

RAPPORT

À L'ATTENTION DE M. LE PREMIER MINISTRE

LES POLITIQUES PUBLIQUES DE SECURITE A L'ERE NUMERIQUE

Établi par M. Florent BOUDIÉ

LETTRE DE MISSION DE M. LE PREMIER MINISTRE

Le Premier Ministre

-- 81 / 26 SG

Paris, le 19 JAN. 2026

Monsieur le Président,

chr Florent,

Le chiffrement de bout en bout (*end-to-end encryption*) contribue directement à la protection des données sensibles de leurs utilisateurs et à la protection de la vie privée de nos concitoyens. Pour autant, il peut également faire obstacle aux enquêtes portant sur des infractions graves ou visant à prévenir les atteintes aux intérêts fondamentaux de la Nation.

Les solutions de messagerie chiffrée offertes au grand public sont en effet couramment utilisées par les organisations terroristes et criminelles notamment celles liées au narcotrafic. C'est le cas des centrales d'achat de produits stupéfiants sur les réseaux sociaux où les trafiquants disposent de boucles de clients auprès desquels ils assurent la promotion de leur offre commerciale, sa vente et sa livraison. Par ailleurs, plusieurs affaires impliquant des tueurs à gage ont permis de constater le recrutement d'exécutants par ces plateformes et ensuite l'utilisation exclusive de ce type de messageries pour communiquer entre donneurs d'ordres et exécutants.

Historiquement, l'organisation des communications était un monopole d'État. L'apparition d'opérateurs privés, notamment avec le développement de la téléphonie mobile, n'a pas remis en cause l'impératif de préserver le besoin légitime d'interception des correspondances au profit de la conduite des enquêtes pénales et de la sauvegarde des intérêts fondamentaux de la Nation.

Les opérateurs qui proposent des services de communication sur le territoire national sont soumis à une obligation générale en matière d'interception au bénéfice de la conduite des enquêtes judiciaires ou des services de l'État habilités par la loi. Le code des postes et des communications électroniques dispose en effet à son article L.33-1 que « L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont libres sous réserve du respect de règles portant sur [...] les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique ».

Ces interceptions de communication peuvent être judiciaires, autorisées par un magistrat de l'ordre judiciaire et ayant vocation probatoire, ou bien administratives autorisées par le Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignements (CNCTR), autorité administrative indépendante.

...

Monsieur Florent BOUDIÉ
Président de la Commission des Lois
Assemblée nationale
126 rue de l'Université
75007 PARIS

2.

Les opérateurs proposant des services de messagerie chiffrée sont par ailleurs soumis à un cadre juridique : en matière administrative, l'article L.871-1 du code de la sécurité intérieure crée une obligation pour les « *personnes physiques ou morales qui fournissent des prestations de cryptologie (...) de remettre dans un délai de soixante-douze heures (...) les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies* ». Le refus de satisfaire à cette obligation est passible de deux ans d'emprisonnement et de 150 000 € d'amende.

Néanmoins, ce dispositif se trouve aujourd'hui privé d'effet : dans un contexte où les opérateurs mettent en œuvre du chiffrement de bout en bout, ceux-ci affirment ne pas détenir les clés cryptographiques qui permettraient de remettre le contenu en clair, c'est-à-dire les conventions de déchiffrement dont la remise aux services concernés est prévue par la loi. Ils invoquent ainsi une impossibilité technique inhérente à la conception même de leurs services. Les opérateurs espèrent ainsi que les administrations se contentent de leurs déclarations.

La difficulté rencontrée avec ces messageries chiffrées devrait s'accroître avec la norme qui remplace les SMS, le RCS (Rich Communication Services). Ce protocole, adopté à l'échelle internationale, intègre des fonctionnalités de chiffrement de bout en bout et permet l'échange de messages écrits, vocaux et vidéos.

Cette situation illustre un véritable dilemme de politique publique : concilier la nécessité d'un accès légal et légitime aux communications dans le cadre du renseignement et des enquêtes judiciaires, avec l'impératif tout aussi fondamental de préserver la robustesse des technologies de communication utilisées quotidiennement par nos concitoyens, par les entreprises, par les opérateurs essentiels ou vitaux et par l'État lui-même.

A ce titre, j'ai décidé de vous confier une mission visant à établir un état des lieux de la situation et du droit positif ainsi que des possibilités d'évolution des dispositifs juridiques existants. Vous veillerez en particulier à :

1. réaliser un état des lieux des besoins des services de renseignement, des services d'enquête et des autorités judiciaires, ainsi qu'une cartographie des risques existant pour la sécurité des Français et la protection des intérêts fondamentaux de la Nation.
2. effectuer une synthèse comparative de la situation au niveau international, notamment via le parangonnage des solutions existantes dans d'autres pays (Royaume-Uni, Etats-Unis, Canada, Australie, Allemagne, Suède).
3. analyser l'impact de la réglementation existante et en projet au niveau de l'Union européenne. Devront être pris en compte, dans ce contexte, les textes et travaux suivants :
 - les impacts de la directive vie privée et communications électroniques (ePrivacy), mais aussi de la proposition de règlement abus sexuels sur mineurs (ASM), en cours de négociation et par laquelle les plateformes pourraient, en l'état actuel des négociations sur le texte, analyser les messages privés afin de détecter certains contenus illégaux, notamment en lien avec la pédopornographie ;
 - les travaux du groupe d'experts européens de haut niveau sur l'accès aux données par les forces de l'ordre (HLEG), créé sous présidence suédoise en juin 2023 pour faire face à l'importance croissante de la dimension numérique de la criminalité organisée ;

.../...

3.

- enfin, la stratégie de sécurité intérieure 2026-2030, publiée le 1^{er} avril 2025, qui annonce une feuille de route avant la fin du premier semestre 2026, une étude d'impact sur la conservation des données, une feuille de route technologique sur le chiffrement, doit également faire l'objet d'une attention forte.

Ces différents éléments soulignent que le sujet doit aussi être regardé à l'échelle de l'UE car, sans préjudice des solutions nationales, il reste nécessaire, pour être pleinement efficace, de réfléchir à des pistes d'action s'appliquant à l'ensemble du marché intérieur.

4. Sur cette base, engager une réflexion approfondie sur les leviers d'action à l'échelle européenne, dans le cadre judiciaire, incluant par exemple l'identification de pistes de « manœuvres européennes » permettant une action coordonnée sur le chiffrement et l'accès légal aux données.
5. En vous appuyant sur les travaux menés sous l'égide du SGDSN et de la CNRLT, à la demande du Président de la République, proposer des pistes de réflexion et de travail, tant dans le domaine normatif (législatif et réglementaire) que non normatif (institutionnel, technique, méthodologique, doctrinal) afin de préserver l'accès nécessaire et encadré aux communications dans le cadre de la lutte contre le terrorisme et la criminalité organisée.
6. Étudier la portée effective des dispositifs normatifs envisagés.

Vos recommandations contribueront à répondre aux objectifs prioritaires de protection des intérêts fondamentaux de la Nation et de nos concitoyens dans le cadre préservant les libertés fondamentales de chaque citoyen et les infrastructures numériques du pays.

Vous veillerez à procéder à une large consultation des acteurs concernés qu'il s'agisse des différents ministères concernés (intérieur, justice, armées, économie, numérique), du SGDSN, du SGAE, des autorités indépendantes et des acteurs du secteur privé. Vous pourrez bien entendu vous appuyer autant que de besoin sur les services de l'État et plus particulièrement ceux du ministère de l'intérieur et du ministère de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique pour mener à bien votre mission.

Vous me remettrez vos travaux d'ici trois mois.

Vous veillerez à élaborer vos propositions dans le respect des règles d'indépendance, d'impartialité et d'objectivité qui s'imposent au titre de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, et à m'informer des éventuelles mesures prises à cet effet.

En application de l'article L.O.144 du code électoral, un décret vous nommera parlementaire en mission auprès M. Laurent NUÑEZ, ministre de l'intérieur, et de M. Roland LESCURE, ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique.

Je vous remercie par avance pour votre engagement au sein de cette mission et vous prie de croire, Monsieur le Président, à l'assurance de mes salutations les meilleures.

A-tion,

Sébastien LECORNU

SYNTHESE

En réduisant l'accès des services de renseignement et d'enquête judiciaire au contenu des communications, le chiffrement « de bout en bout » confronte les politiques de sécurité publique à un défi inédit à l'ère numérique.

Pour l'État, le défi est d'abord sécuritaire : de nouvelles formes de criminalité prospèrent sur l'usage d'outils numériques protégés par le chiffrement, au point de favoriser l'affirmation d'un écosystème criminel numérique à la fois protéiforme et préoccupant.

Pour les services de l'État, le défi est opérationnel : les techniques de renseignement et d'enquête numérique judiciaire sont dès à présent contraintes de migrer vers les données qui demeurent accessibles hors chiffrement, interrogeant notre cadre juridique comme nos outils capacitaires.

Dans le même temps, le chiffrement est devenu une composante indispensable de la sécurité numérique et de la confidentialité des échanges. Or, dans un contexte de massification des échanges numériques et de cybermenaces accrues et hybrides, il n'existe pas, en l'état de la technologie disponible, de solutions alternatives au chiffrement « de bout en bout » permettant d'assurer, à grande échelle, la sécurité et la robustesse des systèmes d'information.

La réponse publique doit, dès lors, à l'échelle nationale comme européenne, poursuivre une double exigence : poser la question de l'accès aux données protégées par le chiffrement « de bout en bout », dans le but de prévenir et réprimer les infractions les plus graves, sans toutefois compromettre la sécurité des échanges numériques ni créer des risques nouveaux pour nos libertés publiques. Le Conseil européen de l'Union européenne a pu résumer ce dilemme par la formule suivante : « *la sécurité grâce au chiffrement et malgré le chiffrement* ».

Dans cette perspective, la mission propose une stratégie articulée autour de trois orientations.

La première consiste à renforcer la position de l'État à l'égard des plateformes en leur imposant de nouvelles obligations de transparence et en rendant plus effectives les procédures permettant de sanctionner les comportements non coopératifs.

La seconde consiste à préserver la capacité de la France à promouvoir, à l'échelle européenne, des règles harmonisées applicables aux plateformes, en écartant les initiatives nationales qui figeraient sa position dans les négociations en cours et dont les effets sur les politiques publiques de sécurité seraient au mieux sans effet, au pire délétères.

Enfin, cette stratégie doit s'accompagner d'un réengagement du dialogue avec les plateformes, sans naïveté. D'abord, sur des avancées mesurées mais concrètes, par exemple dans le domaine du traitement des réquisitions administratives et judiciaires dont elles font l'objet. Ensuite, sur le plan des capacités techniques, en renforçant celles de l'État à identifier, prototyper et éprouver des solutions permettant un accès ciblé aux contenus, sans affaiblir le chiffrement ni compromettre la sécurité numérique et la confidentialité des échanges.

SOMMAIRE

I) Un défi sécuritaire pour l'État : les mutations de la criminalité par le chiffrement	9
A) La généralisation de la confidentialité : une innovation et un choix de politique publique	10
1) Un standard porté par l'enjeu de sécurité des contenus	10
a) L'affirmation d'un nouveau modèle de sécurité des échanges numériques	10
• Première étape : les algorithmes cryptographiques de chiffrement des données (DES, AES)	10
• Deuxième étape : les protocoles de chiffrement du transport des données (SSL, TLS)	11
• Troisième étape : le principe du « end-to-end » et le déplacement des clés vers les utilisateurs	11
b) La diffusion du chiffrement à l'ensemble des communications numériques	12
• L'effondrement des modes de communication accessibles aux enquêteurs	12
• Le chiffrement poursuit son extension vers les modes traditionnels de communication	14
2) Un standard encouragé par la puissance publique	17
a) La complexité de la cybermenace justifie l'adoption de solutions robustes	17
• Le contexte général de la montée de la cybermenace	18
• Les exfiltrations de données, le ciblage des terminaux et les chocs futurs émergents	19
b) Le chiffrement, une garantie pour la sécurité numérique et les libertés	20
• Une priorité pour la cybersécurité et la souveraineté technologique	21
• Un instrument de protection des droits fondamentaux	23
B) Le recours au chiffrement a gagné l'ensemble du spectre infractionnel	25
1) Un outil désormais banalisé dans la délinquance dite « de masse »	25
a) L'omniprésence des données numériques dans toutes les formes de délinquance	25
• Le révélateur des violences intrafamiliales	26
b) La confidentialité est un critère d'usage prioritaire pour les auteurs d'infractions	27
• Le cas emblématique des « petites mains » du trafic de stupéfiants	27
• Un facteur de convergences inédites entre délinquance du quotidien et crime organisé	29
2) Le chiffrement comme infrastructure d'écosystèmes criminels intégrés	31
a) L'intégration de services numériques dans une chaîne criminelle complète	32
• L'internalisation de fonctions criminelles numériques	32
• L'externalisation de fonctions criminelles numériques	34
b) La création de services numériques à vocation spécifiquement criminelle	35
• L'affaire EncroChat, un succès français éclairant les nouveaux modes opératoires	35
• L'émergence de criminels « digital natives »	37
II) Un défi opérationnel pour les services : adapter les capacités d'accès aux données	38
A) Le modèle d'accès légal aux communications à l'épreuve du chiffrement	39
1) L'obligation de coopération imposée aux opérateurs de communication électroniques	40
a) Les obligations imposées pour l'interception et la conservation des données	40
• Les obligations techniques mises à la charge des opérateurs et des fournisseurs	40
• Des durées de conservation variables selon la nature des données et leurs finalités	42
b) Les garanties exigées par le droit interne et le droit de l'Union européenne	42
2) La dualité des régimes d'accès aux communications électroniques	43
a) Les régimes administratifs et judiciaires d'accès aux communications électroniques	44
• Le cadre propre au renseignement	44

• Le régime judiciaire : la dématérialisation accélérée de l'enquête pénale	48
b) Un principe d'effectivité aux effets limités appelant des aménagements.....	58
B) La perte d'accès au contenu réoriente les voies d'accès à l'information pour les enquêteurs	61
1) Le droit cède le pas devant la disponibilité technique des données	62
a) Les données en clair dépendent de leur détention par les fournisseurs	62
b) Le « going dark » ou l'approche fondée sur les données encore disponibles.....	63
• L'importance prise par le recueil des données de connexion	64
• La montée en puissance du recueil de données informatiques.....	64
2) La « nouvelle économie des investigations » demeure imparfaite	65
a) Les opérateurs et les OTT doivent répondre à des exigences de transparence	65
• Contenir les stratégies de « data minimisation » qui pèsent sur la disponibilité des métadonnées ...	65
• Organiser l'obligation de transparence sur les métadonnées effectivement détenues	67
• Faire la lumière sur les réponses aux réquisitions administratives et judiciaires	68
b) Les capacités des services doivent être renforcées	71
• Le volume des données collectées appelle une stratégie de retraitement renforcée.....	71
• Les réflexions à conduire sur les techniques de recueil et de captation des données informatiques.....	73
III) Conclusion : Face aux tensions sur le chiffrement, repenser la relation aux plateformes	77
A) Les clivages autour du chiffrement doivent être dépassés.....	77
1) Un débat hélas binaire : pour le chiffrement, tapez « 16 bis » ; contre, tapez « 8 ter »	77
2) L'article 16 bis du projet de loi « résilience » : de très nombreuses réserves juridiques	79
B) Une double approche à construire avec les plateformes, coopérative et contraignante	82
1) Une meilleure coopération avec les acteurs numériques doit être engagée	83
• Renouer avec l'esprit de 2015 et le « groupe de contact permanent »	83
• Développer et confronter des solutions techniquement neutres d'accès aux données.....	83
2) Un déchiffrement forcé n'emporterait aucun avantage pour les politiques de sécurité	87

Liste des recommandations de la mission

- 1) Favoriser l'émergence d'un programme pluridisciplinaire de recherche pour documenter la transformation des activités criminelles à l'heure du numérique et des communications chiffrées.
- 2) Achever l'adaptation du régime des réquisitions judiciaires de données de connexion aux exigences du droit de l'Union européenne en instaurant un contrôle par une autorité indépendante.
- 3) Engager une refonte du cadre juridique des techniques d'enquête numérique judiciaire, afin d'en renforcer la cohérence, la lisibilité et la sécurité juridique pour les enquêteurs et de mieux proportionner les garanties applicables.
- 4) Rehausser le niveau des sanctions financières en cas de non-réponse aux réquisitions judiciaires adressées à une plateforme numérique.
- 5) Créer une obligation de communiquer les éléments justifiant l'impossibilité de remettre ou mettre en œuvre les conventions de déchiffrement, et sanctionner les manquements à cette obligation.
- 6) Faire de la préservation de la disponibilité des métadonnées un objectif stratégique à part entière face aux politiques de « *data minimisation* » déployées par les opérateurs et les fournisseurs.
- 7) Imposer aux plateformes une obligation d'information et de transparence des données qu'elles détiennent et conservent effectivement.
- 8) Instaurer un dispositif national, permanent et interministériel de suivi de l'exécution des réquisitions administratives et judiciaires adressées aux opérateurs de communication et aux fournisseurs de services.
- 9) Soumettre les plateformes à une nouvelle obligation de publication d'indicateurs harmonisés sur l'exécution des réquisitions qui leur sont adressées.
- 10) Établir une doctrine de réquisition tenant compte du rôle de chaque acteur dans la chaîne de gestion de la donnée de contenu des messageries chiffrées.
- 11) Créer une agence nationale chargée du développement et de la coordination de la stratégie en matière de retraitement des données numériques collectées dans le cadre des enquêtes administratives et judiciaires.
- 12) Créer une direction technique nationale rattachée aux ministères de l'intérieur et de la justice pour la conception, le développement et la certification des dispositifs techniques de recueil des données informatiques.
- 13) Instaurer, en matière de renseignement, un régime juridique gradué du recueil de données informatiques reposant sur un socle commun de garanties et des exigences adaptées au degré d'intrusion des différentes modalités de captation.
- 14) Renoncer aux dispositions de l'article 16 bis du projet de loi « résilience », compte tenu des sérieuses zones d'ombre juridiques qu'emporterait sa rédaction actuelle.
- 15) Engager un dialogue structuré et permanent entre l'État et les acteurs du numérique afin d'améliorer les conditions de leur coopération opérationnelle.
- 16) Constituer une *task force* interministérielle, pilotée par la CNRLT et le SGDSN, pour identifier, concevoir et évaluer les solutions techniquement neutres envisageables pour permettre l'accès aux contenus à caractère criminel et terroriste.
- 17) Écarter toute disposition comparable à l'ancien article 8 ter tant que n'a pas été établie la faisabilité d'une solution technique permettant un accès ciblé aux contenus protégés sans affaiblir le chiffrement ni la sécurité des systèmes numériques.

I) Un défi sécuritaire pour l'État : les mutations de la criminalité par le chiffrement

Véritable rupture dans l'économie des communications électroniques, la généralisation du chiffrement, et plus particulièrement du chiffrement « de bout en bout » ou *E2EE*¹, a profondément transformé les conditions dans lesquelles s'exercent les politiques publiques de sécurité.

La mise à la disposition des auteurs d'infractions d'espaces numériques dont le contenu échappe, par construction technique, aux capacités d'investigation des services de renseignement et d'enquête judiciaire, engendre un défi inédit. Initialement cantonné à des activités criminelles spécialisées, l'usage des communications chiffrées s'étend désormais à l'ensemble du spectre infractionnel, de la délinquance de « droit commun » aux formes les plus menaçantes et organisées de criminalité, contribuant à créer **un nouvel écosystème numérique criminel**.

Ce défi sécuritaire procède toutefois d'un paradoxe.

Si la diffusion du chiffrement « de bout en bout » neutralise une partie des prérogatives de puissance publique, elle résulte, dans le même temps, de choix de politiques publiques anciens et assumés, en France comme ailleurs, visant à protéger les citoyens et les entreprises, les infrastructures critiques et les systèmes d'information (SI), en préservant l'intégrité des données stratégiques et personnelles. Ainsi, encouragés à promouvoir le perfectionnement des procédés cryptologiques, à l'image des orientations du Secrétariat général de la Défense et de la Sécurité nationale (SGDSN) présentées dans sa *Stratégie nationale de cybersécurité 2026-2030*², les services de l'État sont tout autant invités à percer le « mur du chiffrement ».

La résolution du Conseil de l'Union européenne du 24 novembre 2020 résumait ce dilemme, auquel l'ensemble des États membres de l'Union européenne est confronté, par cette formule : « **la sécurité grâce au chiffrement et malgré le chiffrement** »³.

Le débat est d'ailleurs ancien. Dès 2017, la Commission nationale de l'informatique et des libertés (CNIL) observait qu'« *à la suite des attentats intervenus en 2015 et 2016, plusieurs autorités publiques [affichaient] des positions défavorables au chiffrement. Confrontées à des matériels chiffrés à la main de l'utilisateur (...), les autorités judiciaires [avaient] en effet des difficultés substantielles à accéder à des informations pourtant nécessaires à leurs enquêtes, portant sur des faits particulièrement graves* »⁴. Cette problématique n'a fait depuis que s'accroître.

Aussi est-ce toute la difficulté de la tâche confiée à la présente mission : le chiffrement constitue, tout à la fois, un vecteur de sécurité numérique, de protection de libertés constitutionnellement garanties et une cause – d'une ampleur jusqu'alors inconnue – de complexité pour les nécessités d'ordre public, la recherche des auteurs d'infractions et la protection des intérêts fondamentaux de la Nation.

¹ Pour « *end-to-end encryption* ».

² SGDSN, *Stratégie nationale de cybersécurité 2026-2030*, 2026.

³ Résolution du Conseil de l'Union européenne n° 13084/1/20 du 24 novembre 2020.

⁴ CNIL, *L'accès des autorités publiques aux données chiffrées*, 30 août 2017.

A) La généralisation de la confidentialité : une innovation et un choix de politique publique

1) Un standard porté par l'enjeu de sécurité des contenus

Sans remonter à l'âge de pierre de la cryptologie, ni même à l'époque d'*Énigma* et des travaux d'Alan Turing à *Bletchley Park*, l'émergence de la cryptographie moderne prend sa source dans les années 1970, à l'aube de l'ère numérique. Mathématiciens, informaticiens et cryptographes⁵ développent alors des systèmes chiffrés pour protéger les données sensibles sous l'impulsion, principalement aux États-Unis, des pouvoirs publics.

a) L'affirmation d'un nouveau modèle de sécurité des échanges numériques

L'émergence du chiffrement « de bout en bout » comme standard des communications numériques résulte d'un processus d'évolution dont trois grandes étapes peuvent être détachées, chacune d'entre elles ayant permis de franchir un stade plus avancé de sécurisation des données.

- **Première étape : les algorithmes cryptographiques de chiffrement des données (DES, AES)**

Dans la désormais longue chaîne des évolutions cryptographiques, la technologie dite **Data Encryption Standard** (DES), issue d'un algorithme développé par *IBM*, avec l'appui technique de la *National Security Agency* (NSA), a marqué une étape importante. Adoptée en 1977 comme norme fédérale américaine par le *National Institute of Standards and Technology* (NIST), elle s'impose comme le principal standard de chiffrement, particulièrement dans le secteur financier, et vise à protéger les données dites « de valeur » pendant de leur transmission et leur stockage.

Destiné aux usages civils, alors que le chiffrement relevait auparavant des sphères militaires et du renseignement, le DES bouleverse les procédés cryptographiques en posant le principe selon lequel, dans un système véritablement protégé, **la méthode de chiffrement n'a pas à être secrète : seule la clé doit rester confidentielle**. Le DES est donc conçu comme un algorithme public dont la robustesse doit pouvoir être vérifiée par tous, tandis que la confidentialité des communications repose exclusivement sur la protection de la clé de chiffrement.

Face à l'augmentation de la puissance des ordinateurs, le NIST lance, en 1997, l'**Advanced Encryption Standard** (AES). Avec une ambition : produire des clés plus longues, reposant sur plusieurs milliards de milliards de combinaisons possibles, pour accroître la résistance du standard de sécurité et faire face à des attaques dites par « force brute » consistant à tester systématiquement toutes les clés possibles pour les percer. Si le DES et l'AES définissent la méthode pour chiffrer et déchiffrer des données, **les clés de chiffrement demeurent toutefois « à la main » des fournisseurs de services qui disposent de la capacité technique d'accéder au « clair »**.

⁵ L'émergence de la cryptologie moderne est généralement rattachée à la publication, en 1976, de l'article de W. Diffie et M. E. Hellman, *New Directions in Cryptography*, qui pose les fondements de la « cryptographie à clé publique » (cryptographie asymétrique). Cette rupture est suivie, en 1977, par l'élaboration du système *RSA*, acronyme formé des initiales de Ronald L. Rivest, Adi Shamir et Leonard M. Adleman, premier cryptosystème asymétrique, publié l'année suivante.

- **Deuxième étape : les protocoles de chiffrement du transport des données (SSL, TLS)**

Alors que le DES et l'AES visaient à chiffrer les données elles-mêmes, quel que soit leur support (données stockées ou acheminées), le chiffrement se déplace, dès les années 1990, vers le canal de communication entre deux points d'un réseau.

Le protocole **Secure Sockets Layer** (SSL), développé par *Netscape* dans les années 1990, puis le **Transport Layer Security** (TLS) qui lui succède en 1999 sous l'égide de l'*Internet Engineering Task Force* (IETF), née en 1986 dans le cadre de programmes fédéraux américains, garantissent la sécurisation des données pendant leur transport. Le but est alors de protéger les communications entre clients et serveurs, contre les tiers situés sur le réseau.

Dans les architectures mettant en œuvre le DES, l'AES ou le TLS, **le fournisseur de services, parce qu'il demeure une extrémité cryptographique de la communication, dispose d'un point de déchiffrement lui permettant d'accéder au contenu en clair**. L'effectivité des capacités d'investigation des services de renseignement et d'enquête judiciaire est par conséquent maintenue, jusqu'à la rupture introduite par le *E2EE*.

- **Troisième étape : le principe du « end-to-end » et le déplacement des clés vers les utilisateurs**

La première application de chiffrement « de bout en bout » destinée au grand public, dont la normalisation par l'IETF intervient en 1998 (*OpenPGP*⁶), sa mise en œuvre sur des messageries instantanée en 2004 (*Off-the-Record Messaging – OTR*), puis l'apparition de *Signal Protocol*⁷ en 2014, marquent une rupture technologique. **Les clés permettant de déchiffrer le contenu des communications sont alors détenues, non par les opérateurs et fournisseurs de services, mais par les seuls utilisateurs des terminaux informatiques.**

À destination de ses utilisateurs, *WhatsApp* peut ainsi définir le chiffrement « de bout en bout » comme « *des communications qui demeurent chiffrées depuis un appareil contrôlé par l'expéditeur jusqu'à un appareil contrôlé par le destinataire, possédant chacun les clés cryptographiques nécessaires pour chiffrer et déchiffrer les messages échangés entre eux* »⁸, sans accès du fournisseur (ou de *Meta*, en l'espèce) au contenu intermédiaire.

Cette propriété peut être mise en œuvre par différents protocoles. Dans *Signal Protocol*, les utilisateurs de terminaux établissent, entre eux seuls, un « secret cryptographique », à partir duquel sont générées de nouvelles clés pour chaque message. Dans *MLS*⁹, les membres d'un groupe établissent un « secret commun », dont sont dérivées les clés protégeant les échanges du groupe, lesquelles sont renouvelées dès lors que la composition du groupe évolue. Dans *OpenPGP*, chaque message est chiffré au moyen d'une clé de session générée pour ce message, elle-même transmise de manière sécurisée au destinataire, à l'aide de sa clé publique¹⁰.

⁶ *Open Pretty Good Privacy* est un protocoles de chiffrement « de bout en bout » conçu pour la sécurisation des courriers électroniques, de fichiers, de documents ou d'archives.

⁷ *Signal Protