondement de l'article 9, alinéa 1 du code civil qui dispose que « *chacun a droit au respect de sa privée* ». Elle peut être engagée lorsqu'un individu par faute, erreur ou négligence cause un préjudice. Dès que le lien de causalité entre l'acte et le préjudice est établi, l'exploitation d'une vulnérabilité, même sans intention délictuelle, expose l'auteur à des poursuites pour réparation[69]. Cela inclut les cas où l'exploitation de vulnérabilités serait autorisée dans un cadre contractuel.

Précisions et interprétations jurisprudentielles :

Si le lieu privé doit être conçu comme un endroit qui n'est ouvert à personne sauf autorisation de celui qui l'occupe d'une manière permanente ou temporaire[70], le lieu public, est, quant à lui, celui accessible à tous sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions[71].

Les personnes morales ne peuvent se prévaloir de la protection offerte par l'article, qui ne concerne, dès lors, que les personnes physiques[72].

[69] Résorber le dommage, le faire disparaître, remise en l'état avant préjudice.
[70] CA Besançon, 5 janvier 1978, n° 9999.
[71] TGI Paris, 23 octobre 1986.
[72] C.cass,1ère civ., 17 mars 2016, n° 15-14.072.

L'acte délictueux doit concerner la vie privée de la personne au sens strict : ne sont pas visés des propos relatifs à la vie professionnelle[73], ou relatifs à des problèmes d'argent entre époux séparés[74].

Enfin, la complicité d'atteinte à la vie privée peut être retenue dans certains cas, notamment pour le fournisseur de services, selon la nature du moyen utilisé pour la commission de l'acte délictueux. Par exemple, la Cour de cassation a validé la complicité d'atteinte à la vie privée, qui avait été retenue pour le dirigeant d'une société spécialisée dans la sécurité des personnes dans la mesure où les outils utilisés par l'auteur, des branchements clandestins, constituaient par leur conception, leur objet et leur durée, une ingérence dans la vie privée[75].

b) Disposition en droit européen

La CEDH, dans ses interprétations de l'article 8 relatives au droit à la vie privée et familiale, du domicile et des correspondances, l'exploitation de vulnérabilités informatiques n'est pas appréhendée de manière directe.

Elle traite de ce cas au niveau de la surveillance étatique[76], qui implique parfois l'utilisation de logiciels espions, ces derniers exploitant des vulnérabilités non connues à ce jour, et au niveau des violences conjugales. Pour ce qui relève de la surveillance étatique et de l'encadrement de la Cour de ces techniques, l'analyse se fera ultérieurement, dans la section dédiée aux exploitations autorisées sous conditions.

En ce qui concerne le cadre de violences conjugales, la Cour a reconnu par un arrêt de 2020, la notion de « cyberviolence », qui est « *un aspect de la violence à l'encontre des femmes et des filles et (qui) peut se présenter sous diverses formes dont les violations informatiques de la vie privée, l'intrusion dans l'ordinateur de la victime et la prise, le partage et la manipulation des données et des images, y compris des données intimes* »[77]. Dans cette affaire, la Cour, en plus de s'exprimer explicitement sur l'exploitation de vulnérabilité à des fins d'atteintes à la vie privée, crée un précédent.

[73] C.cass, ch. crim., 16 janvier 1990, n° 89-83-075.
[74] C.cass, ch. crim. 20 mai 1977.
[75] C.cass, ch. crim., 7 octobre 1997, n° 96-81.485 : complicité d'atteinte à la vie privé retenue pour le dirigeant d'une société spécialisée dans la sécurité des personnes dans la mesure où les outils utilisés par l'auteur, des branchements clandestins, constituaient par leur conception, leur objet et leur durée, une ingérence dans la vie privée.
[76] Voir par exemple CEDH, 24 septembre 2024, *A.L. et E.J. c. France*, n^{os} 44715/20 et 47930/21.
[77] CEDH, 11 février 2020, *Burutuga c. Roumanie*, n^{o} 56867/15, §74.

Elle rappelle l'impact des nouvelles technologies sur les femmes dans le cas de violence conjugales, et les aménagements ou précautions, que doivent prendre les autorités nationales lorsqu'elles sont confrontées à de telles situations.

Dans ce contexte spécifique, en cas de plainte pour violences conjugales, les autorités compétentes doivent prendre en compte les atteintes à l'intimité de la vie privée d'autrui résultant de l'intrusion dans un ordinateur par l'exploitation de vulnérabilités, sans imposer le dépôt d'une plainte spécifique à ce sujet. L'exploitation de vulnérabilité et ses conséquences sont susceptibles d'être examinées *de facto.*

La circonstance aggravante au titre de l'alinéa 4 de l'article 226-1 du code pénal sur le cadre conjugal s'inscrit dans cette idée de protection des personnes vulnérables, notamment des femmes.

La reconnaissance de l'existence de la notion de *cyberviolence* et les principes de l'affaire *Burutuga c. Roumanie* de 2020 sont également applicables au secret des correspondances.

1.2.2 Les sanctions relatives aux atteintes au secret des correspondances

a) Dispositions en droit national

L'article 226-15 du code pénal, alinéa 2 dispose qu'il est puni d'un an d'emprisonnement et de 45 000 euros d'amende « *le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions* ». Les peines sont renforcées, et portées 2 ans d'emprisonnement et de 60 000 euros d'amende lorsque les faits sont commis par le conjoint, le concubin ou le partenaire lié par PACS à la victime.

Sur la notion de mauvaise foi, celle-ci est caractérisée dès lors que celui qui intercepte, détourne, utilise ou divulgue une correspondance sait que celle-ci ne lui est pas destinée, quel que soit le mobile auquel il obéit[78].

[78] C.cass., ch. crim., 24 mars 2020, n° 19-82.069.

L'exploitation de vulnérabilité peut également être indirectement sanctionnée par le biais des atteintes au secret des correspondances. Il faut préciser qu'au titre de ces atteintes, l'exploitation de vulnérabilité n'est pas le seul moyen, ni nécessairement le plus efficace. Les ISMI-catcher, par exemple, sont généralement utilisés pour intercepter les communications hertziennes. Il s'agit d'un appareil simulant une fausse antenne-relais, qui, s'intercalant entre l'opérateur de réseau et le matériel surveillé, intercepte le trafic des communications. L'exploitation de vulnérabilités au sens strict ne concerne pas que les communications hertziennes, elle peut également viser l'intrusion dans une messagerie électronique, mais aussi, de façon prospective, l'interception d'échanges électroniques à l'aide d'un keylogger[79].

Les termes de *télécommunications* ou de *communications par voie électronique* visés par l'alinéa 2 signifient « *toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignement de toute nature par fil optique, radioélectricité ou autres systèmes électromagnétiques. Cette énumération inclut toutes les communications à distance actuellement connues, qu'il s'agisse de communications téléphoniques, ou celles effectuées par minitel, par télécopie, par fax et par satellite réseau internet ; le réseau mondial du net et l'intégralité des services qu'il offre, comme celui de la messagerie électronique, entrent donc directement dans le champ d'application de la législation relative aux télécommunications* »[80].

Par ailleurs, la correspondance désigne toute relation existante entre deux personnes identifiables. La relation est protégée au titre de l'article 226-15, alinéa 2 du code pénal, lorsque le contenu du message est destiné exclusivement à une personne également individualisée, à la différence des messages mis à disposition du public[81]. Cela suscite des interrogations quant à l'applicabilité de la protection offerte par l'article aux messageries groupées, dont la forme peut aller du groupe familial ou amical, avec des personnes restreintes et individualisées, au groupe entre inconnus sous pseudonyme, mais pas seulement.

Enfin, l'exploitation de vulnérabilités informatiques semble bien être un critère déterminant dans la caractérisation de l'infraction. En effet, la Cour d'appel de Paris avait notamment estimé que « *ne constituaient pas une interception la lecture et la retranscription de messages dès lors que celles-ci ne nécessitaient ni dérivation ou branchement, et étaient effectuées sans artifices ou stratagèmes* »[82]. Il était question, en

[79] Enregistreur de frappe : périphérique qui enregistre électroniquement l'utilisation d'un ordinateur.
[80] TGI Paris, 2 novembre 2000.
[81] *Ibid*.
[82] CA Paris, 11e ch., 17 décembre 2001, n° 00-077565.

l'espèce, de la surveillance de correspondances entre deux étudiants et de la vérification de l'usage du réseau, par un directeur de laboratoire de recherche et un administrateur réseau.

b) Dispositions en droit européen

L'article 8 de la Convention européenne des droits de l'homme s'applique, conformément au libellé de l'article, aux correspondances. La notion de « correspondances » est entendue comme englobant les données provenant d'un smartphone ou d'un ordinateur portable[83], ainsi que la copie de celle-ci, les messages électroniques[84], les données des serveurs informatiques[85], dont les disques durs[86] et les disquettes informatiques[87]. L'exploitation de vulnérabilités, si elle a pour but ou pour conséquence l'interception de correspondance, rentre dans le champ de protection de l'article. Comme expliqué ci-dessus, ces interceptions doivent faire l'objet d'un traitement attentif dans le cadre de violences conjugales[88]. Il est nécessaire pour les autorités compétentes d'appréhender de manière globale ce type de violence, sous toutes ses formes.

La Convention de Budapest sur la cybercriminalité réprime également les interceptions illégales de correspondance, par le biais de l'article 3. Il demande aux Parties d'adopter des mesures pour ériger en infraction pénale, « *l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques.* » La directive 2013/40 de l'Union européenne reprend les mêmes termes, mais ne crée d'obligations que pour les cas qui ne seraient pas jugés mineurs[89].

[83] CEDH, 16 novembre 2021, *Särgava c. Estonie*, n° 698/19.
[84] CEDH, 05 septembre 2017, *Barbulescu c. Roumanie*, n° 61496/08.
[85] CEDH, 16 octobre 2007, *Wiser et bicos beteiligungen gmbh c. Autriche*, n° 74336/01.
[86] CEDH, 27 septembre 2005, *Petri sallinen et autres c. Finland,* n° 50882/99.
[87] CEDH, 22 mai 2008, *Iliya stefanov c. Bulgarie,* n° 65755/01.
[88] CEDH, 11 février 2020, *Burutuga c. Roumanie,* n° 56867/15.
[89] Art. 6, directive 2013/40.

Conclusion

Au niveau des atteintes à la personnalité, l'exploitation de vulnérabilités n'est encadrée qu'indirectement, pour les conséquences qu'elle engendre. Dans le cadre des atteintes aux biens, son implication est plus évidente. D'autant plus qu'au titre des atteintes à la personnalité, l'exploitation de vulnérabilités suppose tout de même une atteinte à un STAD, ou aux données contenues dans celui-ci.

Cependant, l'élément intentionnel n'a pas un poids similaire pour toutes les infractions précitées. Il en résulte que l'exploitation d'une vulnérabilité peut ne pas avoir été frauduleuse, mais, eu égard à son objectif, avoir porté atteinte à l'intimité de la vie privée d'autrui ou au secret de ses correspondances. Pour illustrer cette hypothèse, ce pourrait être le cas d'un ordinateur prêté par son propriétaire à une personne tierce, qui, en exploitant les vulnérabilités informatiques dont il aurait connaissance, activerait la webcam ou le microphone afin d'accéder à l'intimité de cette tierce personne. L'atteinte au STAD serait difficilement caractérisable, puisque l'auteur disposerait théoriquement des droits d'accès et de maintien.

Bien que l'exemple soit quelque peu extrême, il permet d'illustrer la protection supplémentaire offerte par l'article, dans le cadre de l'exploitation de vulnérabilités.

De plus, les atteintes à la personnalité sont structurées de façon à opérer une gradation de gravité selon le contexte.

Le droit européen, quant à lui, renforce la légitimité des infractions en droit français, ainsi que d'une certaine manière, leur effectivité. S'il ne crée pas d'infractions supplémentaires, il inscrit le droit national dans un ensemble cohérent vis-à-vis des autres pays du Conseil de l'Europe et de l'Union européenne, mais aussi des Parties à la Convention sur la cybercriminalité.

Cela étant dit, le cadre juridique analysé dans la présente section, relatif aux atteintes aux STAD et à la personnalité, ne s'applique pas de la même manière aux services de renseignement et de police judiciaire. Ceux-ci disposent de certains aménagements, voire de dérogation, pour l'exercice de leur mission. Il convient à présent d'en étudier le contenu.

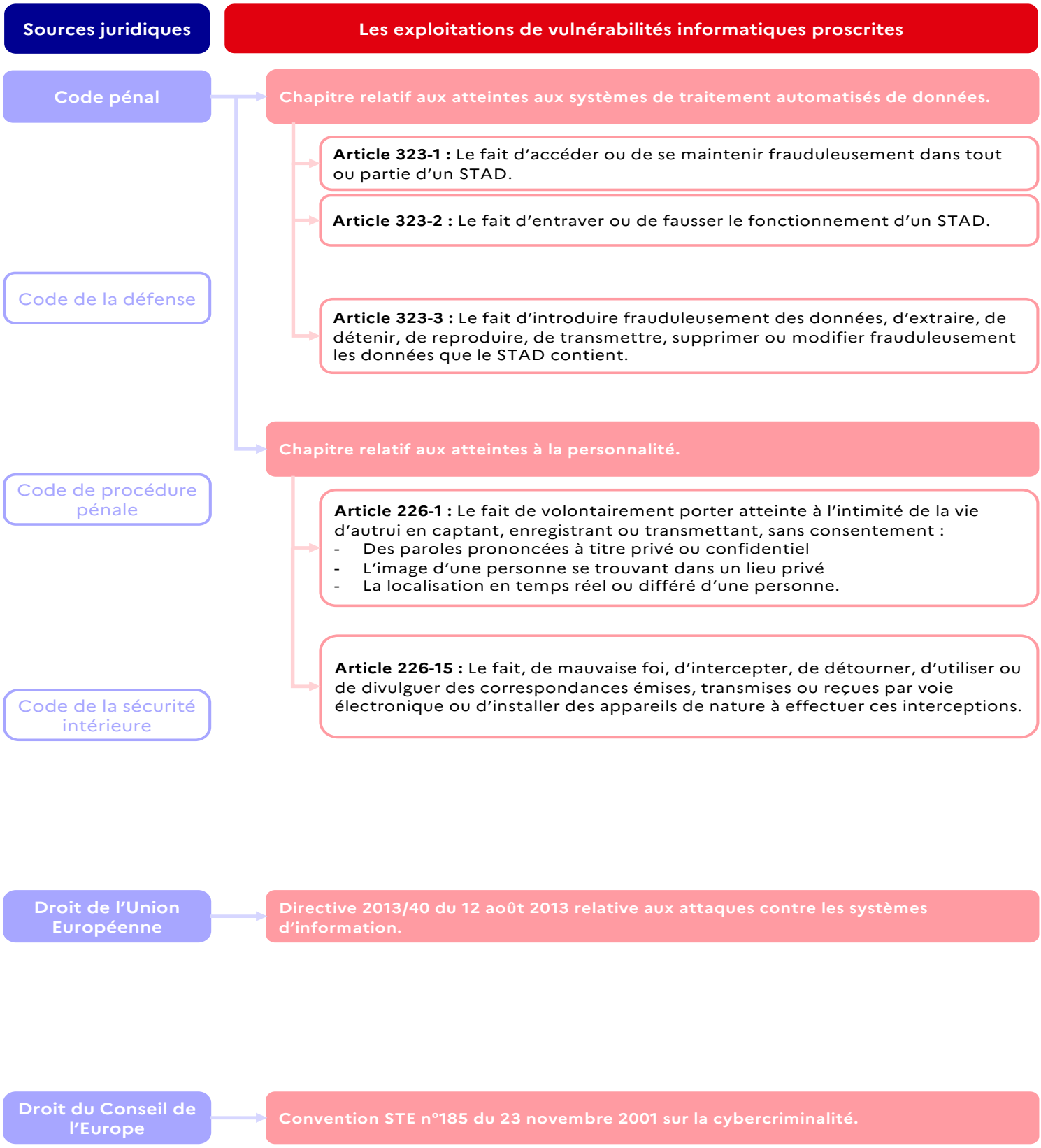

Figure 1. Tableau récapitulatif du cadre juridique des exploitations de vulnérabilités informatiques proscrites.

2. Les exploitations autorisées sous conditions

Si les évolutions technologiques ont participé à faciliter la réalisation d'actes criminels, elles ont également renforcé les outils utilisés par les forces de l'ordre dans l'exercice de leurs missions. Parmi ces outils, trois se distinguent en ce qu'ils peuvent nécessiter l'exploitation de vulnérabilités informatiques. Il s'agit de la captation des données informatiques, de l'accès au support de données informatiques et de la mise au clair des données chiffrées ou inaccessibles. Ces trois techniques sont strictement encadrées par le droit. Elles posent, en effet, de sérieuses problématiques en matière de protection du droit à la vie privée.

La captation des données informatiques est un « *dispositif technique permettant de prendre connaissance du contenu d'un texte avant qu'il ne soit chiffré (crypté) ; de textes tapés sur un ordinateur puis transportés grâce à un périphérique (clé USB, CD rom, disque externe) sur un autre ordinateur, des messages échangés entre deux interlocuteurs sur des forums ou "tchats". […] De tels dispositifs sont des logiciels espions* »[90]. Une délibération de la CNIL, portant avis sur un projet de modification du décret n° 2015-1700 relatif à la mise en œuvre de traitements de données informatiques captées[91], explicite en outre que « *le système de traitement de données captées se matérialise par l'insertion de manière discrète d'une charge logique sur l'équipement de l'individu visé. Une fois activé, le logiciel permet la remontée aux forces de l'ordre de l'ensemble des données présentes sur le support ciblé* ». La captation n'inclut cependant pas le contrôle à distance du système informatique[92]. L'insertion de la charge logique est effectuée par le biais de l'exploitation des vulnérabilités du STAD. Il s'agit d'une forme de malware[93].

Il faut préciser qu'en réalité, deux techniques sont visées lorsque le terme de « *captation de données informatiques* » est utilisé.

---

[90] Étude d'impact, Projet de loi de programmation 2018-2022 et de réforme pour la justice, 19 avril 2018, p. 220.

[91] Décret n° 2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale, *JORF* n° 295 du 20 décembre 2015.

[92] CNIL, Délibération n° 2019-119 du 26 septembre 2019 portant avis sur un projet de décret modifiant le décret n° 2015-1700 du 18 décembre 2015 relative à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale (demande d'avis n° 18004354), *JORF* n° 2 du 3 janvier 2020.

[93] *Ibidem*.

La captation au sens strict « *consiste en un dispositif technique permettant de capter en temps réel des flux de données émis ou reçus par des périphériques (écran, clavier, périphérique audiovisuel) ou des systèmes informatiques détenus par l'objectif* »[94].

Le recueil des données informatiques, quant à lui, permet « *de collecter des données stockées dans un ou plusieurs systèmes informatiques utilisés par un objet, le recueil étant opéré soit directement en accédant au support des données informatiques, soit à distance, au travers des réseaux informatiques* ».

Cette distinction est utile en matière de renseignement, puisque les services autorisés à mettre en œuvre ces deux techniques doivent en outre spécifier à laquelle ils auront recours. Cependant, le présent document utilisera le terme « *captation de données informatiques* » pour désigner l'ensemble de ces techniques. L'objectif étant de ne pas alourdir le propos.

Ainsi, cette technique revêt un caractère particulièrement intrusif. Elle permet de collecter un volume important de données de nature diverse, et de façon indifférenciée. Ce n'est qu'après la collecte, que les données sont triées afin de ne garder que celles utiles dans le cadre de l'affaire en cours. Dès lors, la liste des catégories de données pouvant faire l'objet d'une captation est difficile à dresser. Ce faisant, il n'est pas impossible que soient captées des données relatives ou appartenant à l'entourage de la personne initialement visée[95]. De fait, de solides mécanismes encadrent les conditions de mise en œuvre d'une mesure de captation.

Seuls les services de police judiciaire et de renseignements peuvent mettre en œuvre cette technique. Le cadre juridique de la technique a fait l'objet de plusieurs évolutions, n'ayant été autorisée dans un premier temps en 2011[96], que pour les services de police judiciaire, aux fins de collecter en temps réel les données telles qu'elles s'affichent sur un écran pour l'utilisateur d'un STAD selon les termes de l'article 706-102-1 du CPP. En 2014[97], la technique est étendue aux « *périphériques audiovisuels* ». Elle est ensuite autorisée par la loi relative au renseignement de 2015[98] pour les services de

[94] Étude d'impact, Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement et lettre rectificative, 11 mai 2021, p. 154.
[95] *Ibidem.*
[96] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité (1), *JORF* n° 62 du 15 mars 2011.
[97] Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme (1), *JORF* n° 263 du 14 novembre 2014.
[98] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n° 171 du 26 juillet 2015.

renseignement au titre de l'article L.853-2 du CSI. Il ne s'agit pas seulement d'une réplique de la technique, préalablement autorisée pour les services de police judiciaire, au sein du code de la sécurité intérieure. En effet, la loi renseignement de 2015 autorise, en plus de la collecte en temps réel, l'accès aux données informatiques **stockées**. Il faudra attendre la loi renforçant la lutte contre le crime organisé de 2016[99] pour que les services de police judiciaire puissent également avoir accès aux données stockées.

En outre, la loi renforçant la sécurité intérieure et la lutte contre le terrorisme de 2017[100] a modifié l'article L.853-2 du CSI, la technique pouvant en conséquence viser tous les périphériques et plus uniquement ceux audiovisuels. Une modification étendue au code de procédure pénale pour les services de police judiciaire par la loi de programmation 2018-2022 et de réforme pour la justice de 2019[101]. L'objectif étant d'inclure des messageries telles que Telegram ou WhatsApp et, plus largement, les objets connectés.

Cette technique a l'avantage de faciliter le contournement des barrières relatives au chiffrement des données. Celles-ci sont captées avant que des modifications pour limiter leur compréhension soient effectuées.

En ce qui concerne les techniques pour rendre exploitable des données inaccessibles ou incompréhensibles, elles ne sont autorisées que dans le cadre d'une procédure pénale, et sont un palliatif aux méthodes cryptographiques ou d'authentifications, utilisées par les individus. Encadrées par les articles 60-3 et 230-1 à 230-5 du CPP, elles permettent d'obtenir, respectivement, l'accès au support contenant des données numériques et la mise au clair de données chiffrées. Ce peut être le contexte du téléphone portable verrouillé, du dossier sur présent sur un STAD dont l'accès aurait été restreint, mais aussi des procédés entrainant l'effacement, sous certaines conditions[102], de données susceptibles d'intéresser l'enquête ou l'instruction[103].

Parmi les techniques employées pour ce faire, l'exploitation de vulnérabilités informatiques peut se révéler utile. Pour autant, ces méthodes sont parfois longues,

[99] 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, *JORF* n° 129.
[100] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (1), *JORF* n° 0255 du 31 octobre 2017.
[101] Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, *JORF* n° 71 du 24 mars 2019.
[102] Par exemple, un nombre précis de tentatives d'accès.
[103] AUDIBERT (M.), *Le recueil de la preuve numérique : Enjeux et perspectives en procédure pénale*, th., 4 novembre 2024, Nanterre, spéc. p. 78.

coûteuses, voire infructueuses, et peuvent endommager les données. Elles posent également des interrogations sur la validité des preuves obtenues. Pour ces raisons, la captation des données informatiques et les autres techniques permettant de contourner le chiffrement des données offrent une alternative intéressante.

Le choix a été fait dans le présent document, de traiter au sein d'un même point, la captation de données informatiques par les services de police judiciaire et par les services de renseignement, avant de traiter l'accès aux données rendues inaccessibles ou incompréhensibles dans le cadre d'une procédure judiciaire.

Outre le droit national, l'ordre européen s'est déjà saisi des enjeux traduisant les frictions entre sécurité, surveillance, et vie privée.

La CEDH a notamment posé plusieurs conditions pour la mise en œuvre de techniques d'intrusion dans la vie privée des individus limitatrices du droit consacré à l'article 8[104]. Si elle ne s'est pas explicitement prononcée sur l'exploitation de vulnérabilité à des fins de captation de données informatiques, les apports jurisprudentiels des affaires relatives aux activités des services de renseignement d'autres pays européens sont susceptibles d'être appliqués, par analogie, aux activités de police judiciaire et de renseignement. Par ailleurs, la Convention sur la cybercriminalité dispose également de développements relatifs aux perquisitions et aux saisies de données informatiques stockées, qui, là encore, intéressent le sujet de l'exploitation de vulnérabilités[105].

Au niveau de l'Union européenne, la directive « Vie Privée »[106], la directive « Police-Justice »[107], le règlement « Liberté des Médias »[108] ainsi que les jurisprudences de la CJUE[109] ont participé à construire un cadre contraignant en matière d'exploitation de vulnérabilités par les forces de l'ordre.

Il conviendra d'apprécier la captation de données informatiques par les services de police judiciaire et de renseignement (**2.1**), l'accès aux données inaccessibles ou

[104] Convention EDH, Art. 8 *« toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».
[105] Titre 4 « perquisition et saisie de données informatiques stockées », Convention sur la cybercriminalité.
[106] Directive « Vie Privée ».
[107] Directive « Police-Justice ».
[108] Règlement sur la liberté des médias.
[109] CJUE, gr. ch., 6 octobre 2020, n°C-511/18 et C-512/18 ; CJUE, gr. ch., 30 avril 2024, n°C-670/22.

inintelligibles au cours de la procédure judiciaire (**2.2**), et enfin le droit européen pertinent en la matière (**2.3**).

2.1 La captation de données informatiques par les services de police judiciaire et de renseignement

Comme expliqué ci-dessus, la captation de données informatiques peut être opérée par deux types de services. Ceux relevant de la police judiciaire, et ceux relevant du renseignement.

Placée sous l'autorité judiciaire, garante des libertés individuelles, la police judiciaire est chargée de l'investigation dans le cadre d'infractions. Pour ce faire, elle dispose de pouvoirs d'enquêtes, dont les services compétents, les bases juridiques, les méthodes et les finalités varient. Ainsi, la captation des données informatiques, encadrée par l'article 706-102-1 du CPP, est une technique spéciale d'enquête, dont le recours est circonscrit à la répression de la criminalité et de la délinquance organisée, et des crimes[110]. Pour être légalement mise en œuvre, elle doit être conforme aux dispositions applicables à toutes les techniques spéciales d'enquête, au titre des articles 706-95-11 à 706-95-19 du CPP. Elle doit également répondre au cadre traitant spécifiquement de la captation, consacré aux articles 706-102-1 à 706-102-5 du CPP.

Les services de renseignement, quant à eux, sont placés soit, sous l'autorité du Gouvernement[111] (les services dits « de premier cercle »), soit, sous celle des ministres de la Défense, de l'Intérieur et de la Justice, et des ministres chargés de l'économie, du budget ou des douanes[112] (les services dits « de second cercle »). La différence entre ces deux cercles tient à la marge de manœuvre dont ils disposent pour l'exercice de leur mission.

La captation des données informatiques fait partie des techniques de recueil de renseignement soumises à autorisation[113] et doit être conforme, pour être légalement

[110] CPP, Livre IV : De quelques procédures particulières, Titre XXV : De la procédure applicable à la criminalité et à la délinquance organisées et aux crimes, Chapitre II : Procédures, Section 6 : Des autres techniques spéciales d'enquête, Paragraphe 4 : De la captation des données informatiques.
[111] Art. L811-2 code de la sécurité intérieure (CSI).
[112] Art. L811-4 CSI.
[113] CSI, Livre VIII : Du renseignement, Titre V : Des techniques de recueil de renseignement soumises à autorisation, Chapitre III : De la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques.

mise en œuvre, à la procédure applicable à toutes les techniques de recueil soumises à autorisation, prévue par le code de la sécurité intérieure aux articles L.821-1 à L.821-8. Elle doit être aussi conforme aux dispositions spécifiquement applicables à la technique de captation, consacrée à l'article L.853-2 du même code.

Il convient à présent d'analyser en détail les deux cadres juridiques. Dans la mesure où la technique de captation de données informatiques avait été autorisée à l'origine, uniquement pour les services de police judiciaire, l'étude se penchera d'abord sur le cadre juridique de ceux-ci (**2.1.1**), puis celui des services de renseignement (**2.1.2**).

2.1.1 La captation opérée par les services de police judiciaire

L'article 706-102-1 du CPP énonce qu'« *Il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, 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 a introduits par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques* ».

L'alinéa deux de l'article poursuit « *Le procureur de la République ou le juge d'instruction peut désigner toute personne physique ou morale habilitée et inscrite sur l'une des listes prévues à l'article 157, en vue d'effectuer les opérations techniques permettant la réalisation du dispositif technique mentionné au premier alinéa du présent article. Le procureur de la République ou le juge d'instruction peut également prescrire le recours aux moyens de l'État soumis au secret de la défense nationale selon les formes prévues au chapitre 1er du titre IV du livre Ier* ».

Les articles 706-102-3 et 706-102-5 apportent des précisions procédurales sur le détail des informations devant être présentes dans la décision d'autorisation du recours au dispositif technique[114], et les modalités encadrant le cas de l'introduction dans un véhicule ou un lieu privé aux fins d'installer et de désinstaller le dispositif[115].

Devront alors être analysés : le champ matériel des infractions pouvant faire l'objet d'une technique de captation **(2.1.1.1)**, la procédure d'autorisation du recours à cette technique **(2.1.1.2)**, les dispositions spécifiquement applicables à la technique de

[114] Art. 706-102-3 code de la procédure pénale (CPP).
[115] Art. 706-102-5 CPP.

captation des données informatiques **(2.1.1.3)** et celles relatives aux moyens de l'État soumis au secret de la défense nationale **(2.1.1.4)**.

2.1.1.1 Le champ matériel des infractions pouvant faire l'objet d'une technique de captation

L'article 706-95-11, alinéa 2, explique que les techniques spéciales d'enquête « *peuvent être mises en œuvre si les nécessités de l'enquête ou de l'information judiciaire relatives à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent* ».

L'enquête (de flagrance ou préliminaire) est effectuée sous l'autorité du Procureur de la République, contrairement à l'information judiciaire qui est menée par le juge d'instruction. Il s'agit, dans les deux cas, de recueillir des éléments de preuves et de rechercher les auteurs d'infractions.

Selon les termes de l'article, pour recourir à la technique de captation, deux conditions cumulatives doivent être réunies, la présence d'une « *nécessité (vis-à-vis) de l'enquête ou de l'information judiciaire*[116] » et d'une infraction rentrant dans le champ d'application des articles 706-73 et 706-73-1 du CPP.

L'interprétation de la notion de « *nécessité de l'enquête* », peut être éclairée par la décision n° 96-377 du 16 juillet 1996 du Conseil constitutionnel[117] relative à l'examen de la loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire de 1996[118], notamment l'examen de l'article 10 de cette loi, qui modifiait l'article 706-24 du CPP. Le Conseil constitutionnel a estimé, concernant la possibilité d'autoriser des perquisitions, des visites domiciliaires et des saisies de pièces à conviction sans l'assentiment de la personne chez laquelle elles ont lieu « *lorsque les nécessités de l'enquête l'exigent* », que cette expression devait s'entendre comme « *ne permettant d'autoriser une*

[116] De l'enquête ou de l'information judiciaire.
[117] Cons. const., 16 juillet 1996, n° 96-377 DC, *Loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire,* §17.
[118] Loi n° 96-647 du 22 juillet 1996 tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire, *JORF* n° 170 du 23 juillet 1996.

perquisition (…) que si celle-ci ne peut pas être réalisée dans les circonstances de temps définies par l'article 59 du code de procédure pénale ». L'autorisation de ces mesures est alors circonscrite à l'échec supposé de leur mise en œuvre en circonstances ordinaires, selon la procédure habituelle.

Transposée au contexte de l'article 706-95-11 du CPP, cette interprétation semble définir les « *nécessités de l'enquête ou de l'information judiciaire* » comme ne permettant pas d'autoriser le recours à une technique spéciale d'enquête, que si les objectifs visés par l'enquête ou l'information judiciaire ne pourront être atteints par des techniques ordinaires[119].

Concernant la deuxième condition, les articles 706-73 et 706-73-1 du CPP couvrent un large champ d'infractions relevant de la criminalité, de la délinquance organisée et de crimes. Ils sont composés de plusieurs points, chacun renvoyant à différentes infractions réprimées par le biais de divers articles figurants dans plusieurs codes.

L'article 706-73 traitant des crimes et des délits, composé de 21 points, vise des infractions inscrites dans le code pénal[120], mais pas uniquement. Sont également visés certains articles du code de la défense[121], du code de la sécurité intérieure[122], du code de l'entrée et du séjour des étrangers et du droit d'asile[123] ainsi que du code des douanes[124] et du code minier[125].

L'article 706-73-1 traite uniquement des délits et est composé de 13 points. Des dispositions du code pénal sont encore visées[126], mais l'article renvoie également à

[119] Notamment les techniques consacrées au Livre IV, Titre XXV, Chapitre II, section 1 à 5.
[120] Code pénal, art. 221-4, 8° ; art. 132-2 ; art. 222-4 ; art. 222-34 à 222-40 ; art. 224-5-2 ; art. 225-4-2 à 225-4-7 ; art. 225-7 à 225-12 ; art. 311-9 ; art. 312-6 et 312-7 ; art. 322-8 ; art. 442-1 et 442-2 ; art. 421-1 à 421-6 ; les crimes portant atteinte aux intérêts fondamentaux de la nation prévus au titre Ier du livre IV code pénal ; art. 411-2 ; art. 222-52 à 222-54, 222-56 à 222-59, 322-6-1 et 322-11-1 ; art. 324-1 et 324-2 ; art. 321-1 et 321-2 ; art. 450-1 ; art. 321-6-1 ; art. 224-6-1 ; 223-15-2 et 2° du III art. 223-15-3.
[121] Code de la défense, art. L.2339-2, L.2339-3, L.2339-10, L.2341-4, L.2353-4 et L.2353-5.
[122] CSI, art. L.317-2, L.317-7.
[123] CESEDA, art. L.823-1, L.823-2, L.823-3, L.823-3-1.
[124] Code des douanes, art. 414.
[125] Code minier, art. L.512-2, lorsqu'il est connexe avec l'une des infractions ci-dessus.
[126] Code pénal, art. 313-2 ; 323-4-1 ; 434-30, al. 2 ; 324-1 ; 321-1 et 321-2 ; 324-2 ; 450-1 ; 321-6-1 ; 322-3-2 ; 411-5 ; 411-7 ; 411-8 ; 412-2 al. 1 et 2, 413-1 ; 413-13 al. 3, 411-12 ; 323-3-2.

certains délits issus du code du travail[127], du code de l'environnement[128], du code rural et de la pêche maritime[129], du code de la sécurité intérieure[130], et du code de la Sécurité sociale[131].

Pour complexifier tout cela, plusieurs infractions visées par les articles 706-73 et 706-73-1 ne peuvent faire l'objet d'une technique spéciale d'enquête que si elles sont effectuées en relation avec d'autres infractions visées par les articles susmentionnés. C'est le cas par exemple, du délit de non-justification de ressources correspondant au train de vie qui doit être en relation avec l'une des infractions mentionnées aux 1° à 15° et 17° de l'article 706-73 du CPP[132], par exemple, le crime et délit de trafic de stupéfiant (3°), d'enlèvement et de séquestration commis en bande organisée (4°), de traite des êtres humains (5°).

Par ailleurs, les infractions visées aux points 14° à 16° et 19° de l'article 706-73 du CPP, et celles visées aux points 3° à 5° de l'article 706-73-1 du même code, sont dans ce cas précis.

Lorsque les deux conditions sont réunies (les besoins d'une enquête ou d'une information judiciaire, vis-à-vis des infractions limitativement énumérées ci-dessus, nécessitent le recours à une technique spéciale), la captation des données informatiques peut être demandée. Son autorisation de mise en œuvre doit être obtenue, toujours selon une procédure commune aux techniques spéciales d'enquête.

2.1.1.2 La procédure d'autorisation

Aux fins d'obtenir cette autorisation, le procureur de la République a, selon le type de procédure initiée, une fonction d'initiative ou de consultation[133].

[127] Code du travail, art. L.8221-1, al. 1° et 3° ; L.8221-3 ; L.8221-5 ; L.8224-1 ; L.8224-2 ; L.8231-1 ; L.8234-1 ; L.8234-2 ; L.8241-1 ; L.8243-2 ; L.8251-1 et L.8256-2.
[128] Code de l'environnement, art. L.415-6 et L.541-46, VII.
[129] Code rural et de la pêche maritime, art. L.253-17-1, 3° ; L.253-15 et L.253-16, II ; L.254-12, III.
[130] CSI, art. L.324-1 al. 1 et L.324-4 al. 1.
[131] Code de la sécurité sociale, art. L.114-13.
[132] Code de procédure pénale, art. 706-73, 16°.
[133] Art. 706-95-12 CPP.

Au cours d'une enquête préliminaire ou de flagrance[134], l'autorisation est délivrée par le juge des libertés et de la détention à la requête du procureur, pour une durée maximale d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée[135]. Au cours de l'information judiciaire, elle est délivrée par le juge d'instruction après avis du procureur, pour une durée maximale de quatre mois, renouvelable jusqu'à tant que la durée totale des opérations n'ait pas excédée deux ans[136]. En cas d'urgence toutefois, de risques imminents de dépérissement des preuves ou d'atteintes graves aux personnes ou aux biens, l'autorisation du juge d'instruction peut être délivrée sans avis préalable du procureur de la République[137].

L'autorisation prend la forme d'une ordonnance écrite et motivée, faisant référence aux éléments de fait et de droit justifiant la nécessité de l'opération souhaitée. Elle ne possède pas de caractère juridictionnel et n'est susceptible d'aucun recours[138]. Lorsque l'impératif de l'urgence est invoqué, l'autorisation doit énoncer les circonstances de fait établissant l'existence du risque imminent[139].

Pour la mise en place de la technique spéciale d'enquête, un officier de police judiciaire est commis par le juge d'instruction, ou requis par le procureur de la République. L'officier peut également déléguer cette compétence à un agent de police judiciaire, demeurant sous sa responsabilité[140]. Par ailleurs, ces trois acteurs, l'officier de police judiciaire, le juge d'instruction et le procureur, peuvent requérir tout agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité ou la tutelle du ministre de l'Intérieur ou du ministre de la Défense, et dont la liste est fixée par décret[141].

Les opérations se déroulent sous l'autorité et le contrôle du magistrat qui les a autorisées, ce dernier pouvant ordonner leur interruption à tout moment. Le juge des libertés et de la détention est en collaboration étroite avec le procureur de la République, il est informé sans délai des actes accomplis, par le biais de procès-verbaux, dressés en exécution de sa décision d'autorisation. De plus, si ce dernier estime que les opérations n'ont pas été

[134] L'enquête de flagrance est une enquête spécifique qui peut être menée à la suite de la constatation d'un crime ou d'un délit flagrant, tandis que l'enquête préliminaire, qui a pour but de recueillir des éléments permettant d'éclairer de potentielles poursuites, constitue la première étape du procès pénal.
[135] *Ibid*., art. 706-95-16, al. 1.
[136] *Ibid*., al. 2.
[137] *Ibid*., art. 706-95-13, al. 2.
[138] *Ibid*., al. 1.
[139] *Ibid*., al. 2
[140] *Ibid*., art. 706-95-17, al. 1.
[141] *Ibid*., al. 2.

réalisées conformément à son autorisation, ou qu'elles ne respectent pas la loi, une destruction des procès-verbaux et des données enregistrées peut être, par ordonnance motivée, requise. Une fois notifié d'une telle ordonnance, le procureur de la République peut former appel dans un délai de dix jours[142].

Parmi les procès-verbaux obligatoires à dresser, celui de la mise en place des dispositifs techniques et des opérations effectuées, avec l'heure et la date de début et de fin ; celui transcrivant ou décrivant les données utiles à la manifestation de la vérité, les données étrangères à la procédure ne pouvant être conservées[143] ; celui relatant de la destruction des données enregistrées, à l'expiration du délai de prescription de l'action publique[144].

En outre de ces éléments procéduraux, la mise en œuvre de la technique de captation de données informatiques doit répondre aux dispositions des articles 706-102-3 et suivants.

2.1.1.3 Les dispositions spécifiquement applicables à la technique de captation

Selon les termes de l'article 706-102-3 du CPP, la décision d'autorisation doit préciser l'infraction qui motive le recours à cette technique, la localisation exacte ou la description détaillée des STAD visés, ainsi que la durée des opérations[145].

Les services, unités et organismes pouvant procéder aux opérations d'installations des dispositifs techniques, dont la liste est fixée par décret conformément à l'article 706-95-17 du CPP, sont ceux mentionnés à l'article D15-1-6 du CPP, applicable uniquement au contexte de la captation de données. L'article est modifié par décret, au gré des évolutions juridiques et des besoins.

Dans sa version en vigueur au 1er février 2024, comme modifié par l'article 3 du décret n° 2023-1109[146], peuvent procéder aux opérations d'installation : la direction nationale de la police judiciaire et les services territoriaux de la police nationale chargés de la police judiciaire au sein des directions départementales ou interdépartementales de la police nationale ; la direction générale de la sécurité intérieure ; les offices centraux de

[142] *Ibid*., art. 706-95-14.
[143] *Ibid*., art. 706-95-18.
[144] *Ibid*., art. 706-95-19.
[145] *Ibid*., art. 706-102-3.
[146] Décret n° 2023-1109 du 29 novembre 2023 modifiant diverses dispositions relatives à la police nationale, *JORF* n° 277 du 30 novembre 2023.

police judiciaire ; la force d'intervention de la police nationale ; les services territoriaux de la police judiciaire et les services territoriaux du RAIS des directions territoriales de la police nationale ; la sous-direction de la police judiciaire de la gendarmerie nationale ; le commandement de la gendarmerie dans le cyberespace ; le service central de renseignement criminel de la gendarmerie nationale ; les sections de recherches de la gendarmerie nationale ; les sections d'appui judiciaire de la gendarmerie nationale ; le groupe d'intervention de la gendarmerie nationale.

De plus, a été créé par arrêté en 2018, un service à compétence nationale[147] dénommé « *service technique national de captation judiciaire* » (STNCJ)[148]. Rattaché au directeur technique de la direction générale de la sécurité intérieure, ce service est chargé de « *la conception, de la centralisation et de la mise en œuvre des dispositifs techniques mentionnées aux articles 706-102-1 et 706-102-2 du code de procédure pénale. Il coordonne ou réalise, en tant que de besoin, les opérations d'installation de ces mêmes dispositifs techniques* »[149]. Les activités et l'organisation de ce service sont couvertes par le secret de la défense nationale[150][151].

Par ailleurs, le procureur de la République et le juge d'instruction peuvent désigner toute personne physique ou morale, habilitée au titre de l'article 157 du CPP relatif aux experts, en vue d'effectuer les opérations techniques permettant la réalisation du dispositif technique ayant pour objet la captation[152]. Ces experts doivent figurer sur la liste nationale dressée par la Cour de cassation, ou sur l'une des listes dressées par les cours d'appel. Ils y sont inscrits selon les dispositions de la loi relative aux experts judiciaires de 1971[153], et doivent respecter les lois et règlements relatifs à leur profession ou à leur mission d'expert. Tout manquement à la probité ou à l'honneur, même s'ils se rapportent à des faits étrangers aux missions préalablement confiées, expose l'expert à des poursuites disciplinaires[154].

[147] Les services à compétence nationale appartiennent à une catégorie particulière de services administratifs. Ils ne relèvent ni de l'administration centrale, ni de l'administration déconcentrée. Ils exercent des missions opérationnelles sur l'ensemble du territoire.
[148] Arrêté du 9 mai 2018 portant création du service à compétence nationale dénommé « service technique national de captation judiciaire », *JORF* n° 107 du 10 mai 2018.
[149] *Ibid*., art. 2.
[150] *Ibid*., art. 3.
[151] Voir 2.3.
[152] *Ibid*., art. 706-102-1, al. 2.
[153] Loi n° 71-498 du 29 juin 1971 relative aux experts judiciaires, *JORF* du 30 juin 1971.
[154] *Ibid*., art. 6-2, al. 1 et 2.

À titre d'exemple, figurent sur la liste nationale de la Cour de cassation de 2024[155], des consultants en cybersécurité, en sécurité et stratégie des systèmes d'information ou en systèmes et logiciels, ainsi que le laboratoire d'expertise et de recherches de traces numériques (LERTI)[156].

D'un point de vue pratique, peut être rendue nécessaire l'introduction dans un véhicule ou dans un lieu privé, en vue de l'installation ou de la désinstallation du dispositif technique de captation. Le juge des libertés et de la détention (à la requête du procureur de la République) et le juge d'instruction sont compétents pour délivrer l'autorisation. Cette opération peut avoir lieu à l'insu ou sans le consentement du propriétaire ou du possesseur du véhicule, ou de l'occupant des lieux ou autre personne titulaire d'un droit sur celui-ci. Les dispositions de l'article 59 du CPP, relatif aux heures autorisées pour les perquisitions et les visites domiciliaires, ne sont pas applicables[157].

Toujours en vue de la mise en place, la transmission par réseau de communications électroniques du dispositif technique peut être autorisée par le juge des libertés et de la détention (à la requête du procureur) ou par le juge d'instruction[158].

Le recours à un dispositif technique de captation n'est cependant pas exempt de certaines lignes rouges. En effet, des interdictions de mises en œuvre existent dans plusieurs cas précis[159]. Cette technique n'est pas autorisée lorsqu'elle concerne les STAD qui se trouvent : dans le cabinet d'un avocat ou dans son domicile ; dans les locaux de l'ordre des avocats ou des caisses de règlement pécuniaire des avocats[160] ; dans les locaux d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne, d'une agence de presse ; dans les véhicules professionnels de ces entreprises ou agences ou au domicile d'un journaliste lorsque les investigations sont liées à son activité professionnelle[161] ; dans le cabinet d'un médecin, d'un notaire ou d'un huissier[162] ; dans les locaux d'une juridiction ou au domicile d'une personne exerçant des fonctions juridictionnelles[163]. L'utilisation d'un tel dispositif

[155] Liste des experts agréés par la Cour de cassation, année 2024, au point : G-Criminalistique – Sciences criminelles et médico-légales, G-13-Supports numériques, G-13.01 Données numériques.
[156] Liste non-exhaustive pour la seule période de 2024.
[157] Art. 706-102-5, al. 1 CPP.
[158] *Ibid*., al. 2.
[159] *Ibid*., al. 3.
[160] *Ibid*., art. 56-1.
[161] *Ibid*., art. 56-2.
[162] *Ibid*., art. 56-3.
[163] *Ibid*., art. 56-5.

technique est également proscrite dans le cas du véhicule, du bureau ou du domicile d'un député ou d'un sénateur[164].

Enfin, aux spécificités relatives à de la technique de captation de données informatiques, s'ajoutent les dispositions du Chapitre Ier « *De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité* » du code de procédure pénale, lorsqu'est prescrit le recours aux moyens de l'État soumis au secret de la défense nationale.

2.1.1.4 La procédure applicable aux moyens de l'État soumis au secret de la défense nationale

L'alinéa 2 de l'article 706-102-1 précise que le procureur de la République peut également prescrire le recours aux moyens de l'État soumis au secret de la défense nationale[165].

Cette demande spécifique doit respecter la procédure prévue par l'article 230-2 du CPP. Deux conditions cumulatives doivent être remplies pour légitimer la demande. La présence d'une infraction dont la peine d'emprisonnement est égale ou supérieure à deux ans d'emprisonnent, et si les nécessités de l'enquête ou de l'instruction l'exigent[166].

Lorsque ces conditions sont réunies, le procureur de la République peut adresser une réquisition écrite, à l'organisme technique soumis au secret de la défense nationale préalablement désigné par décret[167]. La réquisition fixe le délai de l'opération, celui-ci pouvant être prorogé dans les mêmes conditions de forme. Le procureur peut à tout moment, ordonner l'interruption des opérations prescrites. Lorsque les données et les résultats, ou les indications techniques utiles à leur compréhension sont protégés au titre du secret à la défense nationale, leur communication doit respecter les dispositions des articles L.2312-4 à L.2312-8 du code de la défense.

Malgré l'opacité de ces moyens extraordinaires, la possibilité d'y recourir est considérée comme poursuivant « *l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et (comme mettant) en œuvre les exigences constitutionnelles inhérentes à*

[164] *Ibid*., art. 100-7.
[165] *Ibid*., art. 706-102-1, al. 2.
[166] *Ibid*., art. 230-1, al. 3.
[167] *Ibid*., art. 230-2.

la sauvegarde des intérêts fondamentaux de la Nation »[168]. Il était avancé devant le Conseil constitutionnel, une atteinte aux principes d'égalité des armes et du contradictoire, aux droits de la défense et au droit à un recours juridictionnel effectif, car ce type de moyen privait les personnes de leur capacité à contester la régularité des opérations[169]. Or, après analyse du cadre juridique entourant ces moyens[170], le Conseil constitutionnel a estimé qu'ils procédaient à une conciliation équilibrée entre les exigences constitutionnelles. En effet, l'utilisation de techniques non divulguées serait nécessaire pour garantir l'efficacité des investigations, l'opacité de celles-ci étant intrinsèquement liée à la qualité des opérations. De plus, ces moyens ne sont autorisés qu'en vertu de strictes conditions[171], et l'ensemble des éléments obtenus à l'issue des opérations, fait l'objet d'un procès-verbal de réception[172].

Cela étant dit, la technique de captation de données informatiques est également utilisée dans le cadre des activités de renseignement, bien que ses modalités procédurales, ses objectifs et les acteurs impliqués diffèrent fondamentalement.

2.1.2 La captation opérée par les services de renseignement

L'article L.853-2 du CSI est composé de cinq alinéas. L'alinéa 1er est rédigé ainsi : « *Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre, et permettant d'accéder à ces mêmes données informatiques, de les enregistrer, de les conserver et de les transmettre, 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* ».

[168] Cons. const. 8 avril 2022, n° 2022-987 QPC, *Conditions de recours aux moyens des services de l'État soumis au secret de la défense nationale dans le cadre de certaines procédures pénales,* §15.
[169] Ibid. §8.
[170] Les moyens consacrés aux articles 230-1 à 230-5 du code de procédure pénale, et 706-102-1 du même code.
[171] *Ibid*. §16.
[172] *Ibid*. §17.

Les termes utilisés pour désigner la technique de captation sont sensiblement les mêmes que ceux de l'article 706-102-1 du CPP.

Conformément au libellé de l'alinéa 1er de l'article L.853-2, pour être légalement mise en œuvre, la technique doit respecter la procédure prévue au Chapitre Ier du Titre II du Livre VIII, qui correspond aux articles L.821-1 à L.821-8 du CSI, et qui est applicable à toutes les techniques de recueil de renseignement soumises à autorisation.

Les quatre derniers alinéas de l'article L.853-2 traitent soit, des modulations ou des dérogations à la procédure applicable à toutes les techniques, soit des précisions opérationnelles quant à la mise en place du dispositif technique :

Alinéa 2 « *par dérogation à l'article L.821-4, l'autorisation de mise en œuvre de la technique mentionnée au I du présent article est délivrée pour une durée maximale de deux mois. L'autorisation est renouvelable dans les mêmes conditions de durée* ».

Alinéa 3 « *Les dispositifs techniques mentionnés au I du présent article ne peuvent être utilisés que par des agents appartenant à l'un des services mentionnés aux articles L.811-2 et L.811-4 dont la liste est fixée par décret en Conseil d'État* ».

Alinéa 4 « *Le service autorisé à recourir à la technique mentionnée au I rend compte à la Commission nationale de contrôle des techniques de renseignement de sa mise en œuvre. La Commission peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits* ».

Alinéa 4 bis « *le caractère d'urgence mentionné à la dernière phrase du deuxième alinéa de l'article L.821-1 ne peut être invoqué que si l'autorisation prévue au présent article a été délivrée au titre du 1°, du 4° ou a du 5° de l'article L.811-3* ».

Et enfin, alinéa 5 « *si la mise en œuvre de cette technique nécessite l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L.853-3* ».

Eu égard à la structure de l'article L.853-2 du CSI, il conviendra de traiter distinctement la procédure d'autorisation commune à toute technique **(2.1.2.1)**, les modalités spécifiques à la technique de captation **(2.1.2.2)** et le détail des agents compétents pour sa mise en œuvre **(2.1.2.3)**.

2.1.2.1 La procédure d'autorisation

Selon les articles L.821-1 à L.821-8 du CSI, l'autorisation de mise en œuvre doit être délivrée par le Premier ministre, après que celui-ci ait obtenu l'avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR)[173]. La CNCTR n'exerce qu'une fonction consultative dans cette procédure d'autorisation. Le Premier ministre n'est pas lié par la teneur de l'avis rendu. Lorsqu'il décide d'autoriser le recours à cette technique en dépit d'un avis défavorable de la Commission, il indique les motifs pour lesquels ce dernier n'a pas été suivi[174]. En parallèle, le Conseil d'État doit cependant être saisi immédiatement par la CNCTR[175], qui, en formation spécialisée habilitée au secret de la défense nationale, statue dans un délai de 24 heures. Sauf en cas d'urgence dûment justifiée, la décision d'autorisation du Premier ministre ne peut être exécutée avant que le Conseil d'État n'ait statué[176].

L'autorisation est délivrée sur demande écrite et motivée d'une personne, qui peut être limitativement, le ministre de la Défense, le ministre de l'Intérieur, le ministre de la Justice ou les ministres chargés de l'économie, du budget ou des douanes. Ils ne peuvent déléguer cette attribution qu'à des collaborateurs directs, habilités au secret de la défense nationale. La demande doit renseigner diverses informations, telles que : la technique à mettre en œuvre ; le service pour lequel elle est présentée ; les finalités poursuivies ; les motifs des mesures ; la durée de validité de l'autorisation ; les personnes, lieux ou véhicules concernés. Lorsque l'identité des personnes visées n'est pas connue, la demande les désigne par leur identifiant ou leur qualité. Les lieux ou les véhicules sont désignés par référence aux personnes faisant l'objet de la demande. Enfin, la demande de renouvellement d'une autorisation expose les raisons qui justifient une telle prolongation, au regard des finalités poursuivies[177].

Les finalités pouvant fonder une demande d'autorisation sont listées à l'article L.811-3 du CSI. Les techniques de renseignement mises en œuvre doivent strictement répondre

[173] Art. L821-1, al. 1, CSI.
[174] *Ibid*., art. L821-4, al. 2.
[175] *Ibid*., art. 831-1, al. 2 et 3 : le pouvoir de saisine du Conseil d'État par la CNCTR est accordé au président de la Commission, aux deux membres du Conseil d'État (d'un grade au moins égal de conseiller d'État) ainsi qu'aux deux magistrats hors hiérarchie de la Cour de cassation, qui forment une partie des neuf membres de la Commission.
[176] *Ibid*., art. L821-1, al. 2.
[177] *Ibid*., art. L821-2.

à l'une d'entre elles. Ces finalités sont les intérêts fondamentaux de la Nation, dont le recours à une technique doit en permettre la défense et la promotion. Ce sont :

1. L'indépendance nationale, l'intégrité du territoire et la défense nationale ;
2. 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 ;
3. Les intérêts économiques, industriels et scientifiques majeurs de la France ;
4. La prévention du terrorisme ;
5. La prévention :
    a. Des atteintes à la forme républicaine des institutions ;
    b. Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L.212-1 du CSI[178] ;
    c. Des violences collectives de nature à porter gravement atteinte à la paix publique.
6. La prévention de la criminalité et de la délinquance organisées ;
7. La prévention de la prolifération des armes de destruction massive.

La demande est communiquée au président de la CNCTR ou à l'un de ses membres[179], qui dispose d'un délai de 24 heures pour rendre son avis au Premier ministre. Le délai est étendu à 72 heures lorsque l'examen est effectué en formation restreinte ou en formation plénière. Si tel est le cas, le Premier ministre en est informé sans délai. Par ailleurs, un avis qui n'aurait pas été transmis au Premier ministre au terme des délais est réputé rendu[180].

L'attribution du Premier ministre, lui permettant de délivrer une autorisation, peut être déléguée individuellement à des collaborateurs directs habilités au secret de la défense nationale[181].

À l'instar des interdictions posées par l'article 706-102-5 du CPP, certaines catégories de personnes bénéficient d'une protection accrue eu égard à la sensibilité de leur profession. En effet, un parlementaire, un magistrat, un avocat ou un journaliste ne peut

[178] *Ibid.*, art. L212-1 : les groupements ou associations qui provoquent à des manifestations armées ou à des agissements violents à l'encontre des personnes ou des biens, qui présente, par leur forme et leur organisation militaires, le caractère de groupes de combat ou de milices privées, ou dont l'activité tend à faire échec aux mesures concernant le rétablissement de la légalité républicaine (liste non-exhaustive).
[179] Parmi ceux mentionnés aux alinéas 2 et 3 de l'article L831-1 du CSI.
[180] *Ibid.*, art. L821-3.
[181] *Ibid.*, art. L821-4.

être l'objet d'une technique de recueil de renseignement à raison de l'exercice de son mandat ou de sa profession. Cette protection n'a pas la même envergure que celle au titre du code de procédure pénale, puisqu'il est tout de même possible d'avoir recours à la captation vis-à-vis de ces personnes, lorsque l'opération ne concerne pas l'exercice du mandat ou de la profession. Cependant, dans le cas où la demande concerne l'une de ces personnes ou de ses véhicules, ses bureaux ou domiciles, la CNCTR fait son examen en formation plénière[182]. En cas de saisine du Conseil d'État pour non suivi d'un avis défavorable de la CNCTR, la décision d'autorisation du Premier ministre ne peut être exécutée, même en cas d'urgence.

Les transcriptions des renseignements collectés sur une personne exerçant de telles fonctions, sont transmises à la CNCTR qui veille au caractère nécessaire et proportionné des atteintes, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats[183].

Il convient de préciser qu'outre son rôle consultatif dans le cadre de la procédure d'autorisation et son rôle renforcé lorsqu'il est question de certaines catégories de personnes, la CNCTR peut faire des recommandations tendant à l'interruption des opérations, et la destruction des renseignements collectés[184]. Elle adresse ces recommandations au Premier ministre, au ministre responsable de l'exécution et au service concerné, lorsqu'elle estime qu'une autorisation a été accordée, ou qu'une technique a été mise en œuvre, en méconnaissance du cadre légal[185]. Le refus de communiquer à la Commission les documents et les renseignements qu'elle a sollicités et la communication d'éléments non conforme au contenu des renseignements collectés tels qu'ils étaient au moment de la demande est puni d'un an d'emprisonnement et de 15 000 euros d'amende[186].

Elle peut également saisir le Conseil d'État, pour d'autres motifs que le non-suivi d'un avis défavorable[187], lorsque le Premier ministre ne donne pas suite à ces

[182] *Ibid*., art. L821-7, al. 1.
[183] *Ibid*. al. 4.
[184] *Ibid*., art. L821-8.
[185] *Ibid*., art. L833-6.
[186] *Ibid*., art. L833-3
[187] *Ibid*., art. L821-8.

recommandations, ou que ces suites sont estimées insuffisantes[188]. Pour l'heure, la CNCTR ne s'est jamais retrouvée dans cette situation[189].

En plus de ces modalités procédurales, applicables à toutes techniques de recueil de renseignement soumises à autorisation, la mise en œuvre d'une technique de captation de données informatiques impose le respect, des dispositions de l'article L.853-2 du CSI.

2.1.2.2 Les dispositions spécifiquement applicables à la technique de captation des données informatiques

Au titre de l'alinéa 2 de l'article L.853-2 du CSI, l'autorisation de mise en œuvre d'une technique est délivrée pour une durée maximale de deux mois. Cette autorisation est renouvelable dans les mêmes conditions de durée.

La demande d'autorisation doit préciser s'il est souhaité recourir à l'utilisation d'un dispositif technique pour de la captation de données informatiques au sens strict (CDI), c'est-à-dire pour accéder à des données, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un STAD, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques, ou pour du recueil de données informatiques (RDI), pour accéder à des données informatiques stockées dans un système informatique. Pour rappel, il s'agit de deux techniques distinctes, bien que, pour des questions de clarté, le document regroupe les deux techniques sous le terme de captation de données informatiques.

Avant la loi relative à la prévention d'actes de terrorisme et au renseignement de 2021[190], dont les articles 11 et 18 ont modifié le libellé de l'article L.853-2 du CSI, la durée maximale d'autorisation était dissociée selon la technique employée, d'un mois pour la technique de RDI, et de deux mois la technique de CDI. Cette différence avait été justifiée par le fait que la première technique était considérée comme plus attentatoire que la deuxième. La loi de 2021 a harmonisé la durée d'autorisation pour les deux techniques, la portant à deux mois sans distinction, notamment parce que « *dans avis sur le projet de loi, la CNCTR a indiqué ne pas avoir "observé, dans l'exercice de son*

[188] *Ibid*., art. L833-8.
[189] CNCTR, *8e Rapport d'activité 2023*, p. 58.
[190] Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, *JORF* n° 176 du 31 juillet 2021.

contrôle, de différences notables entre les deux techniques en termes d'atteintes à la vie privée, dans toutes ses composantes »[191].

Aux termes de l'alinéa 4, le service autorisé à recourir à la technique rend compte à la CNCTR de sa mise en œuvre. De plus, le caractère de l'urgence mentionné par l'article L.821-1 ne peut être invoqué que pour les seules autorisations fondées sur les finalités 1°, 4° et 5 de l'article L.811-3[192].

Lorsque la mise en œuvre de la technique nécessite l'introduction dans un véhicule ou dans un lieu privé, un avis exprès doit être obtenu auprès de la CNCTR, statuant en formation restreinte ou en formation plénière[193]. Le retrait et la maintenance des dispositifs nécessitant une telle intrusion, sont obtenus également par avis exprès de la CNCTR en formation plénière, lors des réunions mensuelles qui lui sont obligatoires dans l'exercice de ses missions[194].

Par ailleurs, la demande de mise en place doit faire état de toute indication permettant d'identifier le lieu, son usage, son propriétaire ou toute personne bénéficiant d'un droit, ainsi que la nature détaillée du dispositif envisagé. L'autorisation est délivrée pour une durée maximale de trente jours, renouvelable dans les mêmes conditions de durée que l'autorisation initiale, et ne vaut que pour les actes d'installation, d'utilisation, de maintenance ou de retrait des dispositifs techniques. En outre, le caractère d'urgence de l'alinéa 2 de l'article L.821-1 du CSI ne peut être invoqué que pour les finalités 1°, 4° et 5° ou, lorsqu'il est question d'un lieu privé à usage d'habitation, que pour la finalité 4° de l'article L.811-3. Enfin, le service autorisé doit rendre compte à la CNCTR de la mise en œuvre[195].

[191] CNCTR, Délibération n°2/2021 du 7 avril 2021, point 5.
[192] Art. L811-3, CSI 1° « *l'indépendance nationale, l'intégrité du territoire et la défense nationale », 4° « la prévention du terrorisme* », 5° « *la prévention : des atteintes à forme républicaine des institutions ; des actions tendant au maintien ou la reconstitution de groupement dissous en application de l'article L212-1 du CSI ; des violences collectives de nature à porter gravement atteinte à la paix publique* ».
[193] *Ibid*., art. L853-3, al. 1, cité par art. L853-2, al. 5.
[194] *Ibid*., art. L832-3, al. 4, cité par art. L853-3, al. 1, auquel fait référence art. L853-2, al. 5.
[195] *Ibid*., art. L853-3.

2.1.2.3 Les services autorisés à recourir à la technique de captation

L'alinéa 3 de l'article L.853-2 du CSI, traite des agents autorisés à utiliser les dispositifs techniques. Ce sont les agents appartenant à l'un des services mentionnés aux articles L.811-2 relatif aux services spécialisés de renseignement, et L.811-4 relatif aux services autres que ceux spécialisés de renseignement, dont la liste est fixée par décret en Conseil d'État.

Ces deux typologies d'acteurs ne bénéficient pas des mêmes compétences et autorisations. Le cadre de leur mission a été codifié par l'article 2 de la loi relative au renseignement de 2015[196] qui a créé les articles L.811-2 et L.811-4 du CSI.

Les services spécialisés de renseignement, ont pour mission, en France et à l'étranger, la recherche, la collecte, l'exploitation des renseignements relatifs aux enjeux géopolitiques et stratégiques, ainsi qu'aux menaces et aux risques susceptibles d'affecter la Nation. Ils mettent ces renseignements à la disposition du Gouvernement. Par cette mission, ils contribuent à l'anticipation, à la prévention et à l'entrave des risques et des menaces qui pèsent.

Ces services, dits « de premier cercle », agissent sous l'autorité du Gouvernement, et leur désignation ne nécessite pas l'avis de la CNCTR, contrairement aux services autres que ceux spécialisés de renseignement. Ces derniers relèvent des ministres de la Défense, de l'Intérieur et de la Justice[197] ainsi que des ministres chargés de l'économie, du budget ou des douanes.

[196] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n° 171 du 26 juillet 2015.
[197] Le ministre de la Justice a été ajouté par l'article 14 de la 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, *JORF* n° 129 du 4 juin 2016.

Le détail des services spécialisés de renseignement de premier cercle figure à l'article R811-1 du CSI, créé par le décret n° 2015-1185[198], tel que modifié successivement par l'article 2 du décret n° 2016-1337[199] et par l'article 2 du décret n° 2017-1095[200].

Selon les dispositions de l'article R811-1 du CSI, les services spécialisés de renseignement sont : la direction générale de la sécurité extérieure (DGSE), la direction du renseignement et de la sécurité de la défense (DRSD), la direction du renseignement militaire (DRM), la direction générale de la sécurité intérieure (DGSI), le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) et le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (TRACFIN).

La DGSE est placée sous l'autorité d'un directeur général qui relève directement du ministre de la Défense[201]. Elle a pour mission 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[202].

La DRSD est un SCN dont dispose le ministre de la Défense pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles[203]. Elle est compétente pour prévenir et rechercher les atteintes à la défense nationale, en mettant notamment en œuvre des mesures de contre-ingérence pour s'opposer à toute menace pouvant prendre la forme d'activités de terrorisme, d'espionnages, de subversion, de sabotage ou de crime organisé[204].

La DRM relève du chef d'état-major des armées, dont elle satisfait les besoins en renseignement d'intérêt militaire[205]. La DRM dispose de plusieurs organismes extérieurs, dont le centre de formation interarmées du renseignement, le centre

[198] Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, *JORF* n° 225 du 29 septembre 2015.
[199] Décret n° 2016-1337 du 7 octobre 2016 portant changement d'appellation de la direction de la protection et de la sécurité de la défense, *JORF* n° 236 du 9 octobre 2016.
[200] Décret n° 2017-1095 du 14 juin 2017 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme, *JORF* n° 139 du 15 juin 2017.
[201] Art. D3126-1, code de la défense (CD).
[202] *Ibid*., art. D3126-2.
[203] *Ibid*., art. D3126-5.
[204] *Ibid*., art. D3126-6, 3°.
[205] *Ibid*., art. D3126-10.

interarmées de recherche et de recueil du renseignement humain, le centre de recherche et d'analyse du cyberespace ainsi que le centre de renseignement géospatial interarmées[206].

La DGSI est un service de la police nationale, chargée de rechercher, de centraliser et d'exploiter le renseignement intéressant la sécurité nationale ou les intérêts fondamentaux de la Nation[207].

La DNRED relève des ministères économiques et financiers, par ailleurs rattachés à la direction générale des douanes et droits indirects. Elle est chargée de mettre en œuvre la politique du renseignement, des contrôles et de lutte contre la fraude de la direction générale des douanes et droits indirects. De plus, elle exerce des missions de recueil, de traitement et de diffusion du renseignement en matière de fraude fiscale grave et complexe et de son blanchiment, pour le compte de la direction générale des finances publiques[208].

TRACFIN est un SCN rattaché au ministre chargé de l'économie et au ministre chargé du budget[209]. Il est notamment compétent pour recueillir, traiter et diffuser le renseignement relatif aux infractions passibles d'une peine privative de liberté supérieure à un an, ou lié au financement du terrorisme[210]. Il peut également bénéficier des mêmes moyens pour les infractions de fraude fiscale[211].

La loi relative au renseignement de 2015 a par ailleurs créé l'article 323-8 du code pénal qui consacre l'inapplicabilité du chapitre relatif aux infractions d'atteintes aux STAD[212]

[206] Art. 1, arrêté du 30 mars 2016 portant organisation de la direction du renseignement militaire, *JORF* n° 83 du 8 avril 2016.
[207] Art. 1, décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure, *JORF* n° 102 du 2 mai 2014.
[208] Art. 2, arrêté du 29 octobre 2007 portant création d'un service à compétence nationale dénommée « direction nationale du renseignement et des enquêtes douanières, modifié par arrêté du 8 mars 2024, *JORF* n° 270 du 21 novembre 2007.
[209] Art. D561-33, CD.
[210] *Ibid*., art. L561-15 al 1.
[211] *Ibid*., art. L561-15 al 2.
[212] Pour rappel, ce chapitre proscrit notamment le fait d'accéder ou de se maintenir frauduleusement sur tout ou partie d'un STAD, l'entrave et le fonctionnement de ce dernier, l'altération frauduleuse des données contenues dans le système, mais aussi, la détention, l'importation (…) d'un équipement, d'un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une des infractions prévues par les articles 323-1 à 323-3 du code pénal.

aux services de premier cercle, pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation, mentionnés à l'article L.811-3 du CSI.

Les services de second cercle ne sont pas concernés par ces aménagements juridiques. Le décret qui les désigne doit préciser en outre, pour chaque service, les finalités et les techniques pouvant donner lieu à une autorisation. Leur marge de manœuvre est réduite par rapport aux services de premier cercle, qui peuvent poursuivre toute finalité sans qu'elles leur aient été limitativement attribuées au préalable.

Le détail de ces services figure à l'article R811-2 du CSI, créé par l'article 2 du décret n° 2015-1639[213]. Cet article a été modifié par dix décrets depuis sa codification en 2015[214]. La dernière modification a été effectuée par le biais de l'article 11 du décret n° 2023-1013[215].

À des fins de clarté et de compréhension, le tableau ci-dessous établit la liste des services visés au titre de la dernière modification par décret, ainsi que les finalités qu'ils peuvent respectivement poursuivre.

[213] Décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L811-4 du code de la sécurité intérieure, *JORF* n° 288 du 12 décembre 2015.

[214] Décret n° 2017-36 du 16 janvier 2017 ; décret n° 2018-543 du 29 juin 2018 ; décret n° 2019-684 du 28 juin 2019 ; décret n° 2019-1502 du 30 décembre 2019 ; décret n° 2019-1496 du 28 décembre 2019 ; décret n° 2021-1543 du 29 novembre 2021 ; décret n° 2022-277 du 28 février 2022 ; décret n° 2022-1359 du 26 octobre 2022 ; décret n° 2022-1703 du 27 décembre 2022.

[215] Décret n° 2023-1013 du 2 novembre 2023 relatif aux services déconcentrés et à l'organisation de la police nationale, *JORF* n° 0255 du 3 novembre 2023.

			F1	F2	F3	F4	F5	F6
Sous l'autorité du directeur général de la police nationale	La direction nationale du renseignement territorial		X			X	X	X
	Au sein de la direction nationale de la police judiciaire	Le service central des courses et jeux						X
		L'office antistupéfiants						X
		La sous-direction de la lutte contre la criminalité organisée et la délinquance						X
		La sous-direction de la lutte contre la criminalité financière						X
		La sous-direction antiterroriste				X		
		L'office anti-cybercriminalité				X		X
	Au sein de la direction nationale de la police aux frontières	Les unités en charge de la police judiciaire au sein de la direction de la police aux frontières des aérodromes parisiens						X
		L'office judiciaire de lutte contre le trafic illicite de migrants						X
		L'unité judiciaire de la division nationale de contrôle des transports internationaux de la sous-direction des frontières						X
	Au sein des directions territoriales de la police nationale	Les services du renseignement territorial	X			X	X	X
		Les services territoriaux de police judiciaire				X		X
	Au sein des directions inter-départementales de la police nationale	Les services départementaux du renseignement territorial	X			X	X	X
		Les services interdépartementaux de police judiciaire				X		X
		Les services départementaux ou locaux de police judiciaire						X
		Les unités en charge de la police judiciaire au sein des services départementaux ou interdépartementaux de police aux frontières						X
	Au sein des directions départementales de la police nationale	Les services départementaux du renseignement territorial	X			X	X	X
		Les services départementaux ou locaux de police judiciaire						X
		Les unités en charge de la police judiciaire au sein des services départementaux de police aux frontières						X
Sous l'autorité du directeur général de la gendarmerie nationale	Au sein de la direction des opérations et de l'emploi	La sous-direction de l'anticipation opérationnelle	X			X	X	
		La sous-direction de la police judiciaire	X			X		X
	Les sections de recherches de la gendarmerie nationale					X		X
	La division des opérations du commandement de la gendarmerie dans le cyberespace							X

Figure 2. Tableau récapitulatif des services de second cercle et des finalités qu'ils peuvent poursuivre dans le cadre de leur activité

Conclusion

Les différences notables de procédure entre la mise en œuvre de la captation par les services de renseignement ou de police judiciaire, tiennent à son contrôle, au nombre des personnes qualifiées l'exécution et, bien évidemment, les motifs invocables.

Les services de renseignement ne peuvent s'affranchir du contrôle de la CNCTR, qui se positionne comme un organe indépendant et autonome de l'exécutif. Bien qu'il soit fréquemment débattu de l'aspect contraignant de ses pouvoirs, puisque le Premier ministre peut outrepasser les avis négatifs d'autorisation émis par celle-ci, il s'agit d'une carence à laquelle le rôle du Conseil d'État semble pallier.

Les services de police judiciaire, quant à eux, n'ont pas d'organe explicitement indépendant et autonome pour le contrôle de la mise en œuvre d'une technique de captation. Ils sont sous l'égide du procureur de la République, dont l'indépendance ne cesse d'être remise en question. En effet les magistrats du parquet sont, selon les termes de l'article 5 de l'ordonnance du 22 décembre 1958[216], sous l'autorité du Garde des Sceaux, ministre de la Justice. Cette circonstance a fait l'objet d'une question prioritaire de constitutionnalité, auprès du Conseil constitutionnel, au regard notamment du principe de séparation des pouvoirs[217].

Lors de l'examen de cette QPC, le Conseil constitutionnel a jugé que les dispositions qui étaient contestées « *assuraient une conciliation équilibrée entre le principe d'indépendance de l'autorité judiciaire et les prérogatives que le Gouvernement tient de l'article 20*[218] *de la Constitution. Elles ne méconnaissent pas non plus la séparation des pouvoirs* ». La décision du Conseil n'est pas sans contradictions avec la vision qu'à la CEDH, des caractéristiques requises pour qualifier un organe « d'autorité judiciaire indépendante et impartiale ». L'autorité devrait en effet présenter des garanties d'indépendance à l'égard de l'exécutif et ne devrait pas, en principe, participer en tant que partie au procès[219].

---

[216] Ordonnance n° 58-1270 du 22 décembre 1958 portant loi organique relative au statut de la magistrature, *JORF* du 23 décembre 1958.

[217] Cons. const., 8 décembre 2017, n° 2017-680 QPC, *Indépendance des magistrats du parquet.*

[218] Constitution, art. 20 « *Le Gouvernement détermine et conduit la politique de la Nation, notamment en ce qui concerne les domaines d'action du ministère public* ».

[219] CEDH, 29 mars 2010, *Medvedyev et autres c. France*, n° 3394/03, §124.

Cependant, contrairement aux services de renseignement, les services de police judiciaire ne peuvent avoir recours à la captation que si « *les nécessités de l'enquête ou de l'information judiciaire l'exigent* ». La captation est une technique spéciale d'enquête, elle ne fait pas partie des outils ordinairement utilisés. Les services de renseignement sont moins liés par la présence d'un impératif ou d'une nécessité : le recours à cette technique n'implique pas des circonstances exceptionnelles. Elle doit simplement répondre à une des finalités limitativement énumérées.

Cela étant, l'essentiel à retenir est que la captation de données informatiques est, dans les deux cadres de sa mise en œuvre, opaque en ce qui concerne ses modalités techniques. Il est certain qu'elle s'appuie sur l'exploitation de vulnérabilités, toutefois, même sans être couvertes par le secret de la défense nationale, les méthodes employées demeurent floues.

Par ailleurs il semblait important de mentionner qu'à la date de rédaction du livrable, la captation de données informatiques en matière judiciaire pourrait être complétée par « *l'activation à distance d'un appareil électronique fixe* »[220] avec la mise en place d'un dispositif dans tout lieu utile, ou, si cela n'est pas concrètement possible pour des raisons de risques à l'intégrité physique des agents chargés de la mise en œuvre, à « *l'activation à distance d'un appareil électronique mobile, à l'insu ou sans le consentement de son propriétaire ou de son possesseur, aux seules fins de procéder à la captation, à la fixation, à la transmission et à l'enregistrement des paroles prononcées par des personnes ou de l'image de ces dernières pendant une durée strictement proportionnée à l'objectif recherché* »[221].

Le premier procédé concernerait tout STAD fixe, tel que les caméras d'ordinateurs et leurs micros, tandis que le deuxième concernerait les téléphones portables ou des voitures, à titre d'exemple. La procédure pour leur mise en place serait la même que pour la captation judiciaire.

Deux problématiques assez évidentes naissent de ce contexte naissant. Ce sont tout d'abord, les intrusions toujours plus attentatoires, puisque désormais, il ne s'agit plus de collecter des données présentes sur l'environnement numérique, mais bien des éléments de l'environnement « *réel* ». Ensuite, à l'instar de la translation de la technique de captation judiciaire, au domaine du renseignement, il n'est pas déraisonnable de supposer que ces deux procédés seront à terme également autorisés dans le cadre du

[220] Art. 38, Proposition de loi visant à sortir la France du piège du narcotrafic, 29 avril 2025, n° 102.
[221] *Ibid.,* art. 39.

renseignement, avec tout ce que les questions du secret de la défense nationale impliquent.

Le Conseil constitutionnel n'a pas jugé contraire à la Constitution ces deux procédés sous réserve que leur mise en œuvre reste cantonnée aux délits présentant des éléments de gravité et de complexité suffisants pour en justifier le recours[222].

2.2 L'accès aux données inaccessibles ou inintelligibles au cours de la procédure judiciaire

Dans le cadre d'une procédure judiciaire, telle que l'instruction, l'enquête préliminaire ou en flagrance, deux moyens sont à la disposition des autorités compétentes pour obtenir toutes les données pertinentes. Ce sont l'accès au support des données informatiques et la mise au clair des données chiffrées nécessaires à la manifestation de la vérité, régis respectivement par les articles 60-3[223], 77-1-3[224], 99-5[225] du CPP et les articles 230-1 à 230-5[226] du même code. Ces moyens sont susceptibles d'avoir recours à l'exploitation de vulnérabilités informatiques.

Il est courant, en effet, que les supports de données informatiques soient protégés par des mécanismes d'authentification[227] : les tablettes, téléphones portables ou ordinateur notamment. Et, même lorsque l'accès ne nécessite pas de techniques particulières, les données intéressant l'enquête peuvent avoir été chiffrées, les rendant inexploitables. Dans ce dernier cas, la procédure de mise au clair prévue par les articles susmentionnés est utilisée.

Les modalités relatives à l'accès au support de données informatiques sont étayées par l'article 60-3, les articles 77-1-3 et 99-5 du CPP renvoyant à ce dernier. Elles visent à régir la mise à disposition de ces supports, pour leur exploitation par les autorités compétentes sans porter atteinte à leur intégrité. Les trois articles ont été créés par

[222] Cons. const., 12 juin 2025, n° 2025-885, DC, *Loi visant à sortir la France du piège du narcotrafic*, cons. 309 à 338.
[223] Dans le cadre de l'enquête en flagrance.
[224] Dans le cadre de l'enquête préliminaire.
[225] Dans le cadre de la commission rogatoire.
[226] Dans le cadre sans distinction, de l'enquête préliminaire ou en flagrance et de l'instruction.
[227] CyberDico de l'ANSSI FR/EN, mis à jour le 5 décembre 2024, *op. cit.*, « *l'authentification a pour but de vérifier l'identité dont une entité se réclame* ». Il existe plusieurs manières d'authentifier une identité, par mot de passe, par certificat, par biométrie (liste non-exhaustive).

l'article 70 de la loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale de 2016[228] avec pour objectif de clarifier le cadre de ces opérations, qui étaient par ailleurs déjà mises en œuvre au cours de la procédure judiciaire, en dépit de l'absence de règles spécifiques[229].

Concernant la mise au clair des données chiffrées, il s'agit d'un moyen utilisable strictement pour accéder aux informations utiles à la manifestation de la vérité. Le code de procédure pénale définit les « *données chiffrées* » comme étant « *des données ayant fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, ou possédant un mécanisme d'authentification pour les protéger* »[230].

Les articles qui régissent ce moyen ont été créés par l'article 30 de la loi relative à la sécurité quotidienne de 2001[231], pour répondre aux nouvelles méthodes utilisées par les criminels, que les attentats de 2001 ont mis en lumière. En effet, les responsables de ces attentats avaient eu recours à des procédés de chiffrement afin de rendre illisibles certains de leurs messages électroniques. Ainsi, il est apparu impérieux et nécessaire d'offrir aux magistrats, des moyens adaptés aux évolutions techniques des criminels[232].

Les deux moyens précités, permettant l'accès au support de données informatiques et la mise au clair des données chiffrées, ne traitent cependant pas de la réquisition par les autorités, des conventions de déchiffrement, auprès des personnes ayant connaissance de cette dernière[233], ou fournissant une prestation de cryptologie[234]. À titre d'information, ces personnes s'exposent à des poursuites pénales en cas de refus de transmission ou de mise en œuvre, lorsque la convention secrète de chiffrement requise

[228] 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, *JORF* n° 129 du 4 juin 2016.
[229] Compte rendu intégral des débats de la séance du 31 mars 2016 du Sénat, relatif à la Loi n° 2016-731.
[230] Art. 230-1, al. 1 CPP.
[231] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, *JORF* n° 266 du 16 novembre 2001.
[232] LE ROUX (B.), *Rapport n° 3352 de l'Assemblée nationale fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la république en vue de la lecture définitive du projet de la loi relative à la sécurité quotidienne*, 24 octobre 2001, spéc. p. 66-67.
[233] Art. 60-1, al. 1 CPP.
[234] Art. L871-1 CSI.

a été utilisée pour préparer, faciliter ou commettre un crime ou un délit[235]. Il convient de préciser que, selon la Cour de cassation, le code de déverrouillage d'un téléphone mobile constitue une clé de chiffrement lorsque celui-ci est équipé d'un moyen de cryptologie[236].

Les moyens dont il est question dans la présente section, visent uniquement la mise en œuvre d'opérations techniques permettant de rendre accessibles ou intelligibles des données rendues hors de portée.

L'accès au support pouvant suffire dans certaines circonstances, à rendre exploitables des données intéressant la procédure, il conviendra de traiter ce moyen (**2.2.1**), avant celui de la mise au clair des données chiffrées (**2.2.2**).

2.2.1 L'accès au support contenant des données informatiques

Les articles 77-1-3 et 99-5 du CPP renvoient aux dispositions de l'article 60-3 du même code. Celui-ci sera donc pris comme base pour expliciter le cadre juridique qui autorise le procureur de la République, l'officier de police judiciaire (et l'agent de police judiciaire ou l'assistant d'enquête se trouvant sous son contrôle)[237], à requérir « *toute personne qualifiée (...) de procéder à l'ouverture des scellés pour réaliser une ou plusieurs copies de ces données ou de procéder aux opérations techniques nécessaires à leur mise à disposition (...), afin de permettre leur exploitation sans porter atteinte à leur intégrité* »[238].

L'ouverture des scellés, autrement dit des supports, est effectuée par « *l'injection d'un logiciel sur le terminal cible, permettant de casser le code de verrouillage qui participe au chiffrement des données stockées* »[239]. L'objectif étant soit de récupérer les

[235] Art. 434-15-2 CP : 270 000 euros d'amende et trois ans d'emprisonnement, portés à 450 000 euros d'amende et à cinq ans d'emprisonnement si la remise ou la mise en œuvre de la convention permettait d'éviter la commission ou de limiter les effets d'un crime ou d'un délit.

[236] Cass., ass. plén., 7 novembre 2022, n° 21-83.146.

[237] Art. 99-5 CPP « *pour les nécessités de l'exécution de la commission rogatoire, l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire ou l'assistant d'enquête (...) avec autorisation expresse du juge d'instruction* » ; art. 77-1-3 CPP, dans le cadre de l'enquête préliminaire « *sur autorisation du procureur de la République, l'officier ou l'agent de police judiciaire* ».

[238] Art. 60-3, al. 1 CPP.

[239] AUDIBERT (M.), *Le recueil de la preuve numérique : Enjeux et perspectives en procédure pénale*, *op. cit.*, p. 78.

informations de déverrouillage du support numérique ou, à défaut, de désactiver certaines fonctionnalités techniques[240].

Les personnes qualifiées peuvent être des experts judiciaires, selon les dispositions de l'article 157 du CPP, ou des personnes ayant prêté par écrit serment d'apporter leur concours à la justice en leur honneur et en leur conscience, selon les dispositions de l'article 60, alinéa 3 du CPP.

L'article 20 de la loi d'orientation et de programmation du ministère de l'Intérieur de 2023[241] a inséré un deuxième alinéa à l'article 60-3, qui permet aux autorités compétentes de solliciter les services ou organismes de police technique et scientifique de la police nationale et de la gendarmerie nationale, sans qu'il soit nécessaire d'établir une réquisition. Ces services ou organismes n'ont pas pour obligation de prêter serment ou d'être inscrits sur une des listes relatives aux experts judiciaires[242]. Cette modification avait pour objectif de « *libérer du temps d'enquête pour les officiers de police judiciaire, et de faciliter les missions des agents de police technique et scientifique* »[243].

Une fois la tâche exécutée, les personnes qualifiées, experts judiciaires ou services et organismes (ci-après désignés par, « les personnes qualifiées ») doivent rédiger un rapport contenant la description des opérations conduites et leurs conclusions. Ce rapport est signé et mentionne les noms et qualités des acteurs ayant participé aux opérations.

Si nécessaire, les personnes qualifiées sont habilitées à confectionner de nouveaux scellés après avoir procédé au reconditionnement des supports examinés. Le rapport ainsi que les scellés sont remis à l'autorité dont la demande émane, le dépôt faisant l'objet d'un procès-verbal[244].

Par ailleurs, après le recourt à la procédure d'accès au support de données informatiques, es autorités compétentes peuvent également utiliser le moyen consacré par les

[240] *Ibid.*, « *comme la limitation du nombre de tentatives de déverrouillage avant effacement (des données)* ».
[241] Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur, *JORF* n° 21 du 25 janvier 2023.
[242] Art. 60, al. 2 et 3 CPP, cités par art. 60-3, al. 2.
[243] Étude d'impact du Projet de loi d'orientation et de programmation du ministère de l'Intérieur en date du 6 septembre 2022, p. 96.
[244] Art. 163 et 166 CPP, que cité par 60-3, al. 1er.

articles 230-1 à 230-5, relatif à la mise au clair des données chiffrées : les deux moyens ne sont pas alternatifs.

2.2.2 La mise au clair des données chiffrées nécessaires à la manifestation de la vérité

L'article 230-1 alinéa 1, tel que modifié dernièrement par l'article 20 de la loi d'orientation et de programmation du ministère de l'Intérieur dispose que « *sans préjudice des articles 60, 77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, ou que ces données sont protégées par un mécanisme d'authentification, le procureur de la République, la juridiction d'instruction, l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, ou de la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir l'accès à ces informations, leur version en clair ainsi que, dans les cas où un moyen de cryptologie a été utilisé*[245]*, la convention secrète de déchiffrement, si cela apparaît nécessaire.* »

Les opérations de mise au clair doivent permettre de réaliser un des trois objectifs explicités par l'article. Elles peuvent tout d'abord chercher à obtenir l'accès aux informations. Cela semble correspondre à l'objectif d'accès au STAD ou au système d'information contenant les données. Une possibilité à mettre en parallèle avec les dispositions de l'article 57-1 du CPP, relatif à l'accès par les officiers de police judiciaire et les agents sous leur responsabilité, aux données intéressant l'enquête par le biais du système informatique implanté dans les lieux de perquisition, ou à distance si cela est possible, par le biais d'un système informatique leur appartenant. Ils ont la possibilité de requérir toute personne susceptible d'avoir connaissance de mesures appliquées pour protéger les données auxquelles ils leur aient permis d'accéder, ou susceptibles de leur remettre les informations permettant d'accéder à ces données[246].

[245] Art. 29 du code de la cybersécurité « *tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète* ».
[246] Art. 57-1, al. 5 CPP.

Les opérations techniques peuvent également avoir pour unique objectif, l'accès à la version en clair des informations saisies ou obtenues au cours de l'enquête. Ce serait l'hypothèse de données dont le support matériel ou numérique n'est pas verrouillé.

Enfin, l'article traite du cas où un moyen de cryptologie aurait été utilisé, en légitimant l'objectif de l'obtention de la convention secrète de déchiffrement. Cependant cette légitimité est conditionnelle. Il faut que l'obtention de la convention soit nécessaire aux fins de la mise au clair. De façon spéculative, cette condition semblerait répondre à l'importance de pouvoir garder secrètes les conventions de chiffrement, dans le cas où la connaissance de celles-ci donnerait aux autorités compétentes, l'accès théorique à toutes les communications chiffrées qui utiliseraient un système de chiffrement similaire.

Eu égard à ce qui a été dit, l'exploitation des vulnérabilités présentes dans le protocole de chiffrement, dans le STAD ou le système d'information, est une opération technique certainement utilisée.

Il convient de préciser que le type d'opération technique autorisée n'est pas explicité dans les articles. Il s'agit d'un choix de rédaction cohérent à l'aune des multiples et diverses méthodes de chiffrement, de protection des données, ainsi que des différents supports dans lesquelles elles sont susceptibles stockées. Il participe aussi à la longévité du cadre juridique.

Bien qu'une certaine marge de manœuvre soit nécessaire pour l'efficacité des opérations, l'opacité des techniques pose des risques en termes d'abus et d'arbitraire. Ce risque est particulièrement prégnant dans le cadre du recours aux moyens de l'État soumis au secret de la défense nationale.

Ce faisant, les modalités qui entourent ce moyen doivent être suffisamment explicites et propres à limiter ces fameux risques, dont la section **(2.2.2.1)** abordera le contenu. Les spécificités procédurales encadrant le recours aux moyens de l'État soumis au secret de la défense nationale seront traitées dans la section suivante **(2.2.2.2)**.

2.2.2.1 Les modalités encadrant les opérations techniques de mise au clair

Selon les dispositions de l'alinéa 1er de l'article 230-1 du CPP, sont autorisés à désigner toute personne physique ou morale qualifiée pour mettre en œuvre les opérations techniques ci-dessus visées, le procureur de la République, la juridiction d'instruction,

l'officier de police judiciaire sur autorisation de ceux-ci, ainsi que la juridiction de jugement saisie de l'affaire. Le contenu de cet article ayant été modifié par l'article 15 de la loi renforçant les dispositions relatives à la lutte contre le terrorisme de 2014[247], ce pouvoir de désignation est également étendu aux officiers de police judiciaire, sous autorisation du procureur ou du juge d'instruction.

Les données sur lesquelles les opérations vont être effectuées doivent avoir été saisies ou obtenues au cours de l'enquête ou de l'instruction, et leur contenu doit avoir été rendu inaccessible ou incompréhensible par des opérations de transformation, ou par un mécanisme d'authentification.

Les personnes désignées dans le cadre de cet article peuvent figurer sur une des listes dressées par la Cour de cassation ou des cours d'appel relatives aux experts judiciaires[248], ou être choisies en dehors de celles-ci. Dans ce cas, elles doivent prêter par écrit serment d'apporter leur concours à la justice en leur honneur et en leur conscience[249].

Par ailleurs, lorsqu'un expert judiciaire est désigné devant une juridiction d'instruction (et non pas dans le cadre de l'enquête préliminaire ou de flagrance), un procès-verbal de prestation de serment doit être dressé et signé par le magistrat compétent, l'expert et le greffier. En cas d'empêchement, le serment peut également être reçu par écrit et annexé au dossier de la procédure. Les motifs doivent être précisés[250].

Si la personne désignée est une personne morale, son représentant légal doit soumettre à l'agrément du procureur de la République, de l'officier de police judiciaire ou de la juridiction saisie de l'affaire, le nom des personnes physiques qui, au sein de celle-ci et en son nom, effectueront les opérations techniques demandées[251].

Toutes les personnes désignées sont autorisées à procéder à l'ouverture des scellés[252], qu'il s'agisse du support physique contenant les données, ou d'une copie de celles-ci[253].

---

[247] Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, *JORF* n° 0263 du 14 novembre 2014.
[248] Art. 157 CPP.
[249] *Ibid*., art. 60, al. 3 CPP.
[250] *Ibid*., art. 160.
[251] *Ibid*., art. 230-1, al. 2.
[252] *Ibid*., art. 60, al. 4 ; art. 163 et 77-1, al. 2.
[253] *Ibid*., art. 97, al. 3 ; art. 56, al. 5.

Une fois la tâche exécutée, ou lorsqu'il apparaît que ces opérations sont techniquement impossibles, les personnes désignées doivent rédiger un rapport contenant la description des opérations conduites et leurs conclusions. Ce rapport est signé et mentionne les noms et qualités des acteurs ayant participé aux opérations. Si nécessaire, elles sont habilitées à confectionner de nouveaux scellés après avoir procédé au reconditionnement des supports examinés. Le rapport ainsi que les scellés sont remis à l'autorité dont la demande émane, le dépôt faisant l'objet d'un procès-verbal[254].

Les décisions prises dans le cadre de cette procédure n'ont pas de caractère juridictionnel et ne sont pas susceptibles de recours[255].

En termes de garanties visant à limiter les risques d'arbitraire et d'abus, le cadre juridique de la mise au clair de données chiffrées peut être perçu comme lacunaire. D'une part, l'opacité des techniques autorisées devrait imposer la présence d'un contrôle indépendant, par un organe suffisamment compétent pour comprendre la nature des actes effectués. En effet, en l'absence d'un tel contrôle, la véracité et l'intégrité des éléments obtenus peuvent être légitimement contestées. En conséquence, la fiabilité des preuves recueillies n'est pas assurée.

D'autre part, les opérations de mise au clair nécessitent le déchiffrement sans distinction de toutes les données saisies. Or, le chapitre traitant de cette procédure ne fait pas mention de mesures de minimisation, qui participeraient pourtant à garantir que l'ingérence dans la vie privée des personnes visées, serait proportionnée.

La question de la véracité des éléments obtenus et de la bonne foi des personnes désignées pour effectuer ces opérations est d'autant plus cruciale lorsqu'il est fait usage des moyens de l'État soumis au secret de la défense nationale. Dans ce cadre précis, la procédure a été adaptée pour répondre aux risques que le recours à ce type de moyen engendre. Par ailleurs, ces aménagements ont été appréciés et validés par le Conseil constitutionnel dans sa décision du 8 avril 2022, relative aux conditions de recours aux moyens de l'État soumis au secret de la défense nationale dans le cadre des articles 230-1 à 230-5 et 706-102-1 du CPP[256].

[254] *Ibid*., art. 163 et 166.
[255] *Ibid*., art. 230-4.
[256] Cons. Const., 8 avril 2022, n° 2022-987 QPC, *Conditions de recours aux moyens des services de l'État soumis au secret de la défense nationale dans le cadre de certaines procédures pénales*.

2.2.2.2. Les spécificités encadrant le recours aux moyens de l'État soumis au secret de la défense nationale

L'article 230-1, alinéa 3, dispose que « *si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction, l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'État soumis au secret de la défense nationale* »

Les deux conditions cumulatives à son recours : une peine d'emprisonnement égale ou supérieure à deux ans et si des nécessités de l'enquête ou de l'instruction l'exigent, permettent de qualifier ce moyen de « dernière solution ». Ce constat laisse entendre que les moyens ordinaires auraient échoué à la mise au clair.

Contrairement à la procédure ordinaire, consacrée aux alinéas 1 et 2 de l'article, les autorités compétentes doivent adresser une réquisition, il ne peut s'agir d'une simple désignation.

Celle-ci doit être adressée par écrit à un organisme technique soumis au secret de la défense nationale désigné par décret, avec le support physique contenant les données à mettre au clair ou une copie de celui-ci[257]. Elle fixe également le délai prévu pour les opérations de mise au clair, qui peut être prorogé dans les mêmes conditions de forme. Les autorités judiciaires susvisées peuvent à tout moment ordonner l'interruption.

En application de l'alinéa 1er de l'article 230-2, le décret n° 2002-1073[258] a créé le **C**entre **T**echnique d'**A**ssistance (CTA), pour remplir les fonctions de l'organisme technique soumis au secret de la défense nationale visé par l'article. Il est placé sous l'autorité du directeur général de la sécurité intérieure. Le CTA est habilité à l'ouverture ou à la réouverture des scellés, ainsi qu'à la confection de nouveaux. Il doit cependant obtenir l'autorisation du procureur de la République, de la juridiction d'instruction ou

[257] Art. 230-2, al. 1 CPP.

[258] Décret n° 2002-1073 du 7 août 2002 d'application de l'article 30 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d'assistance, *JORF* 5 janvier 2002.

de jugement saisie de l'affaire pour altérer le support physique, lorsqu'il existe un risque de destruction des données ou du support qui les contient[259].

Le fait d'imposer une autorisation supplémentaire dans le cas ci-dessus envisagé semble viser la protection du CTA d'éventuelles retombées, dans le cas où la destruction des données ou du support entrainerait l'échec ou la mise en difficulté de la poursuite judiciaire.

Les résultats obtenus et les pièces reçus sont retournés par le responsable du CTA à l'auteur de la réquisition[260] dès l'achèvement des opérations ou lorsqu'elles apparaissent techniquement impossibles, mais aussi à l'expiration du délai prescrit ou à la réception d'un ordre d'interruption. Les résultats sont accompagnés des indications techniques utiles à leur compréhension et leur exploitation. Enfin, le CTA doit également transmettre une attestation certifiant la sincérité des résultats transmis[261].

La transmission d'indications techniques participe à garantir que les autorités réceptrices disposeront de suffisamment de connaissances pour apprécier avec justesse les éléments mis au clair. Dans le cadre d'un hypothétique procès, cette circonstance est cruciale : elle permet d'assurer un certain degré de qualité, vis-à-vis des observations, examens et analyses effectués par les magistrats. Cependant, la Cour de cassation a rappelé que la seule transmission d'indications techniques n'était pas suffisante, et que l'attestation certifiant de la sincérité des résultats était cruciale.[262]

Par ailleurs, les données nécessitant une mise au clair, les résultats obtenus et les indications techniques qui les accompagnent sont susceptibles d'être protégés au titre du secret de la défense nationale. Dans ce cas, il est impératif d'obtenir l'avis favorable de l'autorité administrative en charge de la classification des informations au titre du secret de la défense nationale. Une fois la demande de transmission déposée, cette autorité administrative a l'obligation de saisir de la Commission du secret de la défense nationale (CSDN), qui dispose d'un délai de deux mois pour lui rendre un avis favorable ou défavorable. La CSDN dispose de pouvoirs d'investigation. L'autorité administrative doit ensuite transmettre sa propre décision assortie de l'avis de la CSDN dans un délai de quinze jours après réception de celui-ci, ou à l'expiration du délai de deux mois qui

[259] Art. 230-2, al. 2 CPP.
[260] Ou au magistrat mandat lorsque la réquisition a été adressée directement.
[261] Art. 230-3 CPP.
[262] C. cass., ch. crim., 25 octobre 2022, n° 21-85.763, c. 33-39.

lie la Commission[263]. Les éléments obtenus font l'objet d'un procès-verbal de réception et sont versés au dossier de la procédure.

Toutes les décisions prises dans le cadre de l'ensemble de la procédure de mise au clair de données chiffrées n'ont pas de caractère juridictionnel, elles ne sont pas susceptibles de recours.

Comme expliqué dans la section relative à la captation de données informatiques par les services de police judiciaire, le Conseil constitutionnel n'a pas jugé inconstitutionnel le recours aux moyens de l'État soumis au secret de la défense nationale. La procédure encadrant ces moyens serait le fruit d'une conciliation équilibrée entre les droits de la défense, le principe du contradictoire, « *l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation, dont participe le secret de la défense nationale* »[264].

Cet équilibre est renforcé par les obligations qui incombent au CTA, notamment l'impératif d'une attestation certifiant la sincérité des résultats obtenus ou l'autorisation supplémentaire en cas de risques d'altération du support numérique. Le procès-verbal est également souligné par le Conseil constitutionnel, dans la mesure où il permet aux personnes concernées par la mise au clair d'avoir accès à son contenu.

[263] Procédure visée aux art. L2312-4 à L2312-8 CD, cités par art. 230-2 al. 3 CPP.
[264] Cons. Const., 8 avril 2022, préc., §15.

Conclusion

Qu'il s'agisse de la captation de données informatiques, de l'accès au support de données informatiques ou de la mise au clair de données chiffrées, le voile qui couvre les techniques employées ne semble pas pouvoir être levé.

L'opacité de celles-ci est une condition non discutable, une qualité intrinsèque à leur efficacité. Il va sans dire que la connaissance du grand public des méthodes employées, en dehors des enjeux d'efficacité, accentuerait le risque de détournement de leur usage pour commettre une des infractions visées aux articles 323-1 à 323-3 du code pénal, relatifs aux atteintes aux STAD, ou 226-1 et 226-15 du même code, relatifs aux atteintes à la personnalité.

Partant, le cadre juridique semble davantage prioriser la clarification des critères permettant de distinguer la commission d'une des infractions susmentionnées, de l'exercice d'une mission légitime. Les types d'exploitation de vulnérabilités informatiques ne sont pas l'objet du cadre en application duquel, ces techniques pourraient être employées. Pourtant, toutes les méthodes d'exploitation ne se valent pas en termes de qualité, d'efficacité ou de coûts financiers. Or, la légalité de l'exploitation ne pouvant être constatée qu'au regard des missions de la police judiciaire ou du renseignement, l'enjeu du choix de la méthode aurait pu être légitimement abordé par le législateur. En effet, les résultats obtenus ont vocation à être utilisés dans le cadre d'une procédure, laquelle aura des conséquences sur la personne concernée.

Cependant, imposer aux autorités nationales d'apprécier en détail les différentes techniques d'exploitation avant désignation ou réquisition supposerait qu'ils soient suffisamment formés pour avoir un regard critique sur le choix.

Cette problématique concerne principalement le cadre des services judiciaires. Les services de renseignement doivent répondre à la CNCTR qui, eu égard à ses missions, dispose en théorie d'un degré suffisant d'expertise pour assurer l'efficacité de son contrôle.

Par ailleurs, les caractéristiques que doivent revêtir les autorités de contrôle, pour être à même de garantir la nécessité de la méthode employée et sa capacité à répondre précisément à l'objectif visé, ont déjà été discutées au niveau européen, par la CEDH. Sa jurisprudence offre un point de vue intéressant sur la conventionnalité du cadre national et des perspectives d'évolutions procédurales.

L'impact du droit de l'Union européenne se situe principalement sur la relation entre la gravité de l'acte réprimé et l'ingérence causée par le moyen envisagé pour y remédier. L'Union s'est également saisie des questions de la surveillance de certaines catégories de personnes, comme les journalistes.

Les liens entre le droit européen et le droit national sont en réalités complexes. L'organisation, le partage de compétence, le type de procédure pouvant donner lieu à une jurisprudence ne favorisent pas la création de lignes de conduite claires, applicables à toutes circonstances où l'exploitation de vulnérabilités informatiques est autorisée.

2.3 Les incidences du droit européen

Pris dans son ensemble, le droit européen traite de deux composantes essentielles à l'établissement du cadre juridique. La création de normes traitant de la prévention, la recherche et la répression des infractions lorsque celles-ci ou l'enquête afférente ont une teneur numérique, et le contrôle stricto sensu des ingérences causées par ces normes dans les droits fondamentaux.

Les différences organisationnelles entre le Conseil de l'Europe (**2.3.1**) et de l'Union européenne (**2.3.2**) ont créé des modes de régulation dont les divergences se situent principalement au niveau de la marge de manœuvre laissée aux États.

2.3.1 Le droit du Conseil de l'Europe

Dans le cadre de ce livrable, l'analyse du droit du Conseil de l'Europe portera sur la Convention de Budapest sur la cybercriminalité (**2.3.1.1**) et sur la jurisprudence de la CEDH. Celle-ci est applicable en matière de captation de données informatiques (**2.3.1.2**), d'accès au support de données informatiques et de mise au clair de données chiffrées (**2.3.1.3**).

2.3.1.1 La Convention de Budapest sur la cybercriminalité

La Convention de Budapest sur la cybercriminalité traite la question du droit procédural en matière d'enquête, dans sa section 2.

Son article 14 enjoint aux Parties d'adopter des mesures législatives pour instaurer des pouvoirs et des procédures aux fins d'enquêtes ou de procédures pénales spécifiques, notamment pour la collecte de preuves électroniques de toute infraction pénale[265]. L'exploitation de vulnérabilités informatiques peut faire partie de ces pouvoirs. La Convention contraint cependant l'adoption de telles mesures, au respect de la Convention européenne et du Pacte international relatif aux droits civils et politiques des Nations Unies[266]. Ceci implique la mise en place, lorsque cela est approprié, d'une supervision judiciaire ou indépendante, de motifs justifiant l'application et des

[265] *Ibid*., art. 14, par. 2, sous c).
[266] Pacte international relatif aux droits civils et politiques des Nations Unies, adopté à New York le 16 décembre 1966.

limitations du champ d'application et de la durée des pouvoirs ou de la procédure en question[267].

L'article 19 sur la perquisition et la saisie de données informatiques stockées reste le plus pertinent aux cas envisagés dans les précédentes sections. Il énonce que « *chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire, à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et, à un support de stockage informatique permettant de stocker des données informatiques sur son territoire* »[268]. L'article enjoint aussi de légiférer le cas où les données recherchées sont stockées dans un autre système d'information, mais qu'elles sont accessibles depuis le système initial. Les termes « *à accéder d'une façon similaire* » ne renvoient pas spécifiquement à la technique de captation de données informatiques, il ne l'exclut cependant pas.

Selon les termes de l'article 19, paragraphe 3, les mesures adoptées donnent aux autorités compétentes les prérogatives nécessaires pour « *saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique ; réaliser et conserver une copie de ces données informatiques ; préserver l'intégrité des données informatiques stockées pertinentes ; rendre inaccessible ou enlever ces données informatiques du système informatique consulté* ».

La Convention ne précise pas le type d'opérations autorisées aux fins de ces objectifs. Et, puisque les autorités compétentes doivent être en mesure de réaliser une copie des données informatiques stockées, elle ne saurait être interprétée comme interdisant l'exploitation de vulnérabilités informatiques. Une interprétation corroborée par le fait que les autorités compétentes devraient avoir pour prérogative de « *préserver l'intégrité des données informatiques pertinentes* ». Cette prérogative ne peut être dissociée de la possibilité de recourir à l'exploitation de vulnérabilités informatiques dans la mesure où ce type d'opération peut être nécessaire pour désactiver certaines fonctionnalités de protection, notamment celles qui entraînent la destruction des données après un nombre défini de tentatives échouées d'accès.

Enfin, le paragraphe 4 de l'article invite les Parties à adopter des mesures pour « *habiliter (leurs) autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les*

[267] Art. 15, Convention sur la cybercriminalité.
[268] *Ibid.*, art. 19, par. 1.

données qu'il contient, de fournir les informations raisonnablement nécessaires ». La Convention ne couvre que la collaboration visant à « *fournir les informations* » et non à « *mettre en œuvre des opérations* ». De plus, seules les informations raisonnablement utiles à l'objectif peuvent être requises. À cet égard, le droit national va plus loin que la Convention en instaurant des mécanismes pour requérir ou désigner des experts et personnes qualifiées, capables d'effectuer les opérations nécessaires à l'accès au système d'information, ou aux données protégées qu'il contient.

Cela ne signifie pas que le droit national est inconventionnel. La Convention n'impose que des mesures minimales afin d'homogénéiser la législation des États signataires, et cherche à concrétiser une vision commune des pouvoirs d'enquêtes utiles à accorder vis-à-vis de l'incidence des nouvelles technologies sur la criminalité.

Ainsi, même en allant au-delà des dispositions de la Convention, le droit national reste conventionnel tant qu'il respecte la Convention européenne des droits de l'homme et le Pacte international relatifs aux droits civils et politiques des Nations unies.

2.3.1.2 La jurisprudence de la Cour européenne des droits de l'homme en matière de captation de données informatiques

Au niveau de la Convention européenne des droits de l'homme, une difficulté peut se poser sur la notion de juridiction de l'État partie. En effet, selon le premier article de la Convention « *les Hautes Parties contractantes reconnaissent à toute personne relevant de leur juridiction*[269] *les droits et libertés définis au titre I de la présente Convention* ».

Sur cette question, la CEDH a déterminé que le caractère transfrontalier de la captation de données informatiques ne faisait pas obstacle à la compétence juridictionnelle d'un État dont l'opération de surveillance aurait concerné des individus en dehors de son territoire. Un individu, même s'il ne réside pas en France, peut engager la responsabilité de l'État français : la juridiction d'un État est établie lorsque les actes dénoncés ont été effectués depuis son territoire[270].

Dans le cadre du recours aux nouvelles technologies par les autorités nationales à des fins de surveillance, des critères ont été dégagés par la Cour pour apprécier la conventionnalité de ces opérations. Ils sont généralement issus des jurisprudences qui

[269] Nous soulignons.
[270] CEDH, 24 septembre 2024, *A.L. et E.J c. France*, n° 44715/20 et n° 47930/21.

traitent des violations de l'article 8 de la Convention, selon lequel « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».

Les droits inscrits à l'article 8 ne sont pas absolus, et peuvent être limités. Cependant, pour être conventionnelles, ces limitations doivent respecter les termes du paragraphe 2 de l'article susmentionné : « *il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi, et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

Pour résumer, l'ingérence doit être prévue par la loi, viser un ou plusieurs des buts légitimes énumérés, et doit nécessaire dans une société démocratique, pour atteindre ce ou ces buts[271]. Les mesures encadrant l'ingérence doivent être compatibles avec le principe de prééminence du droit : être accessibles à la personne concernée et prévisibles quant à ses effets[272]. Toutefois, ces critères ont été adaptés au cas de la surveillance. En effet, la Cour n'est pas sans savoir que ceux-ci peuvent se révéler incompatibles avec l'efficacité des opérations de surveillance, comme le critère de prévisibilité de la loi. Elle a notamment dit que, « *la prévisibilité ne pouvait se comprendre de la même façon que dans la plupart des domaines*[273]. *Dans le contexte particulier des mesures de surveillance secrète, telle que l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles de recourir à ce type de mesures de manière à ce qu'il puisse adapter sa conduite en conséquence* »[274].

Ainsi, pour être conforme au droit conventionnel, le cadre juridique de la captation de données informatiques doit répondre à plusieurs conditions, qu'il convient de lister.

En termes de qualité de la loi, la base légale doit au minimum énoncer la nature des infractions susceptibles de donner lieu à sa mise en œuvre ; les catégories de personnes dont les données sont susceptibles d'être captées ; les limites à la durée d'exécution 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

[271] CEDH, 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06, §227.
[272] *Ibid.*, §228.
[273] Nous soulignons.
[274] CEDH, 25 mai 2021, *Centrum för rättvisa c. Suède*, n° 35252/08, §247.

d'autres parties ; les circonstances dans lesquelles les données captées peuvent ou doivent être effacées ou détruites[275].

La base légale n'a pas pour obligation de détailler la nature des opérations qui pourront être effectuées. Les méthodes d'exploitation de vulnérabilités peuvent être dissimulées.

En effet, la qualité de la loi est davantage liée à la question de la « *nécessité* ». Elle doit être suffisamment claire pour garantir que son application répondra à une nécessité « *dans une société démocratique* », en imposant des garde-fous suffisants et effectifs contre l'abus et l'arbitraire[276]. Ces garde-fous permettent de garantir que l'ingérence causée par les opérations techniques, peu importe leur nature, sera réduite au strict nécessaire.

La mise en place d'une procédure d'autorisation en est un. Il n'est pas impératif que l'organe compétent pour ce faire soit judiciaire, tant qu'il est suffisamment indépendant de l'exécutif[277]. En outre, l'organe doit disposer d'éléments suffisants pour s'assurer que la mesure réponde au critère de « *nécessité dans une société démocratique* », qu'il existe des soupçons ou indices raisonnables que l'objet de surveillance ait ou projette de commettre une ou plusieurs infractions, ou des actes attentant à la sécurité nationale[278].

Sur ce point, la base légale qui traite de la captation de données informatiques par les services de police judiciaire est susceptible d'être inconventionnelle. Comme expliqué dans les sections précédentes selon la Cour, l'indépendance du procureur de la République vis-à-vis de l'exécutif n'est pas suffisamment établie. Une condamnation de la France pour ce motif n'est toutefois pas assurée. La Cour devra scrupuleusement analyser la portée du lien entre l'exécutif et le procureur de la République, notamment la marge de manœuvre dont il dispose, les motifs susceptibles de l'exposer à des sanctions, et si ces faits limitent son autonomie dans le cadre spécifique de l'autorisation d'une mesure de captation.

Le cadre juridique doit également préciser les modalités de contrôle et de supervision de la conduite des opérations, et les recours prévus en droit interne.

Le contrôle et la supervision des opérations peuvent être effectués par une juridiction, ou un organe indépendant, investi de pouvoirs et d'attributions suffisants pour exercer

[275] CEDH, 25 mai 2021, *Big Brother watch c. Royaume-Uni*, n° 58170/14, n° 62322/14, n° 24960/15, § 335.
[276] *Ibid.*, §334.
[277] CEDH, 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06, §258.
[278] *Ibid.*, §260.

un contrôle efficace et permanent[279]. Idéalement, l'autorité de contrôle et de supervision devrait être la même que celle ayant autorisé la mise en œuvre de la mesure. Cette continuité renforce la solidité et l'efficacité du contrôle, assurant ainsi la régularité des opérations.

En termes de recours, la Cour conserve une certaine souplesse, consciente qu'aux fins de contester la mise en œuvre d'une mesure de surveillance, l'individu devrait en théorie avoir été préalablement notifié[280]. Or, cette notification n'est pas compatible avec le principe de surveillance. Ainsi, elle valorise la présence d'un mécanisme permettant à tout individu de faire vérifier qu'aucune mesure n'ait été irrégulièrement mise en œuvre, ou, lorsque la mesure aboutit sur une procédure judiciaire, la possibilité de faire examiner son cadre de mise en œuvre.

2.3.1.3 La jurisprudence de la Cour européenne des droits de l'homme en matière d'accès au support de données ou de mise au clair de données chiffrées

L'accès au support de données informatiques et la mise au clair de données chiffrées tombent également sous le joug de l'article 8 de la Convention, bien que ces opérations ne bénéficient pas d'un cadre jurisprudentiel précis et étoffé, à l'instar de la surveillance.

Cependant, il est évident que des garanties contre l'abus et l'arbitraire doivent être mises en place pour ce type d'opération. La Cour, se prononçant en 2024 dans l'arrêt *Podchasov c. Russie*, a affirmé que « *la protection de l'article 8 serait affaiblie de façon inacceptable, si les recours aux technologies modernes par le système judiciaire étaient autorisés à tout prix, sans mettre en balance précautionneusement les bénéfices de cet usage intensif, et les points d'intérêts cruciaux en matière de vie privée* »[281]. Cet arrêt concernait la réquisition, par les autorités russes, des conventions secrètes de chiffrement de la messagerie électronique Telegram.

Par ailleurs, la législation régissant l'accès au support de données informatiques et la mise au clair de données chiffrées constitue une ingérence au droit consacré par l'article 8 de la Convention. Partant, elle doit respecter le contenu du paragraphe 2 du même article : l'ingérence doit être prévue par la loi, viser un ou plusieurs des buts

[279] *Ibid*., §275.
[280] *Ibid*., §234.
[281] CEDH, 13 février 2024, *Podchasov c. Russie*, n° 33696/19, §62.

légitimes énumérés, et doit nécessaire dans une société démocratique, pour atteindre ce ou ces buts[282].

De plus, certains principes dégagés par la jurisprudence relative à la surveillance peuvent être applicables aux opérations dont il est question dans cette section.

La base légale doit être constituée de règles claires régissant le champ et l'application des mesures afin de limiter les risques d'abus et d'usage arbitraire. Elle doit encadrer strictement la durée des opérations, la conservation des données auxquelles il a été accédé, leur utilisation et leur accès par des tiers. Elle précise en outre les mesures visant à préserver l'intégrité et la confidentialité des données ainsi que les modalités de destruction de celles-ci[283]. Les autorisations de mises en œuvre doivent être délivrées par une autorité judiciaire ou un organe décisionnel, indépendant et impartial.

Ne doivent être conservées que les données strictement nécessaires à la réalisation de l'objectif et la possibilité d'identifier leur propriétaire doit être confinée à une durée qui n'excèdent pas les besoins de la mission[284].

À l'aune de ces principes, il est possible de juger le cadre national, français, lacunaire sur les mesures garantissant l'intégrité des données. Seul le cas du recours aux moyens de l'État soumis au secret de la défense nationale aborde cette question, en imposant que le Centre Technique d'Assistance obtienne une seconde autorisation lorsqu'il existe un risque de destruction ou d'altération. Il ne s'agit cependant pas d'une obligation technique, qui imposerait aux autorités compétentes de recourir uniquement à certaines méthodes, celles qui minimiseraient les risques d'atteinte à l'intégrité. De surcroit, le droit national est opaque quant aux potentielles obligations de minimisation des risques, qui incomberaient aux experts et aux personnes qualifiées requises ou désignées.

Enfin, même si l'opposition de la Cour aux législations qui généraliseraient l'accès aux données de communication électronique et qui auraient pour conséquence d'affaiblir durablement leur chiffrement est avérée[285], elle ne s'est pas prononcée sur les alternatives techniques à privilégier. Simplement, elle valorise les approches ciblées qui circonscriraient les autorisations d'accès ou de déchiffrement à la réunion de

[282] CEDH, 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06, §227.
[283] *Ibid.*, §63.
[284] *Ibidem*.
[285] *Ibid.*, §73.

circonstances précises, systématiquement appréciées pour chaque demande. Sur ce point, le droit national semble être en conformité.

Conclusion

Le droit du Conseil de l'Europe impose à la fois la création de pouvoirs et prérogatives aptes à permettre aux autorités nationales d'exercer efficacement leur mission, et la mise en place de mécanismes précis pour limiter l'arbitraire et les risques d'abus.

Le droit français est lacunaire sur deux points. Au niveau des services de police judiciaire, l'organe responsable de l'autorisation, du contrôle et de la supervision des opérations, ne peut être qualifié d'indépendant selon les critères posés par la CEDH.

Il ne s'agit pas d'une vision partagée par le Conseil constitutionnel qui, rappelons-le, a jugé, lors d'une QPC en 2017[286], que la base légale relative au statut des procureurs de la République « *assurait une conciliation équilibrée entre le principe d'indépendance de l'autorité judiciaire et les prérogatives que le Gouvernement tient de l'article 20*[287] *de la Constitution. Elle ne méconnait pas non plus la séparation des pouvoirs* ».

Ces différences de point de vue pourraient avoir des conséquences sur position de la France à l'égard de la jurisprudence de la Cour puisque, dans l'hypothèse d'une condamnation, il n'est pas certain qu'en résulte une évolution du statut des procureurs de la République.

Second point où le droit national est lacunaire, les mesures garantissant l'intégrité des données en clair, ou auxquelles il a été accédé. L'opacité des techniques utilisant l'exploitation de vulnérabilités informatiques est certes conventionnelle, mais l'absence de mentions sur le choix de la méthode, qui devrait être celui minimisant les risques d'atteintes à l'intégrité, ou sur les processus techniques de minimisation standardisés, interroge la conventionnalité de la procédure relative aux experts et personnes qualifiées.

Par ailleurs, de futurs développements jurisprudentiels pourraient expliciter la portée de la Convention sur l'accès au support de données informatiques ou la mise au clair de données chiffrées, ces deux pans ayant été peu abordés.

Cela étant dit, le cadre juridique actuel doit également être conforme au droit de l'Union européenne, qu'il convient à présent d'analyser.

---

[286] Cons. Const., 8 décembre 2017, n° 2017-680 QPC, *Indépendance des magistrats du parquet.*

[287] Le Gouvernement détermine et conduit la politique de la Nation, notamment en ce qui concerne les domaines d'action du ministère public.

2.3.2 Le droit de l'Union européenne

Les actes de l'Union européenne bénéficient parfois d'une interprétation par la CJUE au regard du droit interne de certains États membres. Ces interprétations permettent à la fois aux normes de perdurer en résistant aux évolutions technologiques, mais également de préciser leur portée à l'aune des jurisprudences déjà rendues afin de former un ensemble cohérent.

Chacune des normes, la directive 2002/58[288] (**2.3.2.1**), la directive 2016/680[289] (**2.3.2.2**), la directive 2014/41[290] (**2.3.2.3**), et le règlement 2022/0277[291] (**2.3.2.4**), seront ainsi abordées conjointement aux jurisprudences pertinentes en la matière.

2.3.2.1 La directive 2002/58 (« directive Vie Privée »)

La directive Vie Privée traite de la protection du droit à la vie privée dans le secteur des communications électroniques, ainsi que de la libre circulation de ces données, équipements ou services de communications électroniques, sur le territoire de l'Union. Son incidence en matière de captation de données informatiques a été étayée par le Parlement européen, dans ses recommandations vis-à-vis de l'utilisation de Pegasus, et autres logiciels espions de surveillance équivalents[292].

---

[288] 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), *JOUE* L 201, 31 juillet 2002, (Directive Vie Privée).

[289] 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, *JOUE* L 119, 4 mai 2016 (Directive Police-Justice).

[290] Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, *JOUE* L 130, 1 mai 2014 (Directive 2014/41).

[291] Règlement (UE)2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE, *JOUE* L, 17 avril 2024 (Règlement sur la liberté des médias).

[292] Recommandation du Parlement européen du 15 juin 2023 à l'intention du Conseil et de la Commission à la suite de l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (2023/2500(RSP)).

Selon ces recommandations, le déploiement de ce type d'outils de surveillance constituerait une « *restriction au droit à la protection des équipements terminaux prévu par la directive vie privée et communications électroniques ; de telles restrictions placeraient les législations nationales relatives aux logiciels espions dans le champ d'application de ladite directive ; le déploiement régulier de technologies d'espionnage intrusives serait incompatible avec l'ordre juridique de l'Union* »[293].

En effet, bien que les termes exacts de « *droit à la protection des équipements terminaux* » ne soient pas directement utilisés par la directive Vie privée, l'article 4, alinéa 1er de cette dernière dispose que « *le fournisseur d'un service de communications électroniques accessible au public prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de communication en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant* ».

Par ailleurs, les États membres ont pour obligation de garantir la confidentialité des communications effectuées au moyen d'un réseau public de communication et de services de communications électroniques accessibles au public. Ils doivent interdire à toute autre personne que les utilisateurs « *d'écouter, d'intercepter, de stocker les communications et données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne est y légalement autorisée, conformément à l'article 15, paragraphe 1* »[294]. Il semble pertinent de préciser que cette obligation n'est pas incompatible avec la mise au clair des données chiffrées, puisqu'il s'agit de protéger les utilisateurs des faits de personnes non autorisées.

La captation de données informatiques selon les termes des articles L.853-2 du CSI et 706-102-1 du CPP, nécessitant l'exploitation de vulnérabilités, est, *a priori*, une limitation des dispositions de la directive. L'ambiguïté réside dans le champ d'application de celle-ci, c'est-à-dire, son opposabilité aux mesures de captation. L'article 1er, paragraphe 3 de la directive, dispose que cette dernière « *ne s'applique pas […] aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal* ». Il s'agit

[293] *Ibid*., §C ; §E ; §F.
[294] Art. 5, directive « Vie Privée ».

d'une clause d'exclusion. Les mesures qui s'inscrivent dans le champ d'application de cet article n'ont pas à répondre aux dispositions de la directive, quelles qu'elles soient.

Parallèlement à cela, l'article 15, paragraphe 1er permet aux États d'adopter des mesures visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la directive, lorsqu'une telle limitation constitue une mesure « *nécessaire, appropriée et proportionnée au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques* ». Il s'agit d'une clause de limitation. Au titre de cet article, les États peuvent limiter la portée de certains articles s'ils poursuivent les objectifs ci-dessus, si les mesures adoptées respectent les dispositions de la directive, et les critères de proportionnalité posés par l'article 15.

La distinction entre les deux clauses, d'exclusion ou de limitation, réside dans l'autonomie des autorités nationales, vis-à-vis des fournisseurs[295]. Si ces dernières imposent des obligations aux fournisseurs, et n'agissent pas de manière entièrement autonome, elles doivent répondre aux obligations de l'article 15 de la directive 2002/58[296]. Dans le cas contraire, les mesures ne peuvent être regardées comme « *mettant en œuvre le droit de l'Union européenne* », et répondent au cas envisagé par l'article 1er de la directive. Cette interprétation a été validée par la décision du Conseil d'État, du 21 avril 2021[297].

L'introduction par le Parlement européen, d'un « *droit à la protection des équipements terminaux* », que la captation de données informatiques restreindrait, ferait rentrer les activités relevant des articles L.853-2 du CSI et 706-102-1 du CPP, sous le joug de la directive. Dans ce cas, la captation ne se ferait pas de manière autonome : elle impliquerait une obligation négative pour les fournisseurs (comme s'abstenir de corriger une vulnérabilité détectée). Puisque l'article 4 de la directive, duquel découle le « *droit à la protection des équipements terminaux* », ne peut faire l'objet de limitations en vertu de l'article 15 du même texte, les mesures de captation seraient effectivement contraires au droit de l'Union européenne.

[295] Ventura (D.), « *L'acquisition de données de communications électroniques par les autorités de renseignement à l'épreuve de la directive "e-privacy" 2002/58/CE* », *RDLF*, 2020, chron. n° 22.
[296] CJUE, gr. ch., 6 octobre 2020, n°C-511/18 et n°C-512/18, §103-104.
[297] CE, Ass., 21 avril 2021, *French Data Network et autres,* n° 393099, §94.

Cette interprétation ne fait pas consensus. De plus, son acceptation pourrait avoir comme effet contradictoire d'inciter les États à agir à l'insu des fournisseurs, ce qui encouragerait le développement d'un marché « secret » d'échange de vulnérabilités non connues, échappant au contrôle de l'Union européenne.

Par ailleurs, la CJUE, dans un arrêt du 4 octobre 2024 en réponse à une question préjudicielle posée par les juridictions autrichiennes, a validé l'inapplicabilité de la directive Vie Privée aux mesures qui concerneraient l'accès par les autorités de police aux données stockées dans un téléphone portable verrouillé[298].

Deux conclusions peuvent être tirées de cet arrêt. Tout d'abord, il est fort probable que la directive Vie Privée ne s'applique pas non plus à la procédure consacrée par l'article 60-3 du CPP sur l'accès au support de données informatiques, puisqu'elle concerne également les téléphones portables.

Ensuite, le raisonnement utilisé par la CJUE permet de supposer légitimement que la directive Vie Privée, en dépit des interprétations du Parlement européen dans ses recommandations, ne serait pas applicable aux opérations de captation de données informatiques.

En effet, la Cour valide l'inapplicabilité de la directive parce que l'accès au support de données informatiques aurait été effectué « *sans qu'une quelconque intervention d'un fournisseur de services de communications électroniques ait été sollicitée* ». Cette opération relève de l'article 1er de la directive[299]. Dès lors que la condition de l'autonomie de l'opération vis-à-vis des fournisseurs est remplie si ces derniers n'ont pas été « sollicités », la captation de données informatiques ne peut être jugée comme s'inscrivant dans le champ d'application de l'article 15. En effet, sa mise en œuvre ne nécessite la sollicitation les fournisseurs, et, même si elle restreignait un « *droit à la protection des équipements terminaux* », cette restriction se ferait sans sollicitations.

Sur la base de ce raisonnement, la directive Vie Privée est également inapplicable aux opérations de mise au clair des données chiffrées.

C'est précisément pour l'autonomie qu'elle confère, que l'exploitation de vulnérabilités informatiques est utile. Dans la mesure où la pérennité de la santé financière des fournisseurs de services de communications électroniques repose sur la protection de la vie privée de leurs utilisateurs, les collaborations avec autorités nationales ne sont pas

[298] CJUE, gr. ch., 4 octobre 2024, n°C-548/21, §59.
[299] *Ibid.*, §58.

souhaitées par ceux-ci. En l'absence d'alternatives, le concourt obligatoire des fournisseurs aurait pour conséquence de lier le succès des opérations au bon vouloir d'acteurs privés, et imposerait le respect des dispositions de la directive. L'exploitation de vulnérabilités permet aux autorités nationales de s'affranchir de ces problématiques.

Cela étant dit, les mesures relatives à la captation de données informatiques, à l'accès au support de données informatiques et à la mise au clair de données chiffrées doivent tout de même respecter la Charte des droits fondamentaux de l'Union européenne, et la directive 2016/680[300], dite Police-Justice.

2.3.2.2 La directive 2016/680 (directive « Police-Justice »)

La directive Police-Justice est un instrument juridique, dont l'objectif est d'établir des règles en matière de « *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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* »[301].

Elle ne s'applique pas aux traitements de données à caractère personnel effectués dans le cadre d'une activité ne relevant pas du champ d'application de l'Union, tels que les domaines visés par l'article 4 du TUE[302]. En vertu de cet article, la directive Police-Justice ne s'applique pas aux activités des services de renseignements, lorsqu'elles se fondent sur une des finalités inscrites à l'article L.811-3 du CSI, regardées comme « *relevant de la sauvegarde de la sécurité nationale* » par le Conseil d'État en 2021[303].

Sur la procédure relative à l'accès au support de données informatiques, la Cour a expliqué que « *lorsque les autorités de police saisissent un téléphone et le manipulent à des fins d'extraction et de consultation des données à caractère personnel contenues dans ce téléphone, elles entament un traitement au sens de l'article 3, point 2, de la directive 2016/680, quand bien même ces autorités ne parviendraient pas, pour des*

[300] Directive « Police-Justice ».
[301] *Ibid*., art. par. 1er.
[302] Art. 4 du traité sur l'Union européenne, « *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 particulière, la sécurité nationale reste de la seule responsabilité de chaque État membre* ».
[303] CE, Ass., 21 avril 2021, *French Data Network et autres,* n° 393099, §67.

raisons techniques, à accéder à ces données »[304]. Ce faisant, l'accès et la tentative d'accès à un support numérique rentrent dans le champ d'application de la directive.

L'applicabilité de la directive peut être élargie à la captation de données informatiques effectuée par les services de police judiciaire, puisqu'il s'agit également d'un traitement.

Enfin, la mise au clair des données chiffrées est une opération visant la « modification » des données aux fins de les rendre intelligibles. La définition de « traitement » couvre les opérations de modifications, ce qui rend la directive applicable à cette procédure.

Il convient de revenir sur les principes de la directive (**a**) et ses interprétations jurisprudentielles (**b**).

a) Les principes de la directive

Selon les dispositions de l'article 4 de la directive, les données doivent être traitées de manière licite et loyale, collectées pour des finalités déterminées, explicites et légitimes, adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées, exactes, et si nécessaire, tenue à jour, effacées ou rectifiées sans tarder si elles se révèlent inexactes, conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités poursuivies, traitées de façon à garantir leur sécurité, y compris la protection contre le traitement non autorité ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Le traitement doit avoir pour finalité « *la prévention et la détection des infractions pénales, l'enquête et la poursuite en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* »[305], et doit être mis en œuvre par un responsable de traitement habiliter à traiter ces données pour de telles finalités, conformément au droit de l'Union ou au droit d'un État membre. Le responsable doit être en mesure de démontrer le respect des dispositions ci-dessus.

Outre l'article 4, d'autres obligations incombent au responsable de traitement et à son sous-traitant. À l'instar du RGPD[306] la directive impose la réalisation d'une analyse d'impact lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits

[304] CJUE, 4 octobre 2024, n°C-548/21, §72.
[305] Art. 1, par. 1, directive Police-Justice.
[306] CNIL, Directive « Police-Justice » : de quoi parle-t-on ?, 20 février 2019.

et libertés de la personne concernée[307], la désignation d'un délégué à la protection des données[308], la tenue d'un registre d'activités de traitement[309], par exemple. D'autres sont spécifiques à la directive, comme la distinction entre les différentes catégories de personnes concernées, telles que les victimes, les suspects, les personnes reconnues coupables ou les tiers à l'infraction. De plus, le traitement de données sensibles[310] n'est autorisé qu'en cas de nécessité absolue, sous réserve de garanties appropriées, pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique, ou lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre, ou lorsqu'il porte sur des données manifestement rendues publiques par la personne concernée[311].

Les personnes concernées disposent d'un droit d'information qui se décline deux classes. La personne concernée doit au minimum pouvoir s'informer sur l'identité et les coordonnées du responsable de traitement ou les coordonnées du délégué à la protection des données, les finalités du traitement auquel sont destinées les données, le droit d'introduire une réclamation auprès d'une autorité de contrôle et ses coordonnés, l'existence du droit de demander l'accès aux données, leur rectification, leur effacement et la limitation du traitement[312].

La seconde classe d'informations regroupe la base juridique du traitement, la durée de conservation ou les critères pour déterminer cette durée, les catégories de destinataires, et au besoin, des informations complémentaires lorsque le traitement se fait à l'insu de la personne concernée[313]. Des mesures législatives peuvent restreindre ou retarder l'accès aux informations de seconde classe, « *dès lors et aussi longtemps (que ces mesures sont) nécessaires et proportionnées dans une société démocratique* », pour éviter de gêner les enquêtes, les recherches ou autres procédures, protéger la sécurité publique, la sécurité nationale et les droits et libertés d'autrui[314].

[307] Art. 27, Directive « Police-Justice ».
[308] *Ibid*., art. 32.
[309] *Ibid*., art. 24.
[310] *Ibid*., art. 10 « *données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, biométriques aux fins d'identifier une personne physique de manière unique, les données de santé ou concernant la vie sexuelle ou l'orientation sexuelle* ».
[311] *Ibid*., art. 10.
[312] *Ibid*., art. 13, par. 1er.
[313] *Ibid*., par. 2.
[314] *Ibid*., par. 3.

Les personnes disposent également d'un droit d'accès aux données, qui peut être limité entièrement ou partiellement selon les mêmes conditions que ci-dessus[315]. Enfin, la directive impose le droit à un recours juridictionnel effectif contre le responsable de traitement ou de ses sous-traitants, par le biais de son article 54.

La portée de la directive a fait l'objet de plusieurs contentieux, et par un arrêt du 4 octobre 2024, la CJUE s'est exprimée sur la question de l'accès à un téléphone portable au cours d'une procédure pénale, alors que ce dernier était protégé par des mécanismes techniques. Ces précisions ne sont pertinentes que dans le cadre de la procédure autorisée à l'article 60-3 du CPP, l'accès physique à un support de données informatiques. Sa portée à la captation de données informatiques est limitée, puisque cette technique relève davantage d'un accès dématérialisé à un STAD, à des fins de surveillance. Dans le cas relaté devant la CJUE, et celui de la procédure à l'article 60-3 du PP, le suspect, déjà appréhendé, a connaissance de l'investigation menée contre lui.

b) Les précisions jurisprudentielles sur l'accès au support de données informatiques

Dans cet arrêt, la CJUE a expliqué qu'une réglementation nationale qui octroie aux autorités compétentes la possibilité d'accéder aux données contenues dans un téléphone portable, à des fins de prévention, de recherche, de détection et de poursuite d'informations pénales en générales, était conforme à la directive 2016/680 et à la CDFUE, sous trois conditions. La réglementation doit définir de manière suffisamment précise la nature ou les catégories des infractions concernées, elle doit garantir le respect du principe de proportionnalité, et soumettre l'exercice de cette possibilité, sauf cas d'urgence dûment justifiée, à un contrôle préalable d'un juge ou d'une entité administrative indépendante.

En effet, puisque cette possibilité d'accès est une limitation des articles 8[316] et 7[317] de la CDFUE, elle doit respecter le contenu du paragraphe 1er de l'article 52 de cette même Charte. Ce dernier dispose que « *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*

[315] *Ibid*., art. 15.
[316] Charte DFUE, art. 8 « *Protection des données à caractère personnel* ».
[317] *Ibid.,* art. 7 « *Respect de la vie privée et familiale* ».

effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

La Cour accorde à l'enquête policière visant la répression d'une infraction pénale, une teneur relevant de l'objectif d'intérêt général[318]. Elle estime que le caractère nécessaire de la limitation aux droits fondamentaux et aux principes consacrés par la directive 2016/680 est une exigence remplie lorsqu'il n'existe pas d'autres moyens, moins attentatoires, pour atteindre l'objectif visé.

Considérant l'ingérence particulièrement grave dans les droits fondamentaux garantis aux articles 7 et 8 de la CDFUE, l'accès aux données du téléphone étant susceptible de permettre des conclusions très précises sur la vie personnelle de la personne concernée et ses proches, ainsi que sur des informations sensibles, telles que l'appartenance religieuse, ethnique ou l'orientation sexuelle, par exemple, la Cour considère la gravité de l'infraction qui fait l'objet d'une enquête comme critère déterminant dans son examen de proportionnalité[319].

Malgré ses constats, la Cour n'a pas restreint l'accès au téléphone portable à la seule lutte contre la criminalité grave. Elle a toutefois posé des conditions de mise en œuvre.

Le téléphone dont l'accès peut être autorisé, doit être celui d'une personne sur laquelle pèse de soupçons raisonnables, qu'elle a commis, commet ou projette de commettre une infraction, ou qu'elle est impliquée dans une telle infraction. La présence de ces soupçons doit être étayée par des éléments objectifs et suffisants.

Le contrôle préalable par une juridiction ou une entité administrative doit intervenir avant toute tentative d'accès, sauf cas d'urgence dûment justifiée. L'autorité délivrant l'autorisation doit être habilitée à refuser ou restreindre cet accès, et doit pouvoir mesurer l'équilibre entre les intérêts légitimes et les droits fondamentaux.

Sur ces deux points, la procédure nationale à l'article 60-3 du CPP semble être en conformité. Ceci est particulièrement intéressant puisque l'indépendance du procureur de la République n'est pas obligatoire tant que celui-ci est habilité à refuser ou restreindre l'accès. Cependant, il ne s'agit que d'une interprétation de la portée de cet arrêt au cas français.

[318] CJUE, gr. ch., 4 octobre 2024, n°C-548/21, §86.
[319] *Ibid.,* §96.

Enfin, il incombe aux autorités nationales compétentes ayant été autorisées à accéder au support de données informatiques, « *d'informer les personnes concernées des motifs sur lesquels cette autorisation repose, dès le moment où cela n'est pas susceptible de compromettre les enquêtes menées par ces autorités. Elles doivent également mettre à disposition l'ensemble des informations ci-dessus visées. Celles-ci sont nécessaires pour permettre aux personnes d'exercer le droit de recours prévus à l'article 54 de la directive* »[320].

Le critère déterminant est la possibilité que l'enquête soit compromise. Cependant, même dans le cas où l'enquête pourra aboutir sans difficulté, ni la directive Police-Justice ni la Cour dans ses interprétations n'imposent que la méthode utilisée pour accéder au support soit divulguée.

En jugeant conventionnel l'accès au support de données informatiques, la Cour valide par la même occasion l'exploitation de vulnérabilités lorsque nécessaire. L'accès peut se faire par tout moyen, tant que sa mise en œuvre répond aux conditions ci-dessus.

Malgré ces éclaircissements, la portée de cet arrêt est limitée vis-à-vis de la procédure nationale de mise au clair de données chiffrées et de captation de données informatiques. La Cour n'a pas pu se prononcer sur l'articulation entre ces procédures et les dispositions de la directive Police-Justice. D'autant plus que, comme expliquée ci-dessus, la procédure de captation de données informatiques est effectuée à l'insu de la personne pendant plusieurs semaines. Il s'agit d'une technique plus intrusive que l'accès au téléphone portable d'un suspect.

2.3.2.3 La directive 2014/41 relative à la décision d'enquête européenne

La CJUE a apporté des précisions procédurales concernant la captation de données informatiques, dont les propriétaires ne se situeraient pas en France, mais sur le territoire d'un autre État membre, lors de l'affaire EncroChat[321].

Ses explications ont été données dans le cadre du renvoi préjudiciel effectué par juridictions allemandes devant la CJUE, sur l'interprétation de la directive 2014/41 relative à la décision d'enquête européenne[322], et la conformité de la transmission de

[320] *Ibid.,* §122.
[321] CJUE, gr. ch., 30 avril 2024, n°C-670/22.
[322] Directive 2014/41, préc.

données collectées par les autorités françaises, aux autorités allemandes. En effet, une procédure pénale avait été engagée contre M.N par les juridictions allemandes, sur la base de données qui avaient été préalablement collectées par les autorités françaises sur « EncroChat »[323], comme preuves de ses activités criminelles.

Bien que l'affaire porte majoritairement sur l'émission et l'exécution des décisions d'enquêtes européennes[324], notamment la transmission des données ou des preuves, et moins sur la méthode de leur collecte, elle apporte tout de même des éclaircissements quant au cadre juridique applicable, lorsque la captation de données informatiques a une portée extraterritoriale.

Dans l'arrêt EncroChat, la Cour a estimé que « *l'infiltration d'appareils terminaux qui vise à extraire des données de communication, mais également de trafic ou de localisation, à partir d'un service de communication fondé sur l'internet constituait une "interception de télécommunications" au sens de l'article 31, paragraphe 1 de la directive 2014/41* »[325]. L'infiltration fait référence à l'utilisation, par les autorités françaises, d'un logiciel de type « cheval de Troie », sur le serveur qui permettait d'établir la communication chiffrée de bout en bout des utilisateurs de téléphones portables cryptés, ces derniers fonctionnant sous la licence EncroChat.

Cette qualification impose aux États membres le respect des dispositions de l'article 31 de ladite directive. Il traite de la notification *« de l'État membre où se trouve la cible de l'interception et dont l'assistance technique n'est pas nécessaire »* qui n'est pas, contrairement à l'acte émis dans le cadre de l'article 30 relatif à l'interception des télécommunications avec l'assistance technique d'un autre État membre, une décision d'enquête européenne. Rentre dans le champ de l'article 31, l'utilisation d'un dispositif technique de captation et de recueil de données, sur un élément numérique susceptible d'être utilisé par différents utilisateurs, indépendamment de leur lieu d'habitat ou de résidence, comme WhatsApp ou Telegram.

[323] EncroChat est une entreprise de service de télécommunications chiffrées néerlandaise.

[324] Art. 1, par. 1, directive 2014/41 « *La décision d'enquête européenne est une décision judiciaire qui a été émise ou validée par une autorité judiciaire d'un État membre (ci-après dénommé "État d'émission") afin de faire exécuter une ou plusieurs mesures d'enquête spécifiques dans un autre État membre (ci-après "l'État d'exécution") en vue d'obtenir des preuves (…) La décision d'enquête européenne peut également être émise pour l'obtention de preuves qui sont déjà en possession des autorités compétentes de l'État d'exécution* ».

[325] CJUE, gr. ch., 30 avril 2024, n°C-670/22, §114.

L'article impose la notification de l'État du territoire sur lequel l'interception est effectuée, par l'État interceptant. Cette notification doit intervenir avant l'interception, dans les cas où l'autorité compétente de l'État interceptant sait au préalable que l'interception s'effectuera en dehors de son territoire national, ou après le début de l'opération, lorsque la connaissance du caractère extraterritorial de l'interception arrive ultérieurement[326]. L'affaire EncroChat éclaire sur la qualité que doit revêtir l'autorité compétente à notifier, estimant qu'il peut s'agir, lorsque l'autorité notifiant n'est pas en mesure d'identifier l'autorité à notifier, de toute autorité jugée apte à cet effet[327].

L'autorité compétente de l'État notifié peut demander l'interruption de l'opération d'interception ou l'utilisation conditionnelle des données captées sur son territoire, dans le cas où l'interception ne serait pas conforme au droit national de l'État notifié[328]. Il s'agit d'un pouvoir et non d'une obligation, l'État notifié disposant d'une faculté d'appréciation.

L'article 31 de la directive vise à protéger à la fois la souveraineté de l'État notifié, mais également le droit au respect de la vie privée et des communications des cibles de l'interception, conformément à l'article 7 de la Charte des droits fondamentaux. Cet article vise aussi à protéger les droits des personnes concernées lorsque les données sont utilisées à des fins de poursuites pénales dans l'État membre notifié[329].

La conformité et le respect des droits fondamentaux sont en effet une préoccupation pour la CJUE, dans la mise en œuvre d'opérations de captation de données informatiques et plus largement, dans l'usage des nouvelles technologies par les services de police judiciaire. Elle apporte aussi une attention particulière au recours de ces technologies sur certaines catégories de personne, dont quelques dispositions du règlement 2022/0722 sur la liberté des médias, en sont la manifestation.

2.3.2.4 Le règlement 2022/0722 (« règlement sur la liberté des médias »)

Les activités journalistiques et les médias bénéficient d'une protection supplémentaire, au titre du règlement sur la liberté des médias[330]. Ce règlement explique que « *compte*

[326] Art. 31, par. 1, directive 2014/41/UE.
[327] CJUE, gr. ch., 30 avril 2024, n°C-670/22, §119.
[328] Art. 31, par. 3, directive 2014/41/UE.
[329] CJUE, gr. ch., 30 avril 2024, n°C-670/22, §124.
[330] Règlement sur la liberté des médias.

tenu du rôle unique que jouent les services de média, la protection de la liberté et du pluralisme des médias en tant que deux des principaux piliers de la démocratie et de l'état de droit constitue une caractéristique essentielle du bon fonctionnement du marché intérieur des services de médias »[331]. Dans un objectif de protection de la confidentialité des sources journalistiques et des communications, le règlement demande aux États membres de veiller à ce qu'aucune mesure de surveillance n'en soit appliquée aux fournisseurs de services de médias, à leur équipe rédactionnelle et à leur entourage. Cette interdiction s'applique au déploiement de logiciels de surveillance intrusifs, y compris lorsque les autorités étatiques ont recours à des parties privées[332], mais aussi à d'autres mesures, telles que l'interception, la perquisition ou la saisie aux fins d'obtenir des informations[333].

Le règlement définit un logiciel de surveillance intrusif comme étant « *tout produit comportant des éléments numériques spécialement conçu pour exploiter les vulnérabilités d'autres produits comportant des éléments numériques, qui permet la surveillance discrète de personnes physiques ou morales par le suivi, l'extraction, la collecte ou l'analyse de données provenant de ces produits ou provenant des personnes physiques ou morales utilisant ses produits, y compris de façon indifférenciée* »[334]. Les dispositifs de captation de données informatiques rentrent dans cette définition, puisqu'ils permettent d'exploiter les vulnérabilités d'autres produits comportant des éléments numériques aux fins de récolter les données des individus visés.

Pour déroger à l'interdiction de déploiement de logiciels intrusifs, une mesure doit respecter les dispositions de l'article 4, paragraphe 5. Elle doit être prévue par le droit de l'Union ou le droit national, être conforme à l'article 52, paragraphe 1er de la Charte des droits fondamentaux de l'Union européenne[335], être justifiée au cas par cas par une raison impérieuse d'intérêt général, être proportionnée et être soumise à l'autorisation d'une autorité judiciaire ou d'une autorité décisionnelle indépendante et impartiale ou,

[331] *Ibid*., §2.
[332] *Ibid*., art. 4 par. 3, al. c).
[333] *Ibid*., al. b).
[334] *Ibid*., art. 2, par. 20.
[335] Art. 52, par. 1er « *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* », Charte DFUE.

dans des cas exceptionnels et urgents dûment justifiés, autorisée ultérieurement par cette autorité sans retard injustifié[336].

Sur la question de la proportionnalité, il convient de s'assurer « *que l'infraction en cause atteint un seuil de gravité, qu'à la suite d'une appréciation individuelle de toutes les circonstances pertinentes d'une affaire donnée, l'enquête et les poursuites relatives à cette infraction justifient, l'ingérence (...) au moyen d'un logiciel de surveillance intrusif, qu'il existe des preuves suffisantes que l'infraction en question a été commise et que le déploiement d'un logiciel de surveillance intrusif est pertinent aux fins de l'établissement des faits liés à l'enquête et aux poursuites relatives à cette infraction* »[337].

Outre ces conditions, le déploiement ne peut être effectué à des fins d'enquête que pour les infractions visées par la décision-cadre 2002/584/JAI[338], article 2, paragraphe 2[339], et qui sont punissables dans l'État membre concerné d'une peine ou d'une mesure de sûreté privative de liberté, d'un maximum de trois ans au moins ou, pour d'autres infractions graves, punissables dans l'État concerné d'un maximum d'au moins cinq ans, conformément à son droit interne. L'utilisation de logiciels de surveillance intrusifs ne doit intervenir qu'en dernier recours, si les autres mesures autorisées par l'article ne sont pas adéquates et suffisantes pour obtenir les informations recherchées[340].

[336] Art. 4, par. 4, cité par art. 4, par. 5, alinéa a), règlement sur la liberté des médias.
[337] *Ibid.,* §26.
[338] Décision-cadre (2002/584/JAI) du Conseil du 13 juin 2022 relative au mandat d'arrêt européen et aux procédures de remise entre États membres, *JOUE* L 190, 18 juillet 2002.
[339] Liste des infractions : participation à une organisation criminelle, terrorisme, traite des êtres humains, exploitation sexuelle des enfants et pédopornographie, trafic illicite de stupéfiants et de substances psychotropes, trafic illicite d'armes, de munition et d'explosifs, corruption, fraude, blanchiment du produit du crime, faux monnayage, cybercriminalité, crime contre l'environnement, trafic illicite d'espèces animales menacées, trafic illicite d'espèces et d'essences végétales menacées, aide à l'entrée et au séjour irrégulier, homicide volontaire, coups et blessures graves, trafic illicite d'organes et de tissus humains, enlèvement, séquestration et prise d'otage, racisme et xénophobie, vols organisés ou avec arme, trafic illicite de biens culturels y compris antiquités et œuvres d'art, escroquerie, racket et extorsion de fonds, contrefaçon et piratage de produits, falsification de documents administratifs et trafic de faux, falsification de moyens de paiement, trafic illicite de substances hormonales et autres facteurs de croissance, trafic illicite de matières nucléaires et radioactives, trafic de véhicules volés, viol, incendie volontaire, crimes relevant de la Cour pénale internationale, détournement d'avion ou de navire, sabotage.
[340] Art. 4, par. 5, sous b), règlement sur la liberté des médias.

Enfin, chaque mesure de surveillance doit être réexaminée régulièrement par une autorité judiciaire ou décisionnelle, indépendante et impartiale, afin de déterminer si les conditions justifiant l'utilisation continuent d'être remplies[341].

Eu égard à ce qui précède, l'exploitation de vulnérabilités informatiques, nécessaire pour le déploiement de surveillance intrusif, n'est pas entièrement proscrite, mais soumise à des conditions renforcées lorsqu'elle concerne certaines catégories de personnes.

S'il n'est pas possible d'affirmer que l'organe responsable de l'autorisation de mise en œuvre doit être une autorité judiciaire ou d'une autorité décisionnelle indépendante et impartiale pour toute opération de captation, les personnes visées par le règlement Liberté des médias pourraient contester le rôle du procureur de la République vis-à-vis des critères posés par le texte.

Il conviendra d'attendre de futurs développements jurisprudentiels sur l'application de ce règlement. Les limites de celui-ci sont cependant palpables, conformément au principe de répartition des compétences entre l'Union et les États membres, il ne s'applique pas au domaine de la sécurité nationale. Les activités de surveillance des services de renseignement, lorsqu'elles sont effectuées en complète autonomie des fournisseurs de service de télécommunication, ne rentrent en théorie pas dans le champ d'application du règlement. Une circonstance sérieusement problématique, puisqu'il est tout à fait possible pour une journaliste d'être surveillée par les services de renseignement. Ce fut le cas de la journaliste Ariane Lavrilleux par la DGSI, pour suspicion de compromission du secret de la défense nationale[342].

[341] *Ibid*., par. 6.

[342] Destal (M.), « Filature, cyberespionnage… La surveillance hors norme subie par Ariane Lavrilleux », , 04 décembre 2024.

Conclusion

L'analyse du droit de l'Union permet de tirer quelques conclusions sur son incidence en matière d'exploitation de vulnérabilités.

Tout d'abord, pour assurer la longévité des normes de l'Union, la CJUE œuvre à rendre applicables les textes les plus anciens, aux nouvelles technologies et usages. Une tâche complexifiée par le type de procédure qui peut être initié devant celle-ci, puisqu'elle est liée par l'objet de la procédure nationale, dans le cas du renvoi préjudiciel, et l'objet du texte contesté, dans le cas du recours en annulation.

Ensuite, il semblerait que la conformité d'une mesure qui limiterait les droits fondamentaux inscrits à la Charte ne soit pas réellement appréciée selon la gravité de l'infraction en cause, l'intensité de l'ingérence et le volume ou le type de données auxquels les autorités auraient accès. L'appréciation semble être axée sur le caractère général ou ciblé de la mesure limitatrice.

En effet, la Cour avait préalablement jugé « *qu'une règlementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte* »[343]. Elle avait également affirmé, concernant les données de trafic et de localisation ou relatives à l'identité civile des utilisateurs de moyens de communications électroniques, qu'il devait exister une gradation selon l'objectif poursuivi, de l'intensité de l'ingérence autorisée dans les droits fondamentaux de la Charte. L'intensité de l'ingérence est déterminée par rapport au type de données, de conservation (généralisée et indifférenciée ou ciblée) et de durée légale autorisée.

Or, dans l'arrêt du 4 octobre 2024 sur la tentative d'accès au téléphone portable dans le cadre d'une enquête pénale, l'accès à l'entièreté des données contenues dans celui-ci, communications, photos, vidéos et autres, n'a pas été un argument propre à contraindre cette opération à la seule criminalité grave. Il n'a pas non plus été apprécié comme portant atteinte au contenu essentiel des droits fondamentaux inscrits dans la CDFUE.

Il apparaît que cette interprétation est liée au fait que l'accès au support numérique, bien qu'en réalité particulièrement intrusif à l'égard de la personne visée, ne puisse être réalisé que de manière ciblée. Le recours à la technique est individualisé, autorisé au

[343] CJUE, gr. ch., 6 octobre 2015, n°C-362/14, §94.

regard des circonstances propres à l'affaire, ce qui implique d'effectuer un contrôle de proportionnalité à chaque fois qu'une demande est déposée.

Quant à la mise au clair de données chiffrées, l'approche de la Cour pourrait être similaire puisque ces opérations sont également autorisées de façon circonstancielle, mais il n'est pas possible, en l'état, de tenir pour vérité cette supposition. Il en va de même pour la captation de données informatiques.

En ce qui concerne les textes plus récents et la jurisprudence qui en découle, ils ont l'avantage d'être plus précis sur les conditions de conformité, pour la mise en œuvre d'une technique de captation de données informatiques. Leur apport est cependant limité, ne traitant que de la question des effets du caractère extraterritorial de la captation, ou des mécanismes à mettre en place pour certaines catégories de personnes.

Ainsi, beaucoup d'interrogations subsistent quant à l'impact du droit de l'Union en matière d'exploitation de vulnérabilités informatiques par les services de police judiciaire et de renseignement.

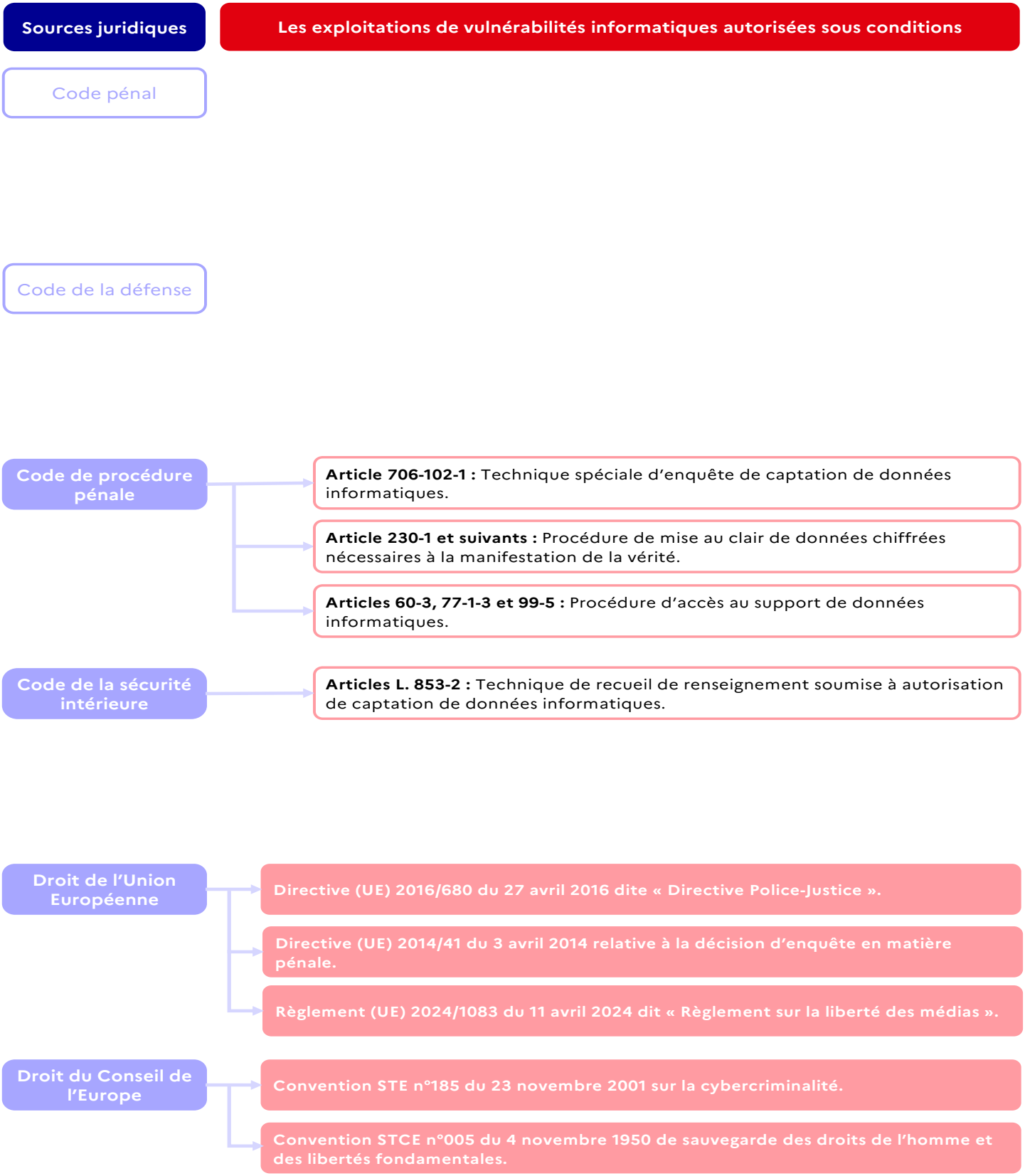

Figure 3. Tableau récapitulatif du cadre juridique des exploitations de vulnérabilités autorisées sous conditions

Conclusion de la Partie 1

Le cadre juridique applicable à l'exploitation de vulnérabilité, lorsque l'exploitation est effective, est relativement abstrait.

En matière d'interdiction, il régit davantage les conséquences de cette exploitation, et non spécifiquement la technique employée. Dans le cadre des atteintes aux STAD ou à la personnalité, par exemple. Sur les autorisations conditionnées, il vise plutôt à définir la procédure et les modalités applicables.

La question de la méthode employée, l'exploitation donc, n'est pas explicitement encadrée.

Le droit européen n'est pas plus clair sur ce point. Outre les recommandations du Parlement européen vis-à-vis de l'utilisation de Pegasus, et autres logiciels espions de surveillance équivalents[344], le fait que les autorités nationales aient recours à l'exploitation de vulnérabilités n'est pas précisément visé ou régulé. L'accent est mis sur les enjeux procéduraux, étayés au regard de ce que les mesures permettent.

En l'absence de telles règles, la responsabilité des personnes qualifiées ou expertes, la qualité de leur prestation et les mesures visant à protéger le droit à la vie privée des personnes concernées ne sont pas appréciables par l'œil externe.

Cela étant, dans le cadre des activités des services de police judiciaire, toutes les mesures susceptibles de recourir à l'exploitation de vulnérabilités informatiques ont une condition procédurale similaire. Elles ne peuvent être mises en œuvre que si les nécessités de l'enquête ou de l'instruction l'exigent. Partant, l'exploitation de vulnérabilités informatiques ne semble pas banalisée.

Ce constat permet de faire le lien avec un autre pan de l'analyse du cadre juridique de l'exploitation de vulnérabilités informatiques, celui du statut des vulnérabilités exploitables, celles qui n'ont pas été encore découvertes. En effet, puisque cette exploitation est unanimement perçue comme particulièrement attentatoire, il est intéressant de voir comment le cadre juridique des vulnérabilités exploitables concilie

[344] Recommandation du Parlement européen du 15 juin 2023 à l'intention du Conseil et de la Commission à la suite de l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (2023/2500(RSP)), *op. cit*.

les besoins des services de police judiciaire et de renseignement, et les risques inhérents à ces besoins pour la sécurité des STAD et des individus.

PARTIE 2 : Le cadre juridique de la vulnérabilité exploitable

Selon le droit de l'Union européenne, la vulnérabilité exploitable est celle « *susceptible d'être utilisée efficacement par un adversaire en conditions de fonctionnement effectives* »[345]. Cette définition souffre quelques limites. Tout d'abord parce que leurs potentielles utilisations ne sont pas restreintes aux seuls adversaires. Comme expliqué dans la Partie 1, les autorités judiciaires, services de renseignement et personnes physiques ou morales sous leur responsabilité, peuvent exploiter des vulnérabilités informatiques dans le cadre de leur mission. Ensuite, parce que le terme « *efficacement* » contraint la vulnérabilité exploitable à être à même de réaliser les objectifs de l'utilisateur. Il pose un seuil de « *qualité supposée de l'utilisation* », en dessous duquel la vulnérabilité, même susceptible d'être utilisée, n'est pas considérée comme exploitable.

Sur la base de ces considérations, la notion de « *vulnérabilité exploitable* » sera entendue comme celle « *susceptible d'être utilisée par une personne physique ou morale, sans le consentement du propriétaire ou du responsable du STAD ou du système d'information sur lequel elle se trouve* ».

Elle est encadrée de façon directe et indirecte, contrairement à la vulnérabilité exploitée qui n'est encadrée que de façon indirecte.

Directement, en matière de sécurité informatique et de la recherche, des atteintes aux STAD et des activités relatives au renseignement ou à la police judiciaire. Indirectement, par la législation portant sur les dispositifs techniques, équipements, instruments ou programmes informatiques destinés à exploiter une vulnérabilité informatique, à l'insu des propriétaires ou des responsables.

Il convient de rappeler que la vulnérabilité exploitable est une source de risques pour les personnes physiques ou morales, et les États. Elle les expose à des cyberattaques, dont les conséquences peuvent se faire ressentir jusque sur l'économie, la démocratie, la sécurité et la santé[346]. En conséquence, la sécurité des systèmes d'information des produits de technologie de l'information et de la communication (produits TIC)[347] a fait l'objet de législations dont le nombre et les obligations associées ne cessent de croître.

[345] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n°168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828, *JOUE* L, 20 novembre 2024 (Règlement sur la cyberrésilience), §41.
[346] *Ibid.*, §1.
[347] Technologie de communications électroniques.

Au niveau de l'Union européenne, ce sont le règlement sur la cyberrésilience de 2024[348], la directive SRI II de 2022[349], le règlement DORA de 2022[350], ou le règlement sur la cybersécurité de 2019[351] pour citer les plus récentes. En droit national, diverses législations[352] traitent de la sécurité des systèmes d'information, dont la promulgation a créé ou modifié plusieurs articles disséminés au sein de différents codes[353]. Il peut s'agir de loi de transposition du droit de l'Union européenne, à l'instar de la loi visant à sécuriser et à réguler l'espace numérique de 2024[354], transposant le règlement sur les marchés numériques de 2022[355] et le règlement sur les services numériques de 2022[356].

L'ensemble des législations relatives à la cybersécurité forme un corpus juridique dense, imposant des obligations graduées selon l'importance du service rendu, la sensibilité du système d'information ou des données qu'il contient, mais également selon le nombre d'utilisateurs qui serait impacté en cas de cyberattaque. Elles ont créé et défini le rôle

[348] *Ibidem*.
[349] 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) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (Directive SRI II).
[350] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n°1060/2009, (UE) n°648/2012, (UE) n°600/2014, (UE) n°909/2014 et (UE) 2016/1011 (Règlement 2022/2554).
[351] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n°526/2013 (Règlement sur la cybersécurité).
[352] Notamment, 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, la loi n°2016-1321 du 7 octobre 2016 pour une République numérique, la 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, la loi n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur, la loi n°2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (liste non exhaustive).
[353] Tels que le code pénal, le code de la défense, le code des postes et des communications électroniques (liste non exhaustive).
[354] Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, *JORF* n°17 du 22 mai 2024.
[355] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur du numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques), *JO* L 265/1 du 12 octobre 2022.
[356] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (Règlement sur les services numériques), *JO* L 227 du 27 octobre 2022.

des autorités de coordination, de chapeautage, comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou la Commission nationale de l'informatique et des libertés à l'échelle nationale (CNIL), ou l'Agence de l'Union européenne pour la cybersécurité (ENISA).

La présente partie n'abordera pas directement le contenu de ce corpus juridique, qui va plus loin que l'analyse requise pour le projet REV. Le statut de la vulnérabilité exploitable en sécurité des systèmes d'information sera étudié sous le prisme de ses interférences avec le cadre juridique de son statut en droit pénal ou en droit du renseignement.

En effet, bien qu'elle soit source de risques, la vulnérabilité exploitable est également un moyen pour les autorités nationales d'accomplir efficacement leurs missions. Elle leur permet de compenser les difficultés émergentes, relatives aux usages faits de la technologie, par les criminels et délinquants. De cette circonstance naissent trois points d'analyse. Celui du cadre juridique des dispositifs techniques fonctionnant sur la base de vulnérabilités exploitables, à savoir, leur création et leur commercialisation ; celui de la correction des vulnérabilités exploitables lorsqu'elles se révèlent utiles pour les autorités nationales dans l'exercice de leur mission, et celui des portes dérobées, vulnérabilités intentionnellement créées à des fins de surveillance ou d'enquête, dont la conformité au droit européen a été récemment discutée[357].

Par ailleurs, il serait complexe de débuter l'analyse de ces trois points sans avoir préalablement explicité le statut de la vulnérabilité exploitable en droit pénal. La compréhension de ce statut est essentielle, puisqu'il s'agit du cadre commun, applicable à tout individu.

Les dispositions jalonnant le cadre commun de la vulnérabilité exploitable sont celles de l'article 323-3-1 du code pénal, relative aux atteintes aux STAD. Sur la base de cet article, des aménagements ont été codifiés pour assurer l'efficacité de certaines missions qui incombent aux autorités nationales (**1**). Enfin, le cadre de la vulnérabilité exploitable qui ne découle pas directement de l'article 323-3-1 du code pénal devra également être exposé (**2**).

[357] CEDH, 13 février 2024, *Podchasov c. Russie,* n°33696/19 ; CJUE, gd. ch., 6 octobre 2015, n°C-362/14 ; Avis conjoint 4/2022 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, 28 juillet 2022 ; Joint statement Europol and ENISA on lawful criminal investigation that respects 21 st Century data protection, 20 mai 2016.

1. Le statut de la vulnérabilité exploitable au titre des atteintes aux STAD

L'article 323-3-1 du code pénal succède aux articles 323-1 à 323-3, dont les tenants et aboutissants ont été analysés dans la première partie. Il n'a pas été créé par la Loi Godfrain[358] contrairement à ces derniers, mais par l'article 46 de la loi pour la confiance dans l'économie numérique de 2004 (dite « LCEN »)[359]. L'objectif était de régir les moyens qui permettaient de commettre une des infractions visées par les articles 323-1 à 323-2 du code pénal.

Tel que modifié par l'article 25 de loi relative à la programmation militaire pour les années 2014 et 2019 et portant diverses dispositions concernant la défense et la sécurité nationale de 2013[360], l'article 323-3-1 dispose désormais que « *le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçu ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 323-1 à 323-3 est puni par des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

L'article consacre une infraction de moyen (**1.1**), dont la caractérisation est complexifiée par la présence des termes « *sans motif légitime, de recherche ou de sécurité informatique* ». Sa portée est modulée dans le cas de la protection de la sécurité nationale (**1.2**).

[358] Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique, *JORF* du 6 janvier 1988.
[359] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, *JORF* n°143 du 22 juin 2004.
[360] 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 (1), *JORF* n°294 du 19 décembre 2013.

1.1 La création d'une infraction de moyen

À l'origine, l'article avait été rédigé dans l'objectif de réprimer les détenteurs ou les fabricants de virus informatiques[361]. Il est cependant applicable aux vulnérabilités informatiques, que les termes « *toute donnée (...) spécialement adapté(e)* » visent directement. Les vulnérabilités exploitables sont bien des données adaptées pour accéder ou se maintenir frauduleusement dans un STAD, entraver son fonctionnement ou introduire et collecter les données qu'il contient.

L'article 323-3-1 du code pénal peut être vu comme consacrant une infraction de « moyen », permettant la réalisation d'une infraction de « fin »[362]. En effet, pour qu'une infraction puisse être caractérisée au titre de l'article 323-3-1, les faits doivent avoir rendu possible ou avoir été susceptibles de permettre la commission d'une des infractions aux articles 323-1 à 323-3 du code pénal, dont les éléments constitutifs seraient réunis. Il faut également une intention coupable, conformément à l'article 121-3 du code pénal[363].

Pour illustrer la manière dont ces critères sont appréciés en droit national, et faciliter leur compréhension, il faut revenir sur l'arrêt du 7 janvier 2020 de la chambre criminelle de la Cour de cassation, dans lequel elle a rejeté le pourvoi formé par l'administration fiscale pour faire condamner deux sociétés, une ayant développé un logiciel de gestion à l'usage des pharmacies, et l'autre ayant assuré sa commercialisation[364]. Elles étaient toutes deux poursuivies au titre de 323-3-1 du code pénal, pour avoir développé et commercialisé un logiciel conçu pour réaliser l'infraction visée par l'article 323-3 du même code, relatif à la suppression frauduleuse des données d'un STAD. En effet, le logiciel permettait, après saisie d'un mot de passe personnel, de faire disparaître des informations liées à des ventes payées en espèce, avant qu'elles ne soient actées d'un point de vue comptable. Cette fonctionnalité facilitait la fraude fiscale.

Selon la Cour de cassation, puisque « *les atteintes aux STAD ne sauraient être reprochées à la personne qui, bénéficiant des droits d'accès et de modification des*

[361] Avis n°608 du 11 février 2003, présenté au nom de la Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de Loi (n°528) pour la confiance dans l'économie numérique.
[362] ROQUES (A.), « Trafic de moyens et atteintes aux STAD : précisions sur les éléments constitutifs », *Dalloz Actualité*, 7 février 2020.
[363] C.cass., ch. crim., 27 octobre 2009, n°09-82.346.
[364] C.cass., ch. crim., 7 janvier 2020, n°18-84.755.

données, procède à la suppression des données, sans les dissimuler à d'éventuels autres utilisateurs du système », la décision des juges de la chambre d'instruction de ne pas condamner les deux sociétés au titre de l'article 323-3-1 était justifiée.

Aux fins de supprimer les données, l'utilisateur devait obligatoirement posséder les privilèges requis pour modifier ces dernières. De plus, cette suppression n'était pas irrémédiable, d'autres utilisateurs pouvaient en prendre connaissance et inverser le processus. La suppression, n'étant pas définitive, a été requalifiée en « modification », celle-ci ne pouvant être frauduleuse puisque l'utilisateur devait bénéficier de certains droits. Ainsi, le logiciel ne permettait pas la commission d'un acte correspondant aux éléments constitutifs de l'infraction prévue par l'article 323-3. Partant, les sociétés n'ont pas commercialisé un « moyen » au sens de l'article 323-3-1.

Déjà complexe, la relation entre l'article 323-3-1 et les articles 323-1 à 323-3 du code pénal devient particulièrement alambiquée lorsque les questions du motif légitime et des vulnérabilités exploitables sont considérées.

Bien que les termes « *sans motif légitime* » aient été présents dès la création de l'article, ceux qui succèdent, « *notamment de recherche ou de sécurité informatique* », ont été rajoutés par la loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale de 2013[365]. La locution « *notamment* » souligne l'idée que la recherche ou la sécurité informatique ne sont pas les seuls motifs potentiellement admissibles. Actuellement, la jurisprudence n'a pas identifié d'autres motifs.

À l'origine, dans la proposition de loi, l'article possédait un deuxième alinéa qui entendait exclure du champ d'application de l'article certains équipements, instruments, programmes ou données, pour les besoins de la recherche scientifique et technique ou la protection de la sécurité des réseaux de communication électronique et des systèmes d'information[366]. Cet alinéa avait été retiré, jugé trop large et imprécis, susceptible de créer un flou juridique sur le type d'organisation, de produit ou de service pouvant se targuer d'une telle exonération.

Il faut préciser qu'avant la modification de la loi, en 2009, la Cour de cassation avait rejeté la présence d'un motif légitime exonératoire pour un individu qui partageait les

[365] 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 (1), *JORF* n°294 du 19 décembre 2013.
[366] Avis n°608 du 11 février 2003, préc.

vulnérabilités non corrigées de programmes informatiques sur son site. L'objectif de dissémination de l'information, de la sensibilisation et de la pédagogie n'a pas permis d'exonérer le prévenu, dès lors que « *du fait de son expertise en la matière, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance* »[367].

Cet arrêt confirme que l'article 323-3-1 s'applique bien aux vulnérabilités informatiques exploitables. Le prévenu a été tenu responsable des hypothétiques infractions qui auraient pu être commises par le biais des informations qu'il partageait. De plus, l'intention coupable est retenue dès qu'il y a eu partage, sans motif légitime et en connaissance de cause, de données propres à réaliser l'infraction consacrée à l'article 323-1 du code pénal. La présence d'une intention coupable est ainsi directement liée à l'expertise du prévenu, sans celle-ci, il n'aurait pu être « *en connaissance de cause* ». Les modifications ultérieures de l'article et l'ajout de motifs exonérant ne changeraient pas l'issue de l'affaire, ils permettent au contraire d'expliciter la portée du motif de la sécurité informatique, qui ne comprend pas la dissémination de l'information, la sensibilisation et la pédagogie.

La solution de cet arrêt a remis au-devant des débats, la place du chercheur non contractuel de vulnérabilités informatiques, qui ne sont pas exempts de poursuites légales en cas de « *remontée sauvage* »[368]. Par « *chercheur* » il faut entendre l'individu exerçant une activité de recherche de vulnérabilités informatiques. Ce terme n'inclut pas le contexte de la recherche académique, les individus agissant dans ce cadre étant nommé « *chercheurs académiques* » dans ce livrable.

Avant d'approfondir ce point, il est nécessaire de revenir sur les fondements du cadre légal des chercheurs contractuels (**1.1.1**), celui des chercheurs non contractuels ayant évolué en 2016 et pouvant éclairer la question du « *motif légitime* » de la recherche ou la sécurité informatique (**1.1.2**).

[367] C.cass., ch. crim., 27 oct. 2009, n°09-82.346.

[368] Remontée d'une vulnérabilité informatique de façon non sollicitée et hors d'un cadre contractuel.

1.1.1 Le statut du chercheur contractuel

Les chercheurs peuvent bénéficier d'une protection légale pour la recherche de vulnérabilités informatiques et pour la possession de données ou d'équipements au sens de l'article 323-3-1, s'ils opèrent dans un cadre contractuel.

Il peut s'agir d'un contrat strictement bilatéral, où le chercheur est engagé par une entreprise pour une mission déterminée. L'intrusion dans le système d'information est alors autorisée, de même que la recherche et l'exploitation de vulnérabilités informatiques. Le contrat doit préciser et définir strictement le périmètre d'intervention autorisé, car la responsabilité du chercheur peut toujours être engagée en cas de faute ou de manquement. Par exemple, en cas d'hébergement de données par une entreprise tierce, les termes doivent expliciter si le périmètre d'intervention inclut le STAD du tiers ou non[369]. Les outils autorisés ou mis à disposition du chercheur sont aussi stipulés par le contrat, ainsi que la rémunération, et la durée de la mission.

Le cadre contractuel peut également prendre la forme d'un programme de bug bounty, une « *chasse à la faille de sécurité* », impliquant une prime. Dans ce cas, plusieurs parties sont associées.

La prime à la faille détectée, autrement appelée « *prime à la faille* » ou « *bug bounty* », est « *une rémunération octroyée par une organisation à un expert informatique indépendant qui découvre une faille de sécurité au sein d'un système informatique utilisé par cette organisation* »[370]. Elle est accordée à l'issue d'une recherche collaborative, axée sur la remontée de failles de sécurité présentes sur le système d'information d'un client demandeur. Le montant de la prime est proportionnel à la sévérité de la faille découverte et au niveau d'impact de cette dernière[371].

Les *bug bounty* sont organisés à travers ces programmes, qui définissent les règles de la collaboration avec les chercheurs : le montant des primes, les outils autorisés, le périmètre d'intervention autorisé, les obligations de confidentialité, les garanties de sécurité ou le régime de responsabilité des parties[372]. Les programmes peuvent être

[369] Ledieu avocat, « *Le droit de pentester l'hébergeur du pentesté en 2023 ?* », 05 janvier 2023, consulté le 21 janvier 2025.
[370] Vocabulaire de la défense (liste des termes, expression et définitions adoptées), JORF n°0299 du 11 décembre 2020.
[371] CyberUniversity, « Bug Bounty : définition et comment participer ? », 12 décembre 2022, consulté le 21 janvier 2025.
[372] Bug Bounty FAQ, Site : CLUSIF, novembre 2023, consulté le 21 janvier 2025.

privés ou publics. Dans le cadre d'un programme privé, les chercheurs sont préalablement sélectionnés, souvent par le biais d'un test technique,[373] et ne sont pas anonymes. Le programme public, lui, s'il n'implique pas nécessairement l'anonymat des participants, est en revanche ouvert à tous.

Le client demandeur fait généralement appel à un intermédiaire, chargé d'organiser le programme. L'intermédiaire, autrement appelé « *plateforme de bug bounty* », peut être un service interne au client ou une entreprise spécialisée dans le domaine. Le contrat est alors tripartite, la plateforme ayant des conditions générales d'utilisation qui devront être acceptées par le client, et les chercheurs.

Les avantages du programme de *bug bounty* sont nombreux. Ils permettent une évaluation continue de la sécurité du système d'information du client, puisqu'ils ne définissent pas nécessairement de limite de temps. Pour les chercheurs, tant qu'ils œuvrent dans le cadre contractuel, ce sont la marge de manœuvre dans les outils utilisables et la minimisation des risques de poursuites légales qui ont popularisé cette pratique.

Cela étant, il n'est pas rare que des individus fassent des remontées sauvages de vulnérabilités informatiques, découvertes de façon spontanée en tant qu'utilisateur, ou par le biais de recherches intentionnelles effectuées hors d'un cadre contractuel. Ils s'exposent à des risques de poursuites au titre des articles 323-1 à 323-3-1 du code pénal. Toutefois, il n'est pas exclu que les « *motifs légitimes* » de l'article 323-3-1 soient susceptibles d'exonérer l'auteur de la remontée sauvage, bien que cette possibilité ne soit pas encore assurée définitivement.

1.1.2 Le statut du chercheur non contractuel

Puisque les termes « *motifs légitimes, notamment de recherche ou de sécurité informatique* » n'ont pas éprouvé le cas de la remontée sauvage, il n'est pas prudent de se prononcer sur la protection qu'ils confèrent au « *trouveur* » non contractuel. Cependant, la prise en considération de l'article L.2321-4 du code de la défense, introduit par l'article 47 de la loi pour une République numérique de 2016[374], permet de supposer la manière dont l'exonération peut fonctionner dans ce cas précis.

[373] *Ibid.*, p. 7 : il s'agit généralement d'un test dénommé « *capture the flag* ».
[374] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique (1) *JORF* n°235 du 8 octobre 2016.

L'article L.2321-4 du code de la défense est rédigé ainsi « *pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale*[375] *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 (ANSSI), une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.* ».

L'alinéa deux poursuit, « *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* ».

Enfin, l'alinéa trois termine, « *l'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information* ».

La portée de cet article est double : il garantit la confidentialité de l'individu faisant la remontée sauvage, et minimise considérablement le risque de poursuites par l'autorité judiciaire pour ses actes, même s'il s'est rendu coupable des faits incriminés aux articles 323-1 à 323-3 du code pénal. Le risque est uniquement minimisé et non absent, l'article ne fait qu'exempter l'ANSSI de l'obligation d'informer sans délai le procureur de la République en cas de crime ou de délit, mais elle conserve cette faculté. L'obligation devient un pouvoir discrétionnaire, que l'ANSSI est susceptible d'utiliser notamment, lorsque les conditions posées par l'article ne sont pas remplies.

Les conditions cumulatives sont les suivantes : l'information transmise doit concerner l'existence d'une vulnérabilité informatique affectant la sécurité d'un STAD, l'information doit avoir été transmise à l'ANSSI uniquement, l'information doit avoir été transmise de bonne foi, et l'exemption de l'obligation à l'article 40 du code de procédure pénale (ci-après, « CPP) doit permettre de répondre à un besoin de sécurité informatique.

De ces conditions découlent plusieurs constats.

[375] Art. 40, al. 2 « *toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes relatifs* », code de procédure pénale (CPP).

L'article ne couvre pas les cas où l'information aurait été mise à disposition du public, ou transmise de manière autonome à l'hébergeur, l'opérateur ou le responsable du STAD. Il pose l'ANSSI comme intermédiaire, mais ne crée pas d'irresponsabilité pénale pour les auteurs de remontées sauvages. L'article ne précise pas le degré de sévérité que la vulnérabilité doit revêtir, pour que « *les besoins de la sécurité des systèmes d'information* » nécessitent son application. Enfin, il ne définit pas la notion de bonne foi.

Cependant, l'applicabilité de l'article et sa mise en œuvre pourrait appuyer une exonération pour « *motifs légitimes (…) de sécurité informatique* » au titre de l'article 323-3-1 du code pénal. Notamment lorsque l'auteur de la remontée sauvage aurait transmis l'information visée par l'article L.2321-4 du code de la défense, aussi bien à l'ANSSI qu'à l'hébergeur, l'opérateur ou le responsable du STAD. En cas de poursuites sur le fondement de l'article 323-3-1 du code pénal, l'auteur de la remontée sauvage pourrait arguer que les conditions de l'article L.2321-4 seraient partiellement remplies, et qu'il agirait bien de bonne foi pour des motifs légitimes de sécurité informatique.

Malgré ces indices, propres à envisager la manière dont s'appliqueraient les motifs légitimes de sécurité informatique, un doute sérieux subsiste quant à l'articulation du motif légitime de la recherche. Il se peut que ces termes visent en réalité à protéger le chercheur académique, œuvrant à faire évoluer les techniques de sécurité informatique, mais leur incidence en cas de poursuites judiciaires n'ayant pas fait l'objet de jurisprudence, les conséquences restent à ce jour abstraites. En effet, particulièrement dans le cas du chercheur académique, il faut se rappeler que l'infraction n'est caractérisable qu'en présence d'un préjudice.

Par ailleurs, dans le cas d'un prototype, présenté par le chercheur académique lors d'un évènement, qui aurait été utilisé à des fins malveillantes, une question se pose quant à la part de responsabilité qui pourrait lui être reprochée. Les suppositions peuvent aller dans le sens d'une complicité par la mise à disposition de moyens, cependant, le chercheur académique pourrait se targuer de bénéficier du motif légitime de la recherche.

Un parallèle pourrait être fait avec l'arrêt du 27 octobre 2009[376], où la Cour de cassation avait estimé que l'individu ne bénéficiait pas de motifs légitimes exonératoires, car « *du fait de son expertise en la matière, il savait qu'il diffusait des informations présentant*

[376] C.cass., ch. crim., 27 oct. 2009, n°09-82.346.

un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance ».

Cela étant dit, les recherches académiques sont nécessaires pour faire évoluer, à la fois, les techniques de recherche de vulnérabilités informatiques, et celles qui permettent leur exploitation. De plus, la formation, les échanges entre pairs et la présentation des avancées académiques sont des composantes indiscutables de la vie du chercheur, sans lesquelles il peut être difficile d'éprouver les outils créés, à l'avis d'autres experts.

Conclusion

La caractérisation d'une infraction au titre de l'article 323-3-1 est difficile à anticiper. Partant, cet article crée une insécurité juridique, qui complexifie la collaboration entre les utilisateurs de STAD (dont font partie les chercheurs non contractuels). La création de l'article L.2324-1 du code de la défense a participé à éclairer le champ d'application de l'article 323-3-1, toutefois, sa portée reste ambiguë et dissuasive.

Combinés, ces articles confèrent une protection partielle et conditionnée aux auteurs de remontée sauvage. Il en va autrement dans le cadre de la sécurité nationale, que les articles 323-8 du code pénal et L.2321-2 du code de la défense régissent.

1.2 Les aménagements relatifs à la sécurité nationale

Aux fins de l'objectif visant la protection de la sécurité nationale, l'article 323-3-1 ne s'applique pas aux agents qui agissent dans le cadre de l'article L.2321-2 du code de la défense (**1.2.1**), et 323-8 du code pénal (**1.2.2**).

1.2.1 L'irresponsabilité pénale des agents chargés de la défense des systèmes d'information : la vulnérabilité exploitable comme moyen défensif

L'article 21 de la loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale de 2013[377] a inséré au sein du code de la défense, l'article L.2321-2, dont l'alinéa 1er dispose que « *pour 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, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque* ». Autrement dit, ce sont les systèmes d'information essentiels, critiques pour l'intégrité de la Nation.

Son alinéa 2 poursuit « *pour être en mesure de répondre aux attaques mentionnées au premier alinéa, les services de l'État déterminés par le Premier ministre peuvent détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs infractions prévues aux articles 323-1 à 323-3 du code pénal, en vue d'analyser leur conception et d'observer leur fonctionnement* ».

Cet alinéa reprend presque à l'identique les termes de l'article 323-3-1 du code pénal pour définir les « moyens » régis. De plus, la loi de 2013 qui a créé l'article L.2321-2 a également modifié l'article 323-3-1 pour ajouter les termes « *notamment, de recherche ou de sécurité informatique* », après ceux relatifs aux motifs légitimes. Une lecture systémique de cette loi et de ces deux articles permet de supposer raisonnablement, que

[377] 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 (1), *JORF* n°294 du 19 décembre 2013.

la « recherche » visée par l'article 323-3-1 du code pénal est celle encadrée au titre de l'article L.2321-2 du code de la défense. L'article L.2321-2 ne consacre pas pour autant pas une irresponsabilité pénale absolue au titre de l'article 323-3-1. En effet, plusieurs jalons cumulatifs délimitent son application.

D'abord, les services peuvent uniquement détenir de tels équipements ou données. Ils ne sont pas autorisés à importer, offrir, céder ou mettre à disposition ceux-ci, sans s'exposer à des poursuites judiciaires sur la base de l'article 323-3-1 du code pénal. Seule la détention qui permet d'être en mesure de répondre à une des attaques informatiques mentionnées au premier alinéa de l'article est autorisée. La détention doit être une valeur ajoutée aux moyens de défense, elle doit répondre à cet impératif précis.

Ensuite, la détention ne peut être autorisée pour d'autres raisons que l'analyse de la conception et l'observation du fonctionnement des équipements ou données. L'article ne proscrit pas la cession et la mise à disposition des résultats de ces analyses à d'autres services. De plus, seuls les agents chargés de la défense des systèmes d'information au sein des services susmentionnés peuvent disposer des équipements et données[378].

Enfin, les services de l'État dont il est question ont été énumérés par arrêté en 2015[379]. Parmi les services relevant du Premier ministre, l'Agence nationale de la sécurité des systèmes d'information ; parmi les services relevant du ministre de la Défense, le service du commandement opérationnel de cyberdéfense de l'état-major des armées, la direction technique de la direction générale de l'armement et la direction technique de la direction générale de la sécurité extérieure ; par les services relevant du ministre de l'Intérieur, le service du haut fonctionnaire de défense et la direction technique de la direction générale de la sécurité intérieure[380].

Finalement, force est de constater que le champ d'application de l'alinéa 2 de l'article L.2321-2 du code de la défense est particulièrement restreint. Il ne concerne que peu de personnes, pour des actions très limitées. Il aborde une logique défensive, en modulant l'applicabilité de l'article 323-3-1 du code pénal, au juste nécessaire pour assurer aux services de l'État des moyens de protection contre les cyberattaques graves.

En effet, en termes de défense, la connaissance technique des procédés utilisés par les attaquants est impérative. Par exemple, l'analyse des différentes utilisations, et des

[378] *Ibid.*, art. 2.
[379] Arrêté du 17 juillet 2015 déterminant les services de l'État mentionnés au second alinéa de l'article L.2321-2 du code de la défense, *JORF* n°173 du 29 juillet 2015.
[380] *Ibid.*, art. 1.

conséquences de celles-ci, qui peuvent être faites des vulnérabilités exploitables, permet de mieux évaluer le degré de sévérité d'une vulnérabilité, et d'appliquer des mesures correctrices adaptées.

En parallèle, la protection de la sécurité nationale passe également par l'utilisation de moyens offensifs lorsque la situation est appropriée. En résultent les aménagements consacrés par l'article 323-8 du code pénal, modulant l'applicabilité de l'article 323-3-1 pour les services de renseignement.

1.2.2 L'irresponsabilité pénale des services de renseignement : la vulnérabilité exploitable comme moyen offensif

L'article 323-8 du code pénal a été introduit au sein du chapitre relatif aux atteintes aux STAD, par la loi relative au renseignement de 2015[381]. Il s'agit de la même loi qui a créé l'article L.853-2 du code de la sécurité intérieure (ci-après, « CSI), sur la captation de données informatiques. L'article crée une « *excuse pénale pour les actions menées sur les systèmes d'information localisés hors du territoire national* »[382].

En effet, selon les dispositions de l'article 323-8 du code pénal, l'article 323-3-1 du même code n'est pas applicable « *aux mesures mises en œuvre, par les agents habilités des services de l'État désignés par arrêté du Premier ministre parmi les services spécialisés de renseignement (…), pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation (…)* ». Pour bénéficier de la protection conférée par cet article, trois conditions cumulatives doivent être remplies.

Tout d'abord, l'agent doit impérativement être missionné par un service spécialisé de renseignement, un service de « premier cercle ». Présentés dans la Partie 1, ces services agissent sous l'autorité du Gouvernement, et leur désignation ne nécessite pas l'avis de la CNCTR, contrairement aux services autres que ceux spécialisés de renseignement, dits de « second cercle ». Le détail des services de premier cercle figure à l'article R811-

[381] Loi n°2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n°171 du 26 juillet 2015.
[382] Étude d'impact du projet de loi relatif au renseignement du 18 mars 2015.

1 du CSI[383], créé par le décret n°2015-1185[384], tel que modifié successivement par l'article 2 du décret n°2016-1337[385] et par l'article 2 du décret n°2017-1095[386].

Ensuite, les mesures mises en œuvre par l'agent doivent strictement viser la protection des intérêts fondamentaux de la Nation, qui sont les sept finalités inscrites à l'article L.811-3. Il s'agit de l'indépendance nationale, l'intégrité du territoire et la défense nationale (1°) ; 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 (2°) ; les intérêts économiques, industriels et scientifiques majeurs de la France (3°) ; la prévention du terrorisme (4°) ; la prévention (5°) : des atteintes à la forme républicaine des institutions a), des actions tendant au maintien ou à la reconstruction des groupements dissous en application de l'article L.212-1 b), des violences collectives de nature à porter gravement atteinte à la paix publique c) ; la prévention de la criminalité et de la délinquance organisées (6°) ; la prévention de la prolifération des armes de destruction massive (7°).

Enfin, les mesures doivent avoir pour objet la protection de ces intérêts fondamentaux, hors du territoire national. Les agents peuvent posséder, obtenir, céder une vulnérabilité exploitable, une donnée conçue pour réaliser une des infractions visées par les articles 323-1 à 323-3 du code pénal, uniquement si elle est pertinente pour mener des actions sur un système d'information localisé en dehors de la France, lorsque leur cible « *porte sur des risques provenant de l'étranger* »[387].

L'articulation de cette excuse pénale avec la captation de données informatiques est intéressante, dans la mesure où la mise en œuvre de cette technique est autorisée sur le

[383] Ce sont la direction générale de la sécurité intérieure (DGSE), la direction du renseignement et de la sécurité de la défense (DRSD), la direction du renseignement militaire (DRM), la direction générale de la sécurité intérieure (DGSI), le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) et le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers » (TRACFIN).

[384] Décret n°2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, *JORF* n°225 du 29 septembre 2015.

[385] Décret n°2016-1337 du 7 octobre 2016 portant changement d'appellation de la direction de la protection et de la sécurité de la défense, *JORF* n°236 du 9 octobre 2016.

[386] Décret n°2017-1095 du 14 juin 2017 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme, *JORF* n°139 du 15 juillet 2017.

[387] Répertoire de droit international, Atteintes aux intérêts fondamentaux de la Nation, Christelle Ravigneaux – Février 2019.

territoire national, qu'elle fonctionne sur la base de l'exploitation de vulnérabilités informatiques et qu'elle vise l'accès et le maintien sur un STAD.

Concrètement, les actes visés par l'excuse pénale vont au-delà de la simple captation, elle englobe plus largement les cyberattaques, aux fins d'entraver ou de fausser le fonctionnement de systèmes d'information. Cela veut dire que les agents peuvent détenir une variété de typologie de vulnérabilités exploitables. Leur utilité n'est pas circonscrite à l'accès ou de maintien dans un STAD.

Conclusion

Il ressort de cette analyse que l'article 323-8, bien qu'ayant un objectif similaire à l'article L.2321-4, la protection de la Nation, dispose d'un champ d'application bien plus large que celui-ci. Les raisons qui expliquent cette circonstance sont variées. La vulnérabilité exploitable dans le cadre de la défense des intérêts fondamentaux de la Nation, n'a pas la même teneur que celle dans le cadre offensif. En défense, elle est objet d'étude, d'analyse, afin de fortifier les capacités de résilience et de résistance. En offensif, elle est un avantage tactique, afin d'assurer la réussite de la mission.

Par ailleurs, l'article L.2321-2 a été créé dans le même temps que la modification de l'article 323-3-1, qui visait à préciser ses motifs légitimes. L'article L.2321-2 a donc été rédigé dans une certaine mesure, pour expliciter ce que le motif légitime de la recherche impliquait. Or, en théorie, la recherche ne nécessite pas de mise à disposition ou de cession des vulnérabilités exploitables. Elle a pour unique objectif la compréhension, l'analyse et la connaissance du mode de fonctionnement.

L'article 323-8 du code pénal, quant à lui, a été créé en même temps que l'article L.853-2 du CSI et que les autres techniques de renseignement soumises à autorisation. Il s'inscrit dans un mouvement qui avait pour objectif d'élargir la marge de manœuvre des services de renseignement.

Ces différences d'intentions se reflètent sur le libellé des articles, et sur leur champ d'application.

Enfin, les aménagements créés par ces articles ne concernent pas les services judiciaires, ce qui interroge puisque ceux-ci utilisent également des vulnérabilités exploitables dans le cadre de leurs missions. La locution « notamment », qui succède à la question des motifs légitimes de l'article 323-3-1 du code pénal, demeure la seule mention à même d'exclure les services judiciaires du champ d'application de cet article.

Il apparaît évident que la vulnérabilité exploitable a un statut protéiforme. Source de risques, moyen offensif extraterritorial et objet d'étude, elle est également un outil de surveillance.

Le droit qui la régit diffère selon ce statut. En tant qu'outil de surveillance, les règles applicables ne relèvent pas que du cadre des atteintes aux STAD. Ces règles concernent à la fois les activités des services de police judiciaire et de renseignement.

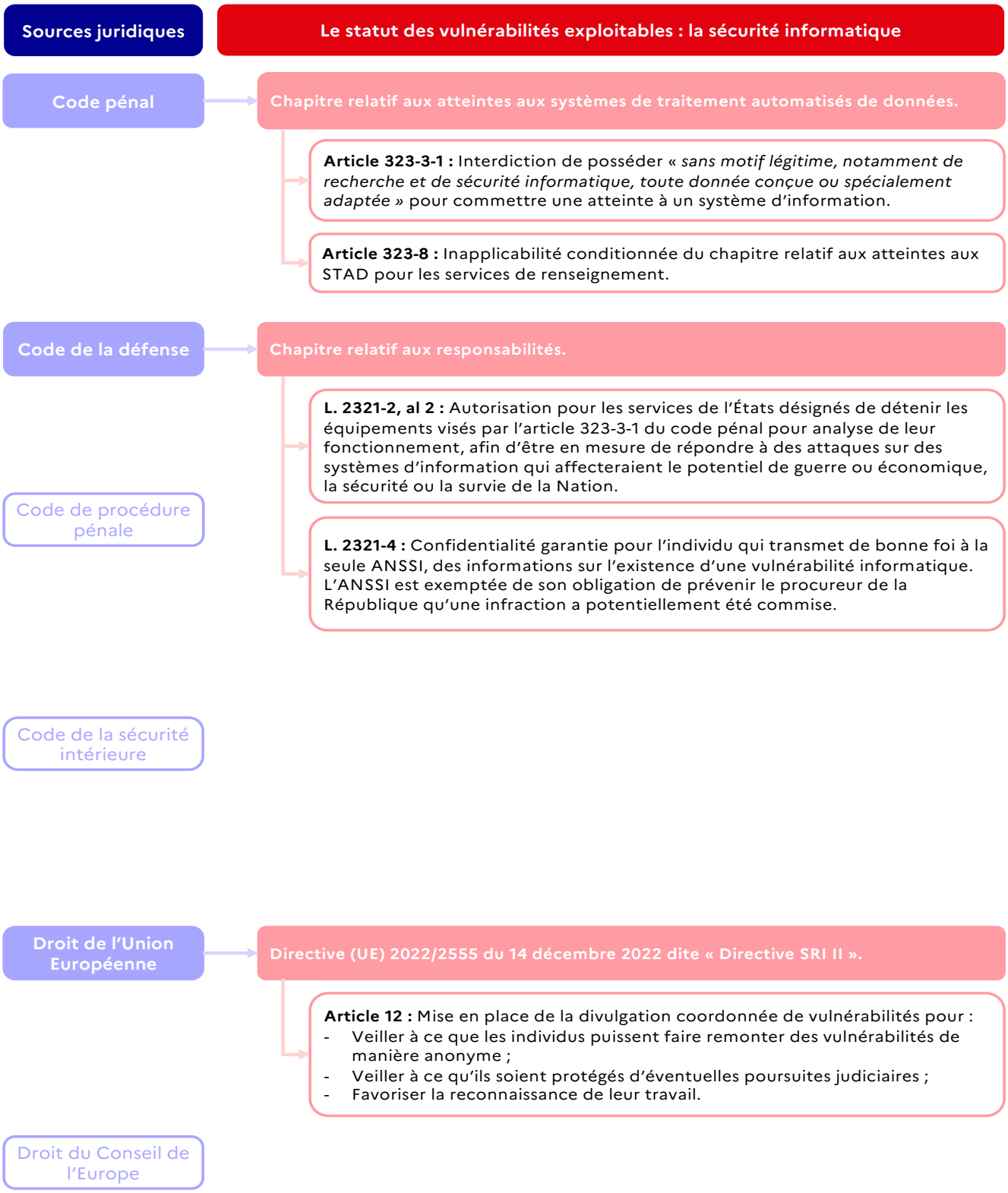

Figure 4. Tableau récapitulatif du cadre juridique des vulnérabilités exploitables dans le cadre de la sécurité informatique.

2. Les autres règles régissant le statut des vulnérabilités exploitables

La question du statut des vulnérabilités exploitables par les services de police judiciaire et de renseignement, hors du cadre des atteintes aux STAD, se décline en deux points d'analyse.

Le premier point, relatif aux dispositifs techniques de captation de données informatiques, traite du cadre juridique qui régule les outils fonctionnant sur la base de vulnérabilités exploitables. Autrement dit, ceux qui permettent aux vulnérabilités exploitables d'être activement exploitées. Leur fabrication et leur acquisition sont régies par le droit national, conformément aux articles 226-3 et R226-1 à R226-12 du code pénal. Leur régime d'exportation, en revanche, relève du règlement européen de 2021 sur les biens à double usage de l'Union européenne[388].

Le deuxième point concerne le cas des vulnérabilités exploitables inconnues du public, utiles pour les missions des services de police judiciaire et de renseignement. Il traite des règles qui entourent la correction de ces vulnérabilités, mais aussi de celles qui régissent la création intentionnelle : les portées dérobées. L'essentiel de ce cadre provient de l'ordre européen, l'Union européenne et le Conseil de l'Europe.

Il conviendra d'analyser la régulation applicable aux dispositifs techniques (**2.1**), puis celle applicable aux vulnérabilités inconnues du public (**2.2**).

2.1 Le cadre applicable aux dispositifs techniques de captation de données informatiques

Pour rappel, les dispositifs techniques de captation de données informatiques sont les outils utilisés par les services de police judiciaire au titre de l'article 706-102-1 du CPP, et par les services de renseignement au titre de l'article L.853-2 du CSI. Ils permettent à ces deux services, « *de prendre connaissance du contenu d'un texte avant qu'il ne soit chiffré (crypté) ; de textes tapés sur un ordinateur puis transportés grâce à un*

[388] 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 (refonte) (Règlement Double Usage).

périphérique (clé USB, CD rom, disque externe) sur un autre ordinateur, des messages échangés entre deux interlocuteurs sur des forums ou « tchats ». […] De tels dispositifs sont des logiciels espions »[389].

Leurs développement, acquisition et commercialisation sont soumis à des règles bien précises, que les fabricants, acquéreurs ou exportateurs (lorsque la commercialisation est internationale) doivent respecter sous peine de sanctions. Comme expliqué précédemment, le cadre juridique provient de règles nationales, inscrites à l'article 226-3 et R226-1 à R226-12 du code pénal (**2.1.1**), et européennes avec le règlement sur les biens à double-usage (**2.1.2**).

2.1.1 La règlementation nationale relative à la fabrication et à l'acquisition de dispositifs techniques

L'article 226-3 du code pénal punit de cinq ans d'emprisonnement et de 300 000 euros d'amende, « *la fabrication, l'importation, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opération (…) ayant pour objet la captation des données informatiques prévues par les articles 706-102-1 du CPP, et L.853-2 du CSI, et qui figurent sur une liste dressée dans des conditions fixées par décret en Conseil d'État, lorsque leur développement et leur commerce sont effectués sans autorisation ministérielle ou sans respecter les conditions fixées par cette autorisation* ». L'infraction est caractérisée même en cas de négligence. Est également sanctionné la publicité de ces outils, en cas d'incitation d'en faire un usage frauduleux.

Dans sa rédaction originale, l'article ne mentionnait pas les « *opérations ayant pour objet la captation des données informatiques* ». L'article 36 de loi d'orientation et de programmation pour la performance de la sécurité intérieure de 2011[390] a modifié l'article 226-3 du code pénal pour englober les opérations des services de police judiciaires, la captation de données informatiques selon la procédure de l'article 706-102-1 du CPP. Ultérieurement, la loi relative au renseignement de 2015[391] a modifié

[389] Étude d'impact, Projet de loi de programmation 2018-2022 et de réforme pour la justice, 19 avril 2018, p. 220.
[390] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (1), *JORF* n°62 du 15 mars 2011.
[391] Loi n°2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n°171 du 26 juillet 2015.

l'article 226-3, pour viser cette fois-ci les activités de services de renseignement : la captation de données informatiques selon l'article L.853-2 du CSI.

La liste des outils visés par l'article 226-3 est établie par arrêté du Premier ministre[392]. Il s'agit de 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 sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un tel système, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels, opération ayant pour objet la captation de données informatiques (…)* »[393].

En théorie, l'article ne concerne pas les dispositifs techniques qui n'auraient pas été spécifiquement conçus pour la captation. Ce peut être des outils dont l'usage aurait été détourné à cette fin.

Les procédures d'autorisation pour le développement et pour l'acquisition de tels dispositifs sont régies par les articles R226-1 à R226-12 de la partie règlementaire du code pénal.

Elles nécessitent toutes deux le dépôt d'une demande auprès du directeur général de l'ANSSI et sont instruites par le bureau des contrôles règlementaires de cette dernière[394]. Ces demandes font l'objet d'un examen par une commission consultative pour avis, qui peut entendre toute personne compétente à titre d'expert[395]. La commission est composée du directeur général de l'ANSSI (ou son représentant, président), d'un représentant du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, d'un représentant du ministre chargé des douanes, du ministre chargé de l'Industrie, du ministre chargé des Télécommunications, d'un représentant de la CNCTR, d'un représentant du directeur général de l'Agence nationale des fréquences, et de deux personnalités choisies en raison de leur compétence désignées par le Premier ministre[396].

[392] Art. R226-1 CP.
[393] Annexe I et II de l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal, *JORF* n°177 du 1er août 2012, modifié par arrêté du 17 juillet 2015 ; arrêté du 15 décembre 2015 ; arrêté du 11 août 2016.
[394] Art. R226-4 (fabricants) et R226-8 (exploitants) CP.
[395] *Ibid*., art. R226-2, al. 2.
[396] *Ibid*., al. 1.

En ce qui concerne le reste de la procédure, il est nécessaire de traiter séparément celle requise pour la fabrication, l'importation, l'exposition, l'offre, la location ou la vente prévue à l'article R226-3, qui concerne les fabricants (équipementiers), de celle requise pour l'acquisition ou la détention, prévue à l'article R226-7 qui concerne les exploitants (opérateurs).

La demande d'autorisation du fabricant doit contenir les informations suivantes[397] :

- Si le demandeur est une personne physique : son nom et son adresse, si le demandeur est une personne morale : sa dénomination et son siège ;
- Le type d'opération pour lequel l'autorisation est demandée (fabrication ; importation ; exposition, etc.) et la description des marchés visés ;
- L'objet et les caractéristiques techniques du dispositif technique, accompagnés d'une documentation technique ;
- Le lieu prévu pour la fabrication du dispositif technique ou pour les autres opérations
- L'engagement de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation.

L'autorisation est délivrée pour une durée maximale de six ans. Elle peut fixer des conditions de réalisation de l'opération ou limiter le nombre de dispositifs techniques concernés[398]. Elle est accordée de plein droit aux services de l'État désignés par arrêté du Premier ministre, pour la fabrication de ces dispositifs. Chaque dispositif technique fabriqué, importé, exposé, offert, loué ou vendu doit porter la référence du type correspondant à la demande d'autorisation et un numéro d'identification individuel[399].

La demande d'autorisation d'acquisition ou de détention doit quant à elle relater les informations suivantes[400] :

- Si le demandeur est une personne physique : son nom et son adresse, si le demandeur est une personne morale : sa dénomination et son siège ;
- Le type de dispositif technique et le nombre pour la détention desquels l'autorisation est demandée ;
- L'utilisation prévue ;

[397] *Ibid*., art. R226-4.
[398] *Ibid*., art. R226-5.
[399] *Ibid*., art. R226-6.
[400] *Ibid*., art. R226-8.

- L'engagement de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation.

La durée d'autorisation est plus courte que pour celle des équipementiers, réduite à trois ans maximums. Des conditions d'utilisation peuvent également s'imposer afin d'éviter tout usage abusif[401]. L'autorisation est délivrée de plein droit aux agents ou services de l'État pour l'acquisition et la détention de dispositifs techniques qu'ils sont autorisés à utiliser en application de la loi. Cette délivrance de plein droit ne concerne que les services de renseignement. Les services de police judiciaire doivent soumettre une demande selon les dispositions de l'article R226-8 du code pénal[402].

Outre les modalités procédurales, les équipementiers titulaires d'une autorisation ne peuvent faire de transactions qu'avec les opérateurs possédant une autorisation d'acquisition. Ils ont pour obligation de tenir un registre de traçabilité sur l'ensemble des opérations relatives aux dispositifs fabriqués. La forme du registre est déterminée par arrêté du Premier ministre, après avis de la Commission consultative[403].

Les autorisations octroyées ne sont pas absolues. Des circonstances spécifiques peuvent entraîner leur retrait, au terme d'une procédure où, sauf cas d'urgence, le titulaire aura pu faire valoir ses observations. Ce retrait peut découler d'une fausse déclaration ou du faux renseignement, de la modification des circonstances au vu desquelles l'autorisation a été délivrée, du non-respect des dispositions règlementaires encadrant l'autorisation, du non-respect des obligations prescrites par l'autorisation, de la cessation de l'activité pour laquelle a été délivrée l'autorisation[404].

Dans ce cas, les personnes disposent d'un mois pour détruire, vendre ou céder à une personne titulaire d'une autorisation, les dispositifs techniques développés. Cette échéance vaut également en cas de non-délivrance ou d'expiration de l'autorisation. Les autorisations peuvent aussi prendre fin de plein droit, en cas de condamnation du titulaire pour l'infraction prévue par l'article 226-3 du code pénal.

Outre ces modalités procédurales, l'exportation de ces dispositifs techniques doit être conforme au droit de l'Union européenne, dans la mesure où ils peuvent être qualifiés de « *biens de cybersurveillance* » au sens du règlement 2021/821.

[401] *Ibid*., art. R226-9.
[402] Question écrite n°11810 de M. Philippe Juvin, « *conditions d'exercice des experts judiciaires en investigation numérique* », 26 mars 2024, p. 2442.
[403] Art. R226-10 CP.
[404] *Ibid*., art. R226-11.

2.1.2 La règlementation européenne applicable aux dispositifs techniques en tant que biens de cybersurveillance

En tant que membre de l'Union européenne, la France est tenue de respecter les dispositions du règlement « double usage » dans sa refonte en 2021[405]. Ce règlement s'applique parallèlement au régime général de l'Union relatif aux exportations vers les pays tiers.

En effet l'Union européenne, compétente en matière de politique commerciale commune entre les États membres[406], a adopté le règlement (UE) 2015/479[407], dont le principe fondamental est la libre exportation vers les pays tiers sans restriction quantitative de tous les produits, autant industriels qu'agricoles[408]. Il ne concerne pas les biens de services. Le règlement autorise aussi l'adoption de mesures de sauvegardes selon certains cas spécifiques, comme la pénurie de produits essentiels ou la menace des intérêts de l'Union[409], mais aussi l'adoption de restrictions quantitatives, pour des raisons de moralité publique, d'ordre public ou de sécurité publique[410].

Ce texte est complété par le règlement 2021/821, afin de minimiser le risque que certains biens « sensibles », bénéficient du principe de libre exportation.

Le règlement (UE) 2021/821, dit « *règlement double usage* » instaure un régime de contrôle des exportations, de courtage, du transit et des transferts[411], pour les « *produits, y compris les logiciels et les technologies, susceptibles d'avoir une utilisation tant civile que militaire* »[412]. Sont ainsi visés les biens de cybersurveillance énumérés à l'annexe I du règlement, conformément à l'article 3, ainsi que les biens de cybersurveillance non énumérés à l'annexe I, si ces produits « *sont ou peuvent être destinés, entièrement ou en partie, à une utilisation impliquant la répression interne et/ou la commission de*

[405] Règlement Double Usage.
[406] Art. 207, par. 2 « *Le Parlement européen et le Conseil, statuant par voie de règlements et conformément à la procédure législative ordinaire, adoptent les mesures définissant le cadre dans lequel est mise en œuvre la politique commerciale commune* », Traité sur le fonctionnement de l'Union européenne (TFUE) (version consolidée) du 25 mars 1957, *JOUE* 7 juin 2016.
[407] Règlement (UE) 2015/479 du Parlement européen et du Conseil du 11 mars 2015, relative au régime commun aux exportations (Règlement 2015/479)
[408] *Ibid*., art. 1.
[409] *Ibid*., art. 5.
[410] *Ibid*., art. 10.
[411] Art. 1er, règlement Double Usage.
[412] *Ibid*., art. 2, par. 1.

violations graves et systématiques des droits de l'homme et du droit humanitaire international »[413].

Les dispositifs techniques utilisés par les services de police judiciaire et de renseignement sont qualifiables de biens de cybersurveillance : des biens « *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* »[414]. Contrairement au droit national, les outils qui n'auraient pas été spécifiquement conçus pour cet objectif, mais dont l'usage pourrait être détourné, sont susceptibles d'être également visés par le règlement.

Cette appréhension extensive du bien de cybersurveillance résulte de l'objectif du règlement, qui est de « *lutter contre le risque que certains biens de cybersurveillance puissent être utilisés abusivement par des personnes complices ou responsables de violations des droits de l'homme* »[415]. Cette notion de risque permet au règlement de s'affranchir d'une définition trop stricte du bien de cybersurveillance, garantissant ainsi son efficacité.

Elle permet également de lutter contre une obsolescence prématurée de ce texte, eu égard les avancées technologiques, dont le rythme est particulièrement soutenu. À cet effet, la Commission dispose d'un pouvoir de modification de l'annexe I, et peut soumettre à autorisation d'autres biens non énumérés dans cette annexe, par le biais des articles 3 et 5 du règlement. Ainsi, si actuellement « *les biens utilisés à des fins purement commerciales, comme la facturation, la commercialisation, les services de qualité, la satisfaction des utilisateurs ou la sécurité des réseaux, sont généralement considérés comme n'entraînant pas de tels risques* »[416], il n'est pas exclu qu'un bien développé à des fins purement commerciales puisse être, dans le futur, considéré comme posant un risque.

Pour l'heure, il convient de traiter les biens figurants à l'annexe I (**2.1.2.1**), ceux n'y figurant pas (**2.1.2.2**), et le régime des autorisations pour leur exportation (**2.1.2.3**).

[413] *Ibid*., art. 5, par. 1.
[414] *Ibid*., art. 2, par. 20.
[415] *Ibid*., §8.
[416] *Ibidem*.

2.1.2.1 Les biens énumérés à l'annexe I du règlement

Les biens directement visés par le règlement sont décrits à l'annexe I, aux catégories 4 et 5. Dans la catégorie 4, il s'agit du numéro 4A005 « *systèmes, équipements et composants spécialement conçus ou modifiés pour la génération, la commande et le contrôle ou la livraison de logiciel d'intrusion* ».

Les logiciels d'intrusion sont des logiciels spécialement conçus ou modifiés pour éviter leur détection par un « *outil de surveillance* »[417], ou pour tromper les « *contre-mesures de protection* »[418] d'un ordinateur, aux fins d'effectuer les tâches suivantes : l'extraction de données ou d'informations à partir d'un ordinateur ou d'un dispositif réseau ; la modification des données système ou utilisateurs ; la modification du chemin d'exécution standard d'un programme ou d'un processus afin de permettre l'exécution d'instructions provenant de l'extérieur.

Ne sont pas inclus dans la catégorie de logiciel d'intrusion, les programmes de débogage, les programmes informatiques assistants les développeurs dans la recherche des erreurs logiciels[419] et se concentrant spécifiquement sur la résolution des erreurs de codage, susceptibles de créer des vulnérabilités informatiques ; les outils de rétro-ingénierie des logiciels, utilisés pour la compréhension d'un système informatique en l'absence de ses spécifications originales, ou permettant en sécurité informatique de connaître les vulnérabilités d'un système, ou de comprendre le fonctionnement de logiciels malicieux ; les logiciels de gestion des droits numériques ; les logiciels conçus pour être installés par les fabricants, les administrateurs ou les utilisateurs, à des fins de suivi ou de récupération des actifs.

Dans la partie 2 « *sécurité de l'information* » de la catégorie 5, au numéro 5A004 « *systèmes, équipements et composants destinés à mettre en échec, à affaiblir ou à contourner la sécurité de l'information* », deux types de biens sont visés.

Tout d'abord, ceux conçus ou modifiés pour effectuer des fonctions cryptoanalytiques. Il s'agit de fonctions conçues pour mettre en échec les mécanismes cryptographiques,

[417] Logiciel ou matériel informatique qui surveille les comportements ou les processus d'un système fonctionnant sur un dispositif. Ces outils incluent les produits antivirus (AV), les produits de sécurité d'accès, les produits de sécurité personnelle, les systèmes de détection d'intrusion ou pare-feu.

[418] Techniques conçues pour garantir l'exécution de codes en toute sécurité telles que la prévention de l'exécution des données, la distribution aléatoire de l'espace d'adressage ou le sandboxing.

[419] Ionos, « *Débogueurs : des outils essentiels pour la recherche des erreurs dans un logiciel* », 13 octobre 2020, consulté le 28 janvier 2025.

afin d'obtenir des variables confidentielles ou des données sensibles, y compris du texte en clair, des mots de passe ou des clés cryptographiques. Sont inclus les systèmes ou équipements effectuant ces fonctions par rétro-ingénierie.

Ensuite, ceux conçus pour accomplir à la fois l'extraction des données brutes d'un appareil informatique ou d'un appareil de communication et le contournement de l'authentification ou des contrôles d'autorisation de l'appareil, afin d'extraire les données. L'extraction des données brutes signifie récupérer des données binaires d'un support de stockage contenu dans l'appareil sans interprétation par le système d'exploitation ou le système de fichier de l'appareil.

Toutefois, ce deuxième type de bien ne concerne pas les systèmes ou équipements de contrôle, spécialement conçus pour le développement ou la production d'un appareil informatique/de communication, les programmes de débogage, les hyperviseurs, les biens limités à l'extraction de données logiques, les biens servant à l'extraction de données qui utilisent la méthode du chip off ou le JTAG (ou) les biens spécialement conçus et limités au jailbreaking ou au routage.

La catégorie 5 semble englober les outils utilisés dans le cadre des procédures inscrites aux articles 60-3 et 230-1 à 230-5 du CPP, concernant respectivement l'accès au support de données informatiques et la mise au clair de données chiffrées. Partant, l'exportation de ces outils pourrait être régulée en tant que « biens de cybersurveillance ».

La liste des biens de l'annexe I peut être modifiée par la Commission selon la procédure détaillée par les articles 17 et 18 du règlement. Dans l'attente de modifications ou lorsque cette modification n'est pas envisagée, certains biens peuvent également être régulés en présence de circonstances précises.

2.1.2.2 Les biens non énumérés par l'annexe I du règlement

L'article 3, paragraphe 2 du règlement, dispose que « *conformément aux articles 4, 5, 9 ou 10, l'exportation vers toutes ou certaines destinations de certains biens à double usage non énumérés à l'annexe I peut également être soumise à autorisation* ». Les modalités de cette possibilité sont étayées aux articles 5 et 9.

Au titre de l'article 5, trois circonstances peuvent justifier que l'exportation d'un bien non énuméré à l'annexe I puisse être soumise à autorisation :

- Lorsque l'autorité compétente a informé l'exportateur que les biens en question sont ou peuvent être destinés, entièrement ou en partie, à une utilisation

impliquant la répression interne et/ou la commission de violations graves et systématiques des droits de l'homme et du droit humanitaire international[420] ;

- Lorsque l'exportateur a connaissance que les biens qu'il entend exporter sont destinés à une utilisation abusive et, qu'en ayant informé l'autorité compétente, celle-ci déciderait de soumettre à autorisation l'exportation[421] ;
- Lorsque les États membres décident d'adopter ou de maintenir des législations nationales soumettant à autorisation l'exportation de biens de cybersurveillance non énumérés à l'annexe du règlement[422].

Ces circonstances n'imposent pas automatiquement à l'État concerné d'avertir ses autorités douanières ou autres autorités nationales compétentes, la Commission européenne et les autres États membres. En raison de la nature de la transaction ou du caractère sensible des informations en question, il peut se soustraire à la notification.

Dans le cas où tous les États membres décideraient et informeraient la Commission qu'une autorisation devrait être imposée sur un ou plusieurs biens, cette dernière publie dans le journal officiel de l'Union européenne les informations pertinentes. Enfin, la soumission d'un bien à une autorisation sur la base de l'article 5 ne crée pas l'obligation, pour les autres États, de requérir eux-mêmes une autorisation d'exportation.

Selon le libellé de l'article 9 du règlement, les États peuvent également interdire ou soumettre à l'autorisation l'exportation d'un bien non énuméré à l'annexe I pour des raisons de sécurité publique, de prévention d'actes terroristes, ou de sauvegarde des droits de l'homme[423]. Ils peuvent prendre des mesures, telles que l'établissement d'une liste de contrôle nationale[424].

Lorsqu'un État impose une autorisation sur le fondement de l'article 9 du règlement et s'il se base sur une liste nationale de contrôle préalablement publiée par la Commission européenne, les autres États sont tenus d'imposer une autorisation d'exportation[425]. En cas de refus, la Commission européenne et les autres États membres doivent impérativement être prévenus. En application de cette procédure, tous les États

[420] Art. 5, par. 1, règlement Double Usage.
[421] *Ibid*., par. 2.
[422] *Ibid*., par. 3.
[423] *Ibid*., art. 9, par. 1.
[424] *Ibid*., par. 2.
[425] *Ibid*., art. 10, par. 1.

concernés doivent notifier leurs autorités douanières ainsi que les autres autorités nationales compétentes[426].

La procédure des articles 5 et 9 du règlement témoigne de la volonté de donner un rôle actif aux États membres, pour appréhender tout type de situations nécessitant un contrôle étroit. Une fois le bien qualifié de « bien à double usage », l'exportation doit remplir les conditions relatives à la procédure d'autorisation.

2.1.2.3 La procédure d'autorisation d'exportation

Les biens visés par le règlement sont soumis à une procédure d'autorisation d'exportation, qui peut prendre différentes formes. Il existe une autorisation individuelle, une autorisation globale, une autorisation générale nationale et une autorisation générale de l'Union[427].

Les autorisations individuelles et globales d'exportation sont délivrées pour une durée maximale de deux ans[428], sauf décision contraire de l'autorité compétente ou dans le cas de « grand projet »[429] et sont valables pour l'ensemble du territoire douanier de l'Union.

Elles sont octroyées par l'autorité compétente de l'État membre où l'exportateur réside ou est établi. S'il ne réside pas ou n'est plus établi sur le territoire douanier de l'Union, l'autorité compétente est celle de l'État membre où se situent les biens[430]. Dans le cas où l'exportateur ne réside pas, ou n'est plus établi sur le territoire douanier de l'Union et que ses biens ne s'y situent pas également, le règlement ne s'applique pas.

L'exportateur demandeur doit fournir exhaustivement toutes les informations pertinentes à l'autorité compétente, telles que l'utilisateur final, le pays de destination, ainsi que toutes les utilisations finales[431].

Il doit également fournir une déclaration d'utilisation finale, requise pour les autorisations individuelles, bien que l'autorité puisse exempter le demandeur, mais facultative pour les autorisations globales. Les exportateurs qui demandent une autorisation globale doivent mettre en œuvre un Programme Interne de Conformité

[426] *Ibid*., par. 3.
[427] *Ibid*., art. 12, par. 1.
[428] *Ibid*., art. 12, par. 3.
[429] Dans ce cas, l'autorisation maximale est de quatre ans, sauf circonstances dûment justifiées.
[430] *Ibid*., art. 12, par. 2.
[431] *Ibid*., par. 4.

(PIC), dont les conventions sont spécifiées par chaque État. Le PIC est un ensemble de politiques et de procédures permanentes efficaces, appropriées et proportionnées, adoptées pour favoriser le respect des obligations du règlement par les exportateurs[432].

Les autorisations générales nationales sont définies par le droit national et peuvent être demandées par tous types d'exportateurs, sous réserve de satisfaire aux exigences du règlement et à la législation nationale complémentaire[433].

Elles concernent un éventail de biens plus restreint que les autorisations individuelles ou globales. Elles ne peuvent pas être délivrées pour les biens figurant à l'annexe II, section I[434] ou susceptibles d'être destinés à un usage militaire[435]. Les États membres notifient immédiatement la Commission de toute autorisation générale nationale d'exportation délivrée ou modifiée.

Pour finir, les autorisations générales d'exportation de l'Union sont strictement définies à l'annexe II du règlement. Elle détaille, pour chaque bien, les pays tiers vers lesquels l'exportation est autorisée et, pour chacune des autorisations qui en découlent, l'autorité de délivrance, les conditions et les exigences d'utilisations. Les autorités compétentes des États membres peuvent interdire à un exportateur le recours à cette dernière catégorie d'autorisation, « *si on peut raisonnablement douter de la faculté de l'exportateur de se conformer aux termes de cette autorisation ou à une disposition de la législation applicable en matière de contrôle des exportations* »[436].

[432] *Ibid*., art. 2, par. 21.
[433] *Ibid*., art. 12, par. 6, sous b).
[434] *Ibid*., sous a).
[435] *Ibid*., sous c).
[436] *Ibid*., art. 12, par. 7.

Conclusion

Considérant l'étude du cadre juridique national et européen, deux constats s'imposent.

D'une part, les règles qui entourent à la fois les dispositifs techniques de captation de données informatiques et de manière générale les biens de cybersurveillance, termes recouvrant les outils utilisés pour l'accès au support de données informatiques et pour la mise au clair de données chiffrées, ont pour traits communs l'impératif de traçabilité et l'identification précise de chaque acteur concerné.

La traçabilité quantifie le nombre de biens en circulation ou en utilisation effective et l'identification de garantie la légalité de la production, de l'acquisition et de l'exportation. Ces deux aspects sont déterminants en cas de manquements potentiels aux obligations juridiques par les acteurs économiques, ils garantissent l'effectivité du cadre juridique.

D'autre part, l'analyse de ces cadres confirme qu'ils ne concernent pas les vulnérabilités exploitables *stricto sensu*.

La vulnérabilité exploitable n'est qu'une information, un ensemble de données qui, tant qu'elle n'aboutit pas sur la création d'un dispositif technique, ne tombe pas sous le joug de l'article 226-3 du code pénal ni, difficilement qualifiable de « *bien de cybersurveillance* », sous celui du règlement double usage. À l'état brut, son acquisition, exportation, cession et détention sont uniquement régies par l'article 323-3-1 du code pénal.

Au vu de ce qui précède, une question demeure. En effet, l'article 323-3-1 du code pénal n'éclaire que peu le cadre juridique des vulnérabilités encore non découvertes par le public. En outre, cette idée de traçabilité et de responsabilité n'est pas nécessairement présente en tout lieu, notamment au niveau des vulnérabilités exploitables par les services de police judiciaire et de renseignement. Il convient à présent d'aborder le cas des vulnérabilités susceptibles de faciliter l'action des services susmentionnés.

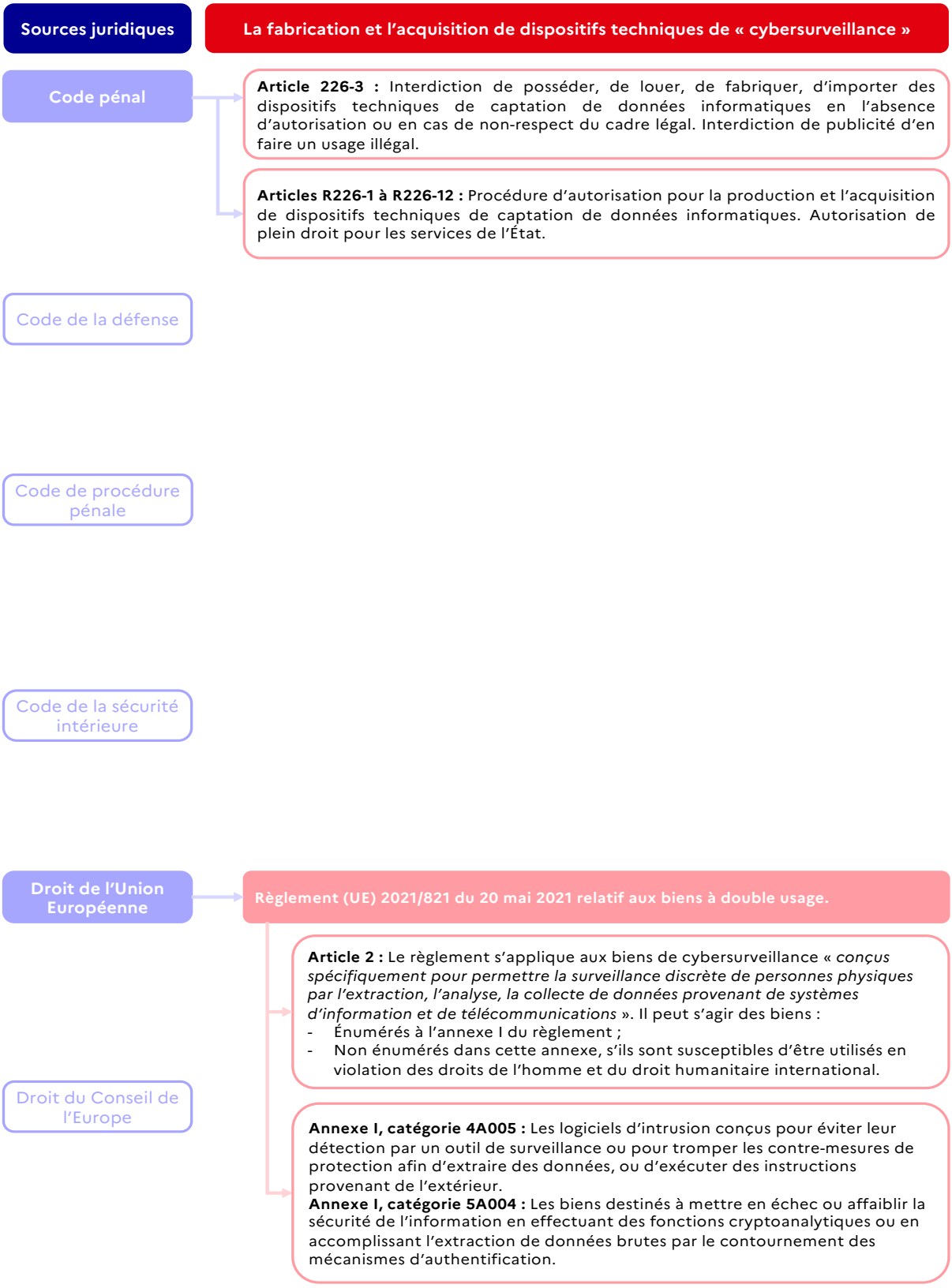

Figure 5. Tableau récapitulatif du régime de fabrication, d'acquisition et d'exportation des biens de cybersurveillance.

2.2 L'autonomisation du cadre juridique des vulnérabilités exploitables utiles aux services de police judiciaire et de renseignement

Les règles générales qui entourent les vulnérabilités exploitables tendent à imposer leur remontée et leur correction sans délai aux autorités compétentes, si elles sont significatives, ou à défaut, leur prompte correction.

Européennes ou nationales, ces règles s'accordent sur l'importance d'assurer un certain niveau de sécurité des systèmes d'information que la remontée et la correction permettent. Or, les recommandations du Parlement européen sur l'utilisation alléguée de Pegasus et autres logiciels espions[437] ont mis en évidence l'importance des vulnérabilités jour zéro dans le fonctionnement de ces logiciels, dont les dispositifs techniques font partie. Une « *vulnérabilité jour-zéro* » est une vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant pas reçu de correctif au moment de son exploitation[438].

Ce type de vulnérabilité permet le déploiement du dispositif technique, sans interaction de la cible avec du contenu infecté. Toujours selon ces recommandations, l'échange d'informations sur les vulnérabilités de systèmes logiciels fait l'objet d'un commerce direct entre différentes parties ou est facilité par des intermédiaires, et qui impliquerait aussi bien des acteurs non étatiques et des organisations criminelles. De plus, « *l'acquisition, le commerce et l'accumulation de vulnérabilités jour zéro compromettent les fondements mêmes de l'intégrité et de la sécurité des communications des citoyens de l'Union et leur cybersécurité* »[439].

[437] Recommandation du Parlement européen du 15 juin 2023 à l'intention du Conseil et de la Commission à la suite de l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (2023/2500(RSP)), *préc*.

[438] CyberDico de l'ANSSI FR/EN, mis à jour le 5 décembre 2024, *préc.*

[439] §E, §F, §G, recommandation du Parlement européen du 15 juin 2023 à l'intention du Conseil et de la Commission à la suite de l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (2023/2500(RSP)), *op. cit*.

Dans la mesure où les règles concernant la remontée et la correction des vulnérabilités jour zéro ne cessent de croître[440], il est pertinent d'analyser comment s'articule ce cadre avec les besoins des services de police judiciaire et de renseignement.

Par ailleurs, cette articulation est également intéressante dans le cas des portes dérobées, des vulnérabilités intentionnellement créées aux fins de faciliter l'action des autorités compétentes.

Sur ces deux points, le droit européen offre un aperçu des points de tension, des solutions envisagées et des lignes rouges qui ne devraient pas être franchies.

En effet, l'enjeu relatif à la non-remontée et correction des vulnérabilités jour zéro bénéficie des apports du règlement sur la cyberrésilience[441] et de la directive sécurité des réseaux informatiques II[442] (**2.2.1**), celui des portes dérobées, de l'arrêt *Podchasov c. Russie* de 2024[443] de la Cour européenne des droits de l'homme (ci-après, « CEDH ») (**2.2.2**).

2.2.1 Le cadre juridique des vulnérabilités jour zéro en matière de police et de renseignement

Une fois découvertes, les vulnérabilités jour zéro doivent faire l'objet de correction. Cela ne veut pour autant pas dire qu'elles doivent être obligatoirement remontées aux autorités compétentes, telles que l'ANSSI en France. La règlementation s'applique de façon différenciée, en fonction de la gravité de la vulnérabilité, de la qualité du propriétaire du système d'information sur lequel elle se trouve.

Il conviendra de revenir succinctement sur cette règlementation, d'en définir les contours (**2.2.1.1**), pour contextualiser les développements concernant le domaine judiciaire et du renseignement (**2.2.1.2**).

[440] Voir la directive SRI II.
[441] Règlement sur la cyberrésilience.
[442] Directive SRI II.
[443] CEDH, 13 février 2024, *Podchasov c. Russie*, n°33696/19.

2.2.1.1 Les obligations nationales et européennes relatives à la gestion des vulnérabilités exploitables

En droit national, l'obligation de signalement et de correction des vulnérabilités significatives découle l'article L.2321-4 du code de la défense. Elle concerne uniquement les éditeurs de logiciels, c'est-à-dire *« toute personne physique ou morale qui conçoit ou développe un produit logiciel ou fait concevoir ou développer un produit logiciel et qui le met à la disposition d'utilisateurs, à titre onéreux ou gratuit »*[444], et qui fournissent leur produit sur le territoire français, à des sociétés ayant leur siège social sur le territoire français ou à des sociétés contrôlées par des sociétés ayant leur siège social sur le territoire français[445].

Cet article, créé en 2023 par la Loi n°2023-703[446], s'inscrit dans une volonté d'informer les utilisateurs de ces produits des vulnérabilités existantes, afin qu'ils soient en mesure de prendre des mesures adaptées pour éviter les incidents[447]. Il a une logique d'anticipation et non de réaction *a posteriori*.

Seules les vulnérabilités significatives doivent être notifiées à l'ANSSI, qui collaborera avec l'éditeur pour sa correction. L'évaluation du degré de sa criticité est effectuée par l'éditeur, au regard des critères posés par l'article R2321-1-16 du code de la défense.

L'éditeur prend en considération les éléments suivants :

- Le nombre d'utilisateurs concernés par la vulnérabilité affectant le produit ;
- Le nombre de produits intégrant le produit affecté ;
- L'impact technique, potentiel ou actuel, de la vulnérabilité sur le fonctionnement attendu du produit. Selon les fonctionnalités du produit, cet impact est évalué au regard de critères de sécurité, tels que la disponibilité, l'intégrité, la confidentialité ou la traçabilité ;
- Le type de produit au regard de ses usages et de l'environnement dans lequel il est déployé ;
- L'exploitation imminente ou avérée de la vulnérabilité ;

[444] Art. L2321-4-1, al. 3 CD.
[445] *Ibid*., al. 1.
[446] Art. 66, loi n°2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, *JORF* n°177 du 2 août 2023.
[447] Étude d'impact, projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, du 4 avril 2023 p. 336.

- L'existence d'une preuve technique d'exploitabilité ou d'un code d'exploitation.

Les dispositions de l'article L.2321-4 ne sont pas les seules applicables en matière de gestion des vulnérabilités. Les dynamiques européennes tendant au nivellement de la sécurité des systèmes d'information des entités économiques ou essentielles ont obligé la France à adopter la loi n°2018-133[448] et le décret n°2018-384[449] qui imposent des obligations aux opérateurs de services essentiels et aux fournisseurs de service numérique.

Cette législation transpose en droit interne la directive 2016/1148 « SRI »[450], texte de l'Union européenne concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité. La Loi, le décret, et la directive s'appliquent aux opérateurs de services essentiels, entités « *publiques ou privées, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services* »[451]. En droit français, la liste de ces services essentiels figure à l'annexe du décret n°2018-384[452].

Ces normes s'appliquent également aux fournisseurs de services numériques. Les termes « *services numériques* » renvoient à « *tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services* », les fournisseurs étant toute personne morale fournissant l'un des services suivants : place de marché en ligne, moteur de recherche en ligne ou service informatique en nuage[453].

[448] 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 (1), *JORF* n°48 du 27 février 2018.
[449] Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, *JORF* n°118 du 25 mai 2018.
[450] 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 de l'Union (Directive SRI I).
[451] Art. 5, 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 (1), *JORF* n°48 du 27 février 2018.
[452] Ce sont les entités dans le secteur de l'énergie (pétrole, gaz, électricité) ; du transport (aérien, ferroviaire, guidé, maritime, routier) ; de la banque ; de l'assurance ; du social ; de la santé ; etc. (liste non exhaustive)
[453] Art. 10, 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 (1), *JORF* n°48 du 27 février 2018.

La gestion des vulnérabilités est mise en place à travers deux catégories d'obligations, relatives aux contrôles et aux politiques de sécurité du système d'information.

Les opérateurs de services essentiels (ci-après, « OSE »)[454] et les fournisseurs de service numérique[455] peuvent se voir imposer un contrôle destiné à vérifier le respect des obligations qui leur incombent. À l'issue de ce dernier, l'ANSSI ou le prestataire ayant effectué le contrôle doit rédiger un rapport exposant ses constatations. Dans ce dernier, les vulnérabilités identifiées sont indiquées, avec des recommandations pour y remédier[456].

Les OSE et les fournisseurs de services numériques doivent mettre en place des mesures techniques et organisationnelles nécessaires et proportionnées pour « *gérer (les) risques, pour éviter les incidents de nature à porter atteinte à ces réseaux et systèmes d'information, ainsi que pour en réduire au minimum l'impact* »[457].

Parmi ces mesures, la mise en place de procédures de maintien en condition de sécurité. Elles ne concernent que les OSE, et définissent « *les conditions permettant de maintenir le niveau de sécurité des ressources des systèmes d'information essentiels en fonction de l'évolution des vulnérabilités et des menaces, et précisent notamment la politique d'installation de toute nouvelle version et mesure correctrice de sécurité d'une ressource et les vérifications à effectuer avant l'installation.* »[458].

Pour les fournisseurs de service numérique, les mesures susvisées concernent la gestion des incidents, avec la mise en place de « *processus et de procédures de détection maintenus et contrôlés afin d'assurer en temps voulu la bonne connaissance des événements anormaux* » et de « *processus et politiques sur le signalement des incidents et des faiblesses et vulnérabilités décelées sur le système d'information* »[459].

---

[454] *Ibid*., art. 8.

[455] *Ibid*., art. 24.

[456] Art. 15, décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, *JORF* n°118 du 25 mai 2018.

[457] Ibid., art. 6 (opérateurs de services essentiels) et art. 12 (fournisseurs de service numérique).

[458] Sect. 4, règle 16, arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, *JORF* n°118 du 25 mai 2018.

[459] Art. 2, par. 2, règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant

Bien que déjà relativement étoffé, le cadre juridique de la gestion des vulnérabilités est amené à évoluer, par le biais de la directive 2022/2555 (SRI II), dont la transposition est en cours, et le règlement sur la cyberrésilience, entré en vigueur le 10 décembre 2024 mais dont les obligations s'appliqueront à partir de 2027[460].

La directive SRI II s'inscrit dans la continuité de la directive SRI de 2016, tout en allant plus loin. Elle fixe des obligations aux États, afin qu'ils adoptent des stratégies nationales en matière de cybersécurité, pour qu'ils désignent ou mettent en place plusieurs types d'entités comme points de contact uniques, des autorités de gestion de cybercrises, des centres de réponse aux incidents de sécurité informatique (CSIRT). Elle impose des mesures de gestion de risques, des obligations d'information, des règles et des obligations pour le partage d'informations ainsi que des obligations en matière de supervision et d'exécution[461].

La directive s'applique toujours aux opérateurs de service essentiel et aux fournisseurs de service numérique, mais englobe désormais d'autres secteurs critiques. Sont visés, par exemple, les services postaux et de messagerie, de gestion des déchets, de fabrication, de production et de distribution de produit chimique, de production, de transformation et de distribution de denrées alimentaires, mais aussi l'industrie manufacturière ou les organismes de recherche[462].

Parmi les obligations, sectorielles ou générales, qui s'imposent à ces entités, la gestion des vulnérabilités est de nouveau mise en avant. La directive explique que l'identification et la correction rapide des vulnérabilités sont un facteur important de la réduction du risque, qu'il est crucial que soient mises en place des procédures appropriées pour gérer les vulnérabilités découvertes[463]. Cela implique une obligation positive pour les États membres d'adopter des politiques portant sur la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée de celles-ci[464].

---

les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif, cité par l'article 18 du décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

[460] Article 71, règlement sur la cyberrésilience.

[461] Art. 1, par. 2, directive SRI II.

[462] *Ibid.*, annexe II.

[463] *Ibid.*, §58.

[464] *Ibid.*, art. 7, par. 2, sous c).

Ainsi, à la différence de la première directive, la directive SRI II considère la participation des utilisateurs et, donc, également, des chercheurs non contractuels, comme nécessaire, voire cruciale. Sur ce point, le droit national est susceptible d'évoluer en vertu de cette directive.

Le règlement sur la cyberrésilience, quant à lui, vise à établir des règles concernant la mise à disposition sur le marché de produits comportant des éléments numériques, afin de garantir la cybersécurité de ces produits ; à établir les exigences essentielles de cybersécurité, en matière de conception, de développement et de production de produits comportant des éléments numériques, et les obligations qui incombent aux opérateurs économiques visés ; à établir également des exigences en termes de gestion des vulnérabilités par les fabricants[465].

Le choix de l'instrument, un règlement et non une directive, fait qu'il s'appliquera tel quel sans nécessiter de transposition. Cette circonstance est particulièrement intéressante, puisqu'il contient la majorité des dispositions pertinentes concernant la remontée et la correction des vulnérabilités jour zéro par les services de police judiciaire et de renseignement.

2.2.1.2 La vision européenne de la gestion des vulnérabilités jour zéro par les services judiciaires ou de renseignement

La vulnérabilité jour zéro est à la fois celle utilisée par les services de police judiciaire et de renseignement aux fins de leurs missions, mais aussi celle potentiellement présente sur les systèmes d'information utilisés par ces services, qu'il s'agisse des équipements techniques de mise au clair de données chiffrées, d'accès au support de données informatiques, ou des dispositifs techniques de captation de données informatiques. Au sein de la présente section, les termes « équipements techniques » engloberont l'ensemble des outils utilisant ou susceptibles d'utiliser des vulnérabilités jour zéro.

Tout d'abord, il faut rappeler que le droit de l'Union européenne ne s'applique pas en matière de sécurité nationale. L'Union « *respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité*

[465] Art. 1, règlement sur la cyberrésilience.

nationale reste de la seule responsabilité de chaque État membre »[466]. En vertu de ce principe, l'activité des services de renseignement, si elle n'impose pas d'obligations aux opérateurs économiques, ne peut être régie par le droit de l'Union [467]. Il en va autrement pour les services de police judiciaire.

En dépit de ce principe, la directive SRI II exclut de son champ d'application, les deux services indifféremment. Son article 2, paragraphe 7, dispose que « *la présente directive ne s'applique pas aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière* ». En France, cela désigne bon nombre de services, dont les services de police judiciaire et de renseignement. Les obligations dont il a été question à la section précédente ne peuvent être opposées à ces deux services.

Par ailleurs, selon le paragraphe 8 du même article, les États membres peuvent également exempter d'autres entités spécifiques, lorsqu'elles exercent des activités comme celles ci-dessus mentionnées, ou qu'elles fournissent des services exclusivement aux entités ci-dessus mentionnées[468]. Les entités visées par le paragraphe pourraient être les personnes morales désignées pour les opérations de captation de données informatiques, d'accès au support de données informatiques ou de mise au clair de données chiffrées. Elles peuvent aussi être les personnes chargées du développement de dispositifs techniques de captation, autorisées en vertu de l'article R226-1 et suivants du code de pénal ou toute autre personne compétente pour le développement d'équipement utile aux missions des services de police judiciaire ou de renseignement.

Ces exemptions ne concernent que les obligations aux articles 21 et 23. L'article 21 traite des mesures de gestion des risques en matière de cybersécurité, c'est-à-dire le fait de prendre des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des

[466] Art. 4, par. 2, Traité sur l'Union européenne (TUE) (version consolidée) du 13 décembre 2007, *JOUE* C 326/13, 26 octobre 2012.
[467] CE, Ass., 21 avril 2021, *French Data Network et autres*, n°393099, n°394922, n°397844, n°397851, n°424717, n°424718, §67 et §93.
[468] Art. 2, par. 9, règlement sur la cyberrésilience : les paragraphes 7 et 8 ne s'appliquent pas aux services de confiances (au sens de l'article 3, paragraphe 16 du règlement (UE) n°910/2014), ceux fournissant des services électroniques contre rémunération, tels que la délivrance de certificats de signature électronique, la création de signatures électroniques ou de cachets électroniques, la délivrance d'attestations électroniques d'attributs, etc.

systèmes d'information que ces entités utilisent[469]. Ces entités doivent prendre en compte les vulnérabilités propres à chaque fournisseur et prestataire de services directs et de la qualité globale des produits et des pratiques de cybersécurité[470].

L'article 23 traite des obligations d'information, la notification sans retard injustifié aux autorités compétentes, de tout incident ayant un impact important sur la fourniture de leurs services.

En somme, les entités visées au paragraphe 8 de l'article 2 sont exemptées des obligations favorisant la transparence, et la sécurité de leur système d'information. Ces obligations pourraient avoir pour effet d'amenuir l'efficacité de leurs missions, bien que l'exemption interroge sur le contrôle de la fiabilité des services et produits fournis.

De plus, les États peuvent également exempter ces entités des obligations prévues aux articles 3 et 27, si elles exercent exclusivement des activités ou fournissent exclusivement des services dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière.

L'article 3 impose la communication aux autorités nationales, des informations relatives au nom de l'entité, son adresse et ses coordonnées actualisées, ses adresses électroniques, plages d'IP et numéros de téléphone. L'article 27 lui impose la communication des mêmes éléments aux fins de la création par l'ENISA d'un registre des entités.

Ces obligations ont pour objectifs le recensement et la traçabilité des entités visées par la directive. Les exemptions garantissent aux États la confidentialité des acteurs missionnés dans le cadre des activités ci-dessus énumérées.

Au vu de ce qui précède, la directive SRI II n'a pas été pensée pour assurer la sécurité des systèmes d'information des services de police judiciaire et de renseignement, et des entités collaborant avec ceux-ci.

Sur le cas des vulnérabilités jour zéro utilisées directement par les services mentionnés, le droit de l'Union semble également ne pas se saisir de la question. Les dispositions du règlement sur la cyberrésilience confirment plutôt cette hypothèse.

[469] *Ibid*., art. 21, par. 1.
[470] *Ibid*., par 3.

En effet, l'article 2, paragraphe 7 du règlement, relatif au champ d'application, est rédigé ainsi « *le présent règlement ne s'applique pas aux produits comportant des éléments numériques qui sont développés ou modifiés exclusivement à des fins de sécurité nationale ou de défense, ni aux produits spécifiquement conçus pour traiter des informations classifiées* ». Son paragraphe 8 continue : « *les obligations prévues dans le présent règlement n'impliquent pas la fourniture d'informations dont la divulgation serait contraire aux intérêts essentiels des États membres en matière de sécurité nationale, de sécurité publique ou de défense* ». Ces deux paragraphes permettent de formuler plusieurs constats.

Seuls les équipements techniques développés ou modifiés pour être utilisés par les services de renseignement sont explicitement exclus du champ d'application du règlement.

Les équipements techniques utilisés par les services de police judiciaire doivent remplir certaines conditions pour bénéficier de la clause d'exclusion (article 2, paragraphe 7) ou de la clause de dérogation (article 2, paragraphe 8).

Pour la clause d'exclusion, il est nécessaire de déterminer si les termes « informations classifiées » recouvrent les vulnérabilités exploitables, auquel cas la clause d'exclusion s'appliquerait à tout équipement technique utilisé par les services judiciaires. Pour la clause de dérogation, il s'agit de savoir si la fourniture d'informations relatives à ces équipements serait contraire aux intérêts essentiels de l'État en matière de sécurité publique, et si ceci serait propre à légitimer la non-remontée de vulnérabilités jour zéro.

Ainsi, pour bénéficier de la clause d'exclusion, les vulnérabilités exploitables devraient non seulement être qualifiées d'informations classifiées, mais également être « traitées » par le produit. La difficulté est d'ordre sémantique. Les équipements techniques fonctionnent en exploitant ces vulnérabilités, pour autant, est-ce qu'ils traitent celles-ci ?

Quant à la qualification de ces vulnérabilités en tant qu'informations classifiées, en dehors du recours aux moyens de l'État soumis au secret de la défense nationale, aucun texte en droit national ne fournit de réponses. En l'état, l'applicabilité de ce paragraphe aux équipements techniques utilisés par les services judiciaires reste indéterminée.

La portée des dispositions du paragraphe 8 de l'article 2 vis-à-vis de ces équipements est en revanche moins ambiguë. Les activités des services judiciaires relèvent bien de la

sécurité publique, puisqu'elles ont pour objectifs de veiller au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens[471].

Eu égard l'ensemble des thématiques abordées dans le livrable, et l'apport de ces analyses, il est possible d'affirmer que l'opacité du mode de fonctionnement des équipements utilisés est indissociable de l'efficacité des opérations conduites (en effet, la divulgation des caractéristiques techniques risquerait de permettre aux cibles de la surveillance d'adapter leur propre technologie pour renforcer leur protection).

Or, l'opacité du mode de fonctionnement implique nécessairement que les vulnérabilités exploitables ne soient pas divulguées au public. Cela est d'autant plus vrai dans le cadre de la captation de données informatiques, où il semblerait que les dispositifs techniques soient conçus précisément sur la base des vulnérabilités jour zéro, découvertes.

Dans l'affaire EncroChat, par exemple, le dispositif technique de captation utilisé par les services de police judiciaire avait été élaboré en analysant le fonctionnement des téléphones saisis. Ces téléphones utilisaient EncroChat, un système d'exploitation secondaire comprenant des fonctionnalités de confidentialité avancées, rendant impossible le déchiffrement des données contenues[472].

Les données provenant des téléphones saisis et les vulnérabilités jour zéro identifiées constituaient des fondements sur la base desquels a été développé ce dispositif technique.

Son mode de fonctionnement étant indissociable des vulnérabilités identifiées, il est possible de supposer que chaque opération de captation nécessite la création d'un dispositif spécifiquement adapté.

Puisque l'opacité du fonctionnement de ces dispositifs est impérative pour leur efficacité, la transparence technique devenant contraire aux intérêts de l'État au sens du paragraphe 8 de l'article 2 du règlement, la remontée des vulnérabilités jour zéro identifiées pourrait aussi être jugée contraire à ces intérêts.

Au titre de cet article, les autorités compétentes et entités collaboratrices qui ne signaleraient pas une vulnérabilité jour zéro utilisée ou susceptible d'être utile ne violeraient pas le droit de l'Union.

[471] Art. L111-1 CSI, relatif à la sécurité publique.
[472] CEDH, 17 octobre 2024, *A.L c. France* et *E.J c. France*, n°44715/20 et n°47930/21, §16.

Il en va de même pour les équipements techniques utilisés dans le cadre de l'accès au support de données informatiques ou de la mise au clair de données chiffrées.

Ce qui est précède est une analyse de la portée hypothétique du règlement sur la cyberrésilience et de la directive SRI II. La Cour de justice de l'Union européenne (ci-après, « CJUE ») ne s'est pas prononcée sur le sujet, il faudra attendre ses développements jurisprudentiels pour être assurés de l'incidence de ces textes sur la gestion des vulnérabilités exploitables par ces services.

Pour l'heure, ces théories semblent conformes à la position de la CEDH, puisqu'elles auraient pour finalité de faciliter l'exercice des missions des services judiciaires et de renseignement, ce qui justifierait, au vu des alternatives présentes, l'interdiction des portes dérobées.

2.2.2 La création de vulnérabilités intrinsèques : les portes dérobées

Les portes dérobées sont une « *création intentionnelle, présente sur un système, servant à compromettre la sécurité de celui-ci, en facilitant l'accès à des informations ou des fonctionnalités nécessitant normalement des droits spécifiques* »[473]. Dans le cadre des missions des services judiciaires et de renseignement, leur utilisation constituerait un gain de temps, réduirait les incertitudes liées au succès des opérations, les coûts financiers et assurerait, de manière générale, une meilleure répression de la criminalité. Leur mise en place pallierait aussi la question de l'intégrité et de la fiabilité des preuves ou données recueillies.

En 2025, la proposition de loi visant à sortir la France du piège du narcotrafic[474] a fait l'objet d'un amendement pour y insérer l'article 8 TER[475]. Cet article a pour objectif de créer des portes dérobées, en imposant aux plateformes de « *mettre en œuvre des mesures techniques afin de permettre aux services de renseignement, d'accéder au contenu intelligible des correspondances et données qui y transitent* ». Cet accès serait conditionné aux modalités procédurales relatives aux services de renseignement, avec le concours de la CNCTR, et les personnes physiques ou morales qui refuseraient de se

[473] Sam L. Thomas, Aurélien Francillon "Backdoors: Definition, Deniability & Detection", 10 septembre 2018, p. 6.
[474] Proposition de loi visant à sortir la France du piège du Narcotrafic, enregistrée à la Présidence du Sénat le 12 juillet 2024, n°735 *Rect.* Présentée par MM. Etienne Blanc et Jérôme Durain.
[475] Proposition de loi sortir la France du piège du narcotrafic, amendement n°73 rect. Ter, 28 janvier 2025.

soumettre à l'obligation s'exposeraient à des sanctions pénales. Débattu dans l'hémicycle, cet article a finalement été supprimé par l'Assemblée nationale. Une suppression confirmée par la Commission mixte paritaire.

Ces avantages ne viennent pas sans conséquences, dont les tenants et aboutissants sont actuellement discutés au niveau de la CEDH et de l'Union européenne.

La CEDH a souligné, dans l'arrêt *Podchasov c. Russie*[476], que les techniques pour sécuriser et protéger le caractère privé des communications électroniques contribuaient à assurer l'exercice d'autres droits fondamentaux, tels que la liberté d'expression. Elles ont été jugées nécessaires pour permettre aux personnes physiques ou morales de se défendre contre les piratages, l'usurpation d'identité, le vol de données ou la divulgation d'informations confidentielles[477]. La CEDH a aussi rappelé que les portes dérobées avaient un impact généralisé, et ne pouvaient être créées de façon ciblée pour un ou plusieurs individus. Qu'il n'était pas exclu qu'elles soient ultérieurement exploitées par des réseaux criminels ou par des services de renseignements étrangers, comme ce fut le cas pour la Grèce en 2004, par l'Agence nationale de la sécurité des États-Unis[478].

En l'espèce, la CEDH juge que la mise en place de portes dérobées par les autorités russes constitue une ingérence disproportionnée au regard du droit au respect de la vie privée. Elle a donné trois raisons pour justifier sa position : une telle création mettrait à risque l'ensemble des utilisateurs du système d'information ou du STAD, elle supposerait d'imposer aux fournisseurs d'affaiblir la sécurité de leur propre produit, et, il existe des méthodes alternatives, moins intrusives[479].

La Russie a ainsi été condamnée par la CEDH pour violation de l'article 8 de la Convention[480].

---

[476] CEDH, 13 février 2024, *Podchasov c. Russie*, n°33696/19.

[477] *Ibid*., §76.

[478] Communément appelée *The Athens Affair*, il s'agit de l'utilisation par l'Agence nationale de la sécurité des États-Unis (NSA) du mécanisme d'interception légale du réseau Vodafone grecque, pour surveiller des membres du gouvernement grec et des fonctionnaires de haut rang. Pour aller plus loin (Article).

[479] *Ibid*., §78-79.

[480] Art. 8 « *Toute personne a droit au respect de la vie privée et familiale, de son domicile et de sa correspondance* », Convention STCE n°005 du Conseil de l'Europe du 4 novembre 1950, de sauvegarde des droits de l'homme et des libertés fondamentales, (Convention EDH).

Dans cet arrêt, la CEDH est revenue sur les prises de position de certains organes de l'Union européenne en matière de portes dérobées, afin de contextualiser son approche.

Elle a cité le considérant 94 de l'arrêt de la CJUE, du 6 octobre 2015 *Maximilian Schrems c. Data Protection Commissioner*[481]. Il est dit « *en particulier, une règlementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communication électronique doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte* »[482]. En droit de l'Union, les limitations d'un droit ne doivent pas porter atteinte à leur contenu essentiel[483]. Bien que la CJUE ne se soit pas précisément positionnée sur le cas des portes dérobées, l'accès généralisé que confèrent les portes dérobées pourrait constituer une atteinte au contenu essentiel de l'article 7 de la Charte des droits fondamentaux.

Le Comité européen de la protection des données[484] et le Contrôleur européen de la protection des données[485] ont également été cités par la CEDH, pour leur avis conjoint sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants[486]. En effet, les dispositions de la proposition du Parlement européen et du Conseil (ci-après, « CSAR »[487]) imposent aux fournisseurs de services internet de déchiffrer les communications en ligne afin de bloquer le matériel pédopornographique. En outre, le considérant 26 du CSAR consacre une liberté de choix pour la technologie de détection

[481] CJUE, gd. ch., 6 oct. 2015, n°C-362/14.

[482] Art. 7 *« toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* », Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000, *JOCE* C 364/01, (Charte DFUE).

[483] *Ibid*., art. 52, par. 1 *« toute limitation de l'exercice des droits et libertés reconnus dans 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* ».

[484] Organisme créé en 2018, veillant à ce que le règlement général sur la protection des données et la directive « Police-Justice » soient appliqués de manière cohérente dans les pays de l'UE, en fournissant par exemple des orientations générales pour clarifier la portée de ces deux textes.

[485] Organisme créé en 2004, veillant à ce que les institutions et organes de l'UE respectent le droit des citoyens à la protection de leur vie privée lors du traitement de données à caractère personnel.

[486] Avis conjoint 4/2022 de l'EDPB et du CEPD adopté le 28 juillet 2022, sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfant.

[487] Proposition de règlement 2022/0155 du Parlement européen et du Conseil du 11 mai 2022 établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants COM(2022)209.

du matériel, mais aussi au niveau des mesures techniques de protection de la confidentialité des communications, tant que ce choix répond aux exigences du règlement, c'est-à-dire que la détection demeure possible[488].

La liberté de choix dans les mesures de confidentialité, couplée à l'obligation de détection, pourrait avoir pour effet de pousser les fournisseurs à affaiblir leurs mécanismes de chiffrement pour faciliter leur conformité aux dispositions règlementaires[489]. L'avis conjoint évoque des craintes concernant la dégradation ou le découragement de l'utilisation du système E2EE (système de chiffrement de bout en bout), ou le recours à des procédés risqués[490]. De tels procédés ou impacts sur le système E2EE aboutiraient à la création de portes dérobées.

Tant la Charte des droits fondamentaux de l'Union européenne que la Convention européenne des droits de l'homme sont partisanes d'une approche individualisée et non systématisée, dans les limitations ayant pour objectif la protection de la sécurité publique ou nationale. Les ingérences causées doivent être limitées au strict nécessaire, répondre à des circonstances précises, afin de garantir leur proportionnalité.

Partant, l'inconventionalité automatique des mesures visant la création de portes dérobées est sans surprise : l'objet même de leur création est l'affaiblissement du système de protection de la confidentialité des communications électroniques, afin d'obtenir un accès généralisé au contenu de celles-ci, sans que cet affaiblissement soit restreint à un individu ou groupe d'individus, sur lesquels pèseraient des soupçons.

Ne pouvant être par essence, limitée au strict nécessaire, il semblerait que le recours aux portes dérobées ne puisse être autorisé sous conditions de garanties techniques et procédurales, à l'instar de la captation de données informatiques ou des autres techniques dont il a été question.

---

[488] Avis conjoint 4/2022 de l'EDPB et du CEPD adopté le 28 juillet 2022, sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfant, p. 6.

[489] *Ibid.*, p. 30.

[490] Songeons notamment à l'examen côté client (en anglais : *client-side-scanning*) qui scannerait le contenu des communications électroniques sur le système d'exploitation ou le STAD d'un utilisateur, avant le chiffrement ou après son déchiffrement. Il reporterait le contenu jugé illégal. Cette technique présente des failles de sécurité dans son application, elle est susceptible d'être piratée ou détournée de son usage ordinaire (*cf.* Joint statement of scientists and researchers on EU's proposed Child Sexual Abuse Regulation, 4 juillet 2023, p. 3-4)

Conclusion

L'absolue prohibition du recours aux portes dérobées rend nécessaire l'assouplissement des conditions de conformité au droit européen applicables aux procédés actuellement utilisés par les services judiciaires et de renseignements.

Le risque de tensions entre l'ordre européen et national favorise la création d'un cadre permissif pour l'exploitation des vulnérabilités informatiques, ce qui influence le statut de la vulnérabilités exploitables.

Au niveau de l'Union européenne, le cadre juridique de la gestion des vulnérabilités exploitables par ces services est complètement dissocié du cadre applicable aux fournisseurs de services, opérateurs de services essentiels et opérateurs de secteurs critiques. Les nouvelles législations de l'Union européenne englobent à la fois les services judiciaires, missionnés au titre de la sécurité publique, et les services de renseignements, missionnés au titre de la protection des intérêts fondamentaux de la Nation. Cela ne signifie pas qu'ils bénéficient d'un statut similaire, les services judiciaires doivent toujours répondre du droit de l'Union, notamment la Charte des droits fondamentaux, ce qui n'est pas le cas des services de renseignements.

Cependant, le rapprochement de leur statut dans ces récentes législations est indéniable.

La CEDH, en matière de vulnérabilités exploitables, n'a pu se prononcer que dans le cadre de l'arrêt *Podchasov c. Russie*. L'absence de jurisprudences traitant précisément de ce type de vulnérabilité ne permet pas d'analyser les conditions requises pour la conventionnalité de leur statut. Pour autant, la présence d'alternatives ayant été utilisée pour justifier l'inconventionalité du recours aux portes dérobées, il semble que la CEDH ne soit pas opposée à l'exploitation de vulnérabilités aux fins d'un objectif légitime.

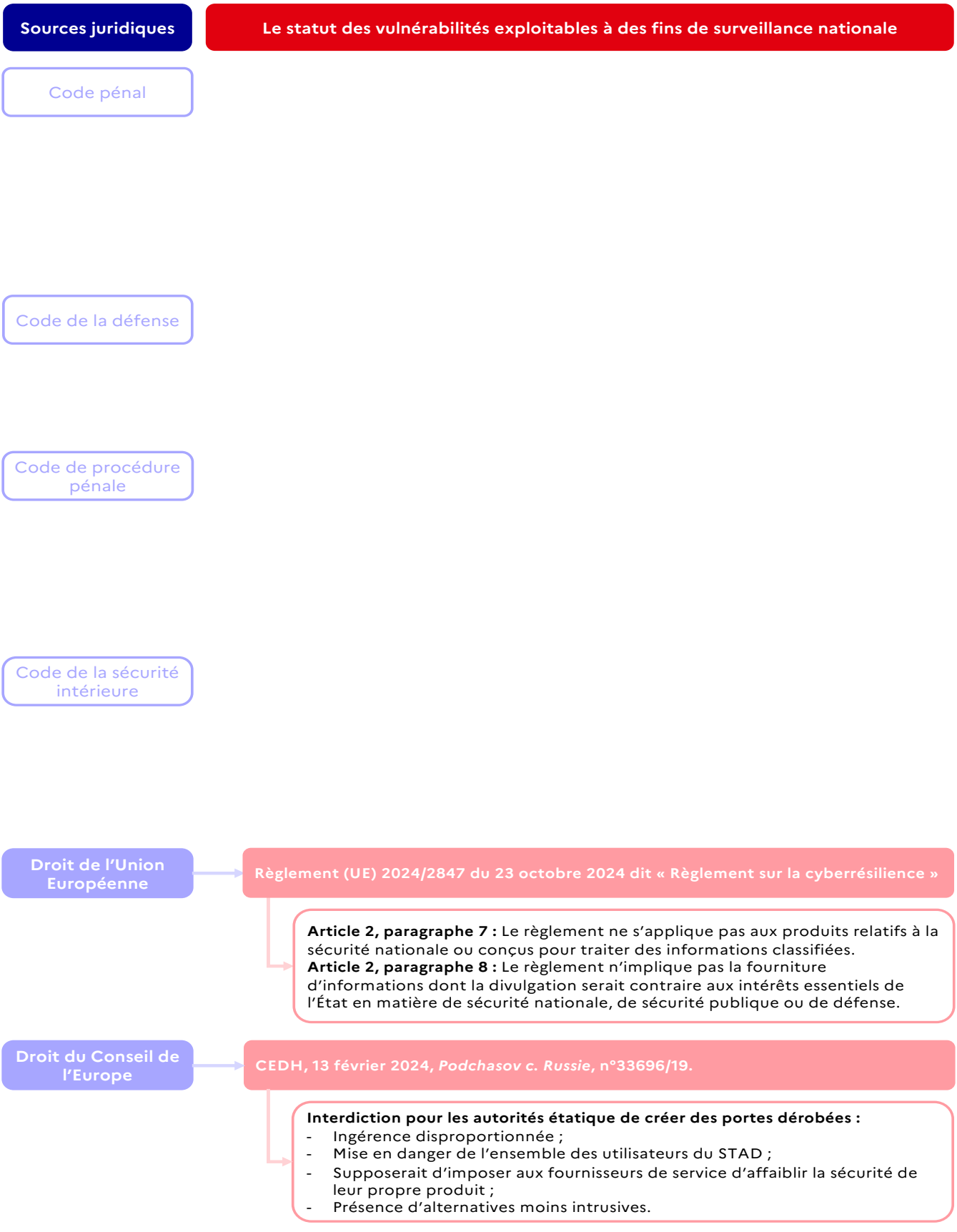

Figure 6. Tableau récapitulatif des dispositions applicables au cas des portes dérobées.

Conclusion de la Partie 2

Le cadre juridique français de la vulnérabilité exploitable se construit au gré de multiples influences, telles celles de l'ordre européen ou des évolutions technologiques.

Il tend à s'autonomiser du droit de l'Union européenne, une tendance récente puisqu'elle s'inscrit dans la stratégie numérique de l'Union, de 2020 à 2030. Les textes issus de cette génération ont un champ d'application restreint pour les matières judiciaires et de sécurité nationale. L'exclusion du domaine de la sécurité nationale du champ d'application des textes européens est conforme au principe de répartition des compétences entre les États membres et l'Union. Une telle exclusion n'est pas cependant pas banale pour le domaine des affaires judiciaires de « sécurité publique ».

Les deux dernières décennies ont vu naître un nombre important de développements autour du droit à la vie privée et du droit à la protection des données personnelles. De ces développements, règlementaires ou jurisprudentiels, résulte une amélioration des technologies de protection de la vie privée, tels que le chiffrement de bout en bout. Parallèlement, cette dernière décennie, les cyberattaques visant les administrations de l'État ou opérateurs essentiels, mais également les citoyens ont pris de l'ampleur. La conséquence directe de ce contexte a été la mise en place de mesures de protection poussées des systèmes d'information, ou support physique de ces systèmes. Par exemple, des mécanismes d'authentification.

Ces deux circonstances ont créé un environnement propice pour les activités criminelles. Le chiffrement de bout en bout, les mécanismes cryptologiques, d'authentification, la nécessité de respecter le droit à la vie privée de tout individu, ont conduit les autorités de l'État à requérir de plus en plus de droits pour dépasser ces barrières pour garantir la sécurité des individus.

Un cercle vicieux s'installe, plus le droit au respect de la vie privée est strictement appliqué, plus les technologies rendent difficile l'accès aux données par les autorités de l'État, plus les activités criminelles prospèrent, plus les autorités de l'État demandent des moyens pour franchir ces barrières, plus il y a d'ingérences dans le droit au respect de la vie privée, plus le droit au respect de la vie privée est strictement appliqué.

Or, un retour en arrière sur les techniques de protection de la vie privée semble difficilement envisageable. Ce retour en arrière constituerait un affaiblissement des techniques de chiffrement, par exemple, et donc, la création de portes dérobées.

Ainsi vient la question des techniques impliquant l'exploitation de vulnérabilités informatiques. L'exploitation de vulnérabilités, au vu de l'analyse du cadre juridique, notamment européen, paraît être conforme au droit européen, sous certaines conditions. Elle est une alternative valide à la création de portes dérobées.

Cependant, plusieurs problématiques entourent le cadre juridique de sa mise en œuvre.

Tout d'abord, « *exploitation de vulnérabilités* » est un terme qui regroupe plusieurs outils, pour des finalités différentes, selon des procédures variées. Il n'est même pas directement mentionné par les textes nationaux ou européens pertinents en matière judiciaire ou de renseignement. Il s'agit d'un terme purement technique, présent dans les textes applicables à la sécurité des systèmes d'information.

En matière judiciaire ou de renseignement, les termes privilégiés sont davantage « *la captation de données informatiques* », « *les opérations de mise au clair* », « *les opérations visant l'accès au support de données* ».

Cette différence de terminologie est source d'insécurité juridique : l'articulation entre les obligations, autorisations et principes découlant des domaines précités reste ambiguë. Une conséquence particulièrement notable au niveau du droit de l'Union, avec la directive SRI II et le règlement sur la cyberrésilience.

Ensuite, il n'est pas certain que la procédure nationale actuellement en vigueur soit conforme au droit de la Convention EDH. Les caractéristiques du procureur de la République ne permettent pas de le qualifier d'autorité indépendante et impartiale au sens de la Convention EDH. Si le Conseil constitutionnel n'a la même lecture que la CEDH à ce sujet, eu égard à la proéminence du rôle du procureur, un alignement de position serait le bienvenu.

Enfin, reste la problématique de l'intégrité des données rendues accessibles ou collectées, celles intéressant l'enquête étant ultérieurement utilisées en procès pénal. Puisque les techniques d'exploitation de vulnérabilités sont opaques, de sérieuses garanties doivent être mises à l'œuvre pour assurer que les données conservées n'ont pas été altérées.

BIBLIOGRAPHIE

I. Manuels, ouvrages généraux et spécialisés

Baud (J.), *Encyclopédie du renseignement et des services secrets,* Lavauzelle, Paris, 2004.

Bioy (X.), *Droits fondamentaux et libertés publiques,* LGDJ, coll. « Cours », Paris, 3ème éd., 2014.

COTTERET (J.-M.), DENECE (E.), *Le renseignement au service de la démocratie. Lois, fichiers, contrôle parlementaire et éthique,* Fauves éditions, Paris, 2018.

SUDRE (F.), *Droit européen et international des droits de l'homme*, PUF, coll. « Droit fondamental », 14ème éd., 2019.

TESQUET (O.), *A la trace. Enquête sur les nouveaux territoires de la surveillance,* Premier Parallèle, Paris, 2020.

VEDEL (G.), DELVOLVE (P.), *Droit administratif,* PUF, coll. « Thémis », Paris, 11ème éd., 1990, 2 tomes.

II. Thèses et mémoires

AUDIBERT (M.), *Le recueil de la preuve numérique : Enjeux et perspectives en procédure pénale*, th., Paris 10, 2024.

DEPRAU (A.), *Renseignement public et sécurité nationale,* th., Paris Panthéon-Assas, 2017.

GAUVIN (F.), *Le secret de la défense nationale en droit français,* th., Grenoble, 1996.

VERON (N.), *Protection des données personnelles et renseignement : contribution à l'identification d'un régime juridique autonome*, th., Pau et Pays de l'Adour, 2021.

III. Contributions dans des ouvrages collectifs et des mémoires

DIEMER (M.-O.), « L'exemple du contrôle des fichiers de renseignement par la formation spécialisée du Conseil d'État dans le cadre de son contrôle de légalité », *in Le juge et la sécurité nationale,* Mare & Martin, Paris, 2019.

EYNARD (J.,), « Les opérateurs de communications électroniques auxiliaires de police ? Réflexions autour de l'obligation de conservation des données de connexion », *in Les fichiers de police,* Institut Universitaire Varenne, coll. « Colloques & Essais », Paris, 2019.

HENNEBEL (L.), VANDERMEERSCH (D.), « Les mesures d'investigation et les droits de l'homme », *in Juger le terrorisme dans l'Etat de droit,* Bruylant, coll. « Magnacarta », Bruxelles, 2009.

IV. Rapports

CNCTR, *Rapport d'activité pour l'année 2023*, La documentation française, Paris, 2023.

Étude d'impact, Projet de loi (n°2669) relatif au renseignement, enregistré à la présidence de l'Assemblée nationale le 18 mars 2015.

Étude d'impact, Projet de loi (n°463) de programmation 2018-2022 et de réforme pour la justice enregistrée à la présidence de l'Assemblée nationale le 19 avril 2018.

Étude d'impact, Projet de loi (n°1033) relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense enregistrée à la présidence de l'Assemblée nationale le 4 avril 2023.

V. Articles

BLAY-GRABARCZYCK (K.), « Vie privée et nouvelles technologies », *RDLF,* 2011, chron. n° 7.

CNIL, Directive « Police-Justice » : de quoi parle-t-on ?, 20 février 2019.

CLUSIF, « Les essentiels : Bug Bounty FAQ », novembre 2023, consulté le 21 janvier 2025.

LASSALE (M.) :

- « L'affaire EncroChat », *Recueil Dalloz*, 2023, p. 1833.
- « La phase supranationale de l'affaire EncroChat », *Recueil Dalloz*, 2025, p. 1195.

THOMAS (S.), FRANCILLON (A.), "Backdoors: Definition, Deniability & Detection", *Research in Attack, Intrusions and Defenses: 21st International Symposium,* 10 septembre 2018.

RAVIGNEAUX (CH.), « Atteintes aux intérêts fondamentaux de la Nation », Répertoire de droit international, Recueil Dalloz – Février 2019.

IONOS, « Débogueurs : des outils essentiels pour la recherche des erreurs dans un logiciel », 13 octobre 2020, consulté le 28 janvier 2025.

CYBERUNIVERSITY, « Bug Bounty : définition et comment participer ? », 12 décembre 2022, consulté le 21 janvier 2025.

Ledieu avocat, « Le droit de pentester l'hébergeur du pentesté en 2023 ? », 05 janvier 2023, consulté le 21 janvier 2025.

DESTAL (M.), « Filature, cyberespionnage… La surveillance hors norme subie par Ariane Lavrilleux », *Disclose*, 04 décembre 2024.

VI. Conclusions, notes et commentaires

ROQUES (A.), « Trafic de moyens et atteintes aux STAD : précisions sur les éléments constitutifs », 7 février 2020, *Dalloz Actualité.*

VENTURA (D.), « L'acquisition de données de communications électroniques par les autorités de renseignement à l'épreuve de la directive "e-privacy" 2002/58/CE », *RDLF,* 2020, chron. N° 22.

VII. Textes officiels

A. Textes internationaux et européens

- Union européenne

Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000, *JOCE* C 364/01,.

Décision-cadre (2002/584/JAI) du Conseil du 13 juin 2022 relative au mandat d'arrêt européen et aux procédures de remise entre États membres, *JOUE* L 190, 18 juillet 2002.

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), *JOUE* L 201, 31 juillet 2002 (directive Vie-Privée).

Traité sur l'Union européenne (TUE) (version consolidée) du 13 décembre 2007, *JOUE* C 326/1326 octobre 2012.

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, *JOUE* L. 218/8, 14 août 2013 (Directive 2013/40).

Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, *JOUE* L 130, 1 mai 2014 (Directive 2014/41).

Règlement (UE) 2015/479 du Parlement européen et du Conseil du 11 mars 2015, relative au régime commun aux exportations, *JO* L 83 du 27 mars 2015 (Règlement 2015/479)

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, *JOUE* L 119, 4 mai 2016 (Directive Police-Justice).

Traité sur le fonctionnement de l'Union européenne (TFUE) (version consolidée) du 25 mars 1957, *JOUE* 7 juin 2016.

Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif, *JO* L 26, 31 janvier 2018.

Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relative à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n°526/201, *JO* L 151, 7 juin 2019 (Règlement sur la cybersécurité).

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 (refonte), *JO* L 206, 11 juin 2021 (Règlement Double Usage).

Proposition de règlement 2022/0155 du Parlement européen et du Conseil du 11 mai 2022 établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants COM(2022)209.

Avis conjoint 4/2022 de l'EDPB et du CEPD adopté le 28 juillet 2022, sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfant.

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) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, *JO* L 333, 27 juin 2022 (Directive SRI II).

Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n°1060/2009, (UE) n°648/2012, (UE)n°600/2014, (UE) n°909/2014 et (UE) 2016/1011, *JO L* 333, 27 décembre 2022 (Règlement 2022/2554).

Recommandation du Parlement européen du 15 juin 2023 à l'intention du Conseil et de la Commission à la suite de l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (2023/2500(RSP)).

Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement sur la liberté des médias), *JOUE* L, 17 avril 2024 (Règlement sur la liberté des médias).

Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des

éléments numériques et modifiant les règlement (UE) n°168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828, *JOUE* L, 20 novembre 2024 (Règlement sur la cyberrésilience).

- Conseil de l'Europe

Convention STE n°185 du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité, Budapest (Convention sur la cybercriminalité).

Recommandation n°R(89)9 du Comité des Ministres aux États membres sur la criminalité en relation avec l'ordinateur (Adoptée par le Comité des Ministres le 13 septembre 1989 lors de la 428e réunion des Délégués des Ministres).

Recommandation n°R(95)13 du Comité des Ministres aux États membres relative aux problèmes de procédure pénale liées à la technologie de l'information (Adoptée par le Comité des Ministres le 11 septembre 1995 lors de la 543e réunion des Délégués des Ministres).

Convention (STCE n°005) du Conseil de l'Europe du 4 novembre 1950, de sauvegarde des droits de l'homme et des libertés fondamentales, (Convention EDH).

- International

Pacte international relatif aux droits civils et politiques des Nations Unies, adopté à New York le 16 décembre 1966.

Joint statement Europol and ENISA on lawful criminal investigation that respects 21 st Century data protection, 20 mai 2016.

Convention A/79/460 sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles de l'Assemblée générale des Nations Unies, du 27 novembre 2024.

B. Textes nationaux

- Lois

Loi n°71-498 du 29 juin 1971 relative aux experts judiciaires, *JORF* du 30 juin 1971.

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique, *JORF* du 6 janvier 1988.

Loi n°92-685 du 22 juillet 1992 portant réforme des dispositions du Code pénal relatives à la répression des crimes et de délits contre les biens, *JORF* n°169 du 23 juillet 1992.

Loi n°96-647 du 22 juillet 1996 tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de

service public et comportant des dispositions relatives à la police judiciaire, *JORF* n°170 du 23 juillet 1996.

Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, *JORF* n°266 du 16 novembre 2001.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, *JORF* n°0143 du 22 juin 2004.

Loi n°2005-493 du 19 mai 2005 autorisation l'approbation de la Convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (1), *JORF* n°116 du 20 mai 2005.

Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité (1), *JORF* N°0062 du 15 mars 2011.

Loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité, *JORF* n°0075 du 28 mars 2012.

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 (1), *JORF* n°0294 du 19 décembre 2013.

Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, *JORF* n°0263 du 14 novembre 2014.

Loi n°2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n°0171 du 26 juillet 2015.

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, *JORF* n°0129.

Loi n°2016-1321 du 7 octobre 2016 pour une République numérique (1) *JORF* n°0235 du 8 octobre 2016.

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 (1), *JORF* n°0048 du 27 février 2018.

Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, *JORF* n°0071 du 24 mars 2019.

Loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, *JORF* n°0176 du 31 juillet 2021.

Loi n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (1), *JORF* n°0021 du 25 janvier 2023.

Loi n°2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, *JORF* n°0177 du 2 août 2023.

Loi n°2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic, *JORF* n°0137 du 14 juin 2025.

- Ordonnances

Ordonnance n°58-1270 du 22 décembre 1958 portant loi organique relative au statut de la magistrature, *JORF* du 23 décembre 1958.

- Décrets

Décret n°2002-1073 du 7 août 2002 d'application de l'article 30 de la loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d'assistance, *JORF* 5 janvier 2002.

Décret n°2014-445 du 30 avril 2014 relatif aux mission et à l'organisation de la direction générale de la sécurité intérieure, *JORF* n°0102 du 2 mai 2014.

Décret n°2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, *JORF* n°0225 du 29 septembre 2015.

Décret n°2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L811-4 du code de la sécurité intérieure, *JORF* n°0288 du 12 décembre 2015.

Décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale, *JORF* n°0295 du 20 décembre 2015.

Décret n°2016-1337 du 7 octobre 2016 portant changement d'appellation de la direction de la protection et de la sécurité de la défense, *JORF* n°0236 du 9 octobre 2016.

Décret n°2017-1095 du 14 juin 2017 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme, *JORF* n°0139 du 15 juin 2017.

Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, *JORF* n°0118 du 25 mai 2018.

Décret n°2023-1013 du 2 novembre 2023 relatif aux services déconcentrés et à l'organisation de la police nationale, *JORF* n°0255 du 3 novembre 2023.

Décret n°2023-1109 du 29 novembre 2023 modifiant diverses dispositions relatives à la police nationale, *JORF* n°0277 du 30 novembre 2023.

- Arrêtés

Arrêté du 29 octobre 2007 portant création d'un service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières, modifié par arrêté du 8 mars 2024, *JORF* n°270 du 21 novembre 2007.

Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal, *JORF* n°0177 du 1 août 2012

Arrêté du 17 juillet 2015 déterminant les services de l'État mentionnés au second alinéa de l'article L.2321-2 du code de la défense, *JORF* n°0173 du 29 juillet 2015.

Arrêté du 30 mars 2016 portant organisation de la direction du renseignement militaire, *JORF* n°0083 du 8 avril 2016.

Arrêté du 9 mai 2018 portant création du service à compétence nationale dénommé « service technique national de captation judiciaire », *JORF* n°0107 du 10 mai 2018.

- Avis et délibérations

Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République, Avis n°608 du 11 février 2003 sur le projet de Loi (n°528) pour la confiance dans l'économie numérique.

Commission d'enrichissement de la langue française, Avis divers n°108, Vocabulaire de la défense (liste de termes, expressions et définitions adoptés), *JORF* n°0299 du 11 décembre 2020.

Commission nationale de contrôle des techniques de renseignement, Délibération n°2/2021 du 7 avril 2021 sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

VIII. Jurisprudences

A. Jurisprudences nationales

Cons. Const., 16 juillet 1996, n°96-377 DC, *Loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire.*

Cons. Const., 8 décembre 2017, n°2017-680 QPC, *Indépendance des magistrats du parquet.*

Cons. Const. 8 avril 2022, n°2022-987 QPC, *Conditions de recours aux moyens des services de l'État soumis au secret de la défense nationale dans le cadre de certaines procédures pénales.*

Cons. Const., 12 juin 2025, n° 2025-885, DC, *Loi visant à sortir la France du piège du narcotrafic*.

C.cass., ch. crim., 26 octobre 1967, n°92-25.566.

C.cass, ch. crim., 16 janvier 1990, n°89-83-075.

C.cass., ch. crim., 7 octobre 1997, n°96-81.485.

C.cass., ch. crim., 8 décembre 1999, n° 98-84.752.

C.cass., ch. crim., 20 mai 2015, n°14-81.336.

C.cass., ch. civ., 17 mars 2016, n°15-14.072.

C.cass., ch. crim., 16 janvier 2018, n°16-87.168.

C.cass., ch. crim., 7 janv. 2020, n°18-84.755.

C.cass., ch. crim., 24 mars 2020, n°19-82.069.

C.cass., ch. crim., 5 avril 2022, n°21-83.590.

CA Besançon, 5 janvier 1978, n°9999.

CA Paris, 11e ch., 17 décembre 2001, n°00-077565.

CA Paris, 12e ch., 30 octobre 2002, n°02/04867, *Tati c. Kitetoa.*

CA Douai, 11 mai 2023, n°15-06278.

C.E, Ass., 21 avril 2021, *French Data Network et autres,* n°393099.

B. Cour européenne des droits de l'homme

CEDH, 26 mars 1987, *Leander c. Suède*, n°9248/81.

CEDH, 27 septembre 2005, *Petri sallinen et autres c. Finland,* n°50882/99.

CEDH, 16 octobre 2007, *Wiser et bicos beteiligungen gmbh c. Autriche*, n°74336/01.

CEDH, 22 mai 2008, *Iliya stefanov c. Bulgarie,* n°65755/01.

CEDH, 29 mars 2010, *Medvedyev et autres c. France*, n°3394/03.

CEDH, 4 décembre 2015, *Roman Zakharov c. Russie*, n°47143/06.

CEDH, 05 septembre 2017, *Barbulescu c. Roumanie*, n°61496/08.

CEDH, 11 février 2020, *Burutuga c. Roumanie*, n°56867/15.

CEDH, 25 mai 2021, *Big brother watch c. Royaume-Uni*, n°58170/14, n°62322/14, n°24960/15.

CEDH, 16 novembre 2021, *Särgava c. Estonie*, n°698/19.

CEDH, 13 février 2024, *Podchasov c. Russie*, n°33696/19.

CEDH, 24 septembre 2024, *A.L. et E.J c. France*, n°44715/20 et n°47930/21.

C. Cour de justice de l'Union européenne

CJUE, gr. ch., 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner,* n°C-362/14.

CJUE, gr. ch., 6 octobre 2020, *La Quadrature du net, French data Network, Fédération des fournisseurs d'accès à internet associatifs, Igwan.net c. Premier ministre, Garde des Sceaux, ministre de la Justice, ministre de l'Intérieur, ministre des Armées,* n°C-511/18 et C-512/18.

CJUE, gr. ch., 30 avril 2024, *M.N,* n°C-670/22.

CJUE, gr. ch., 4 octobre 2024, *CG c. Bezirkshauptmannschaft Landeck,* n°C-548/21.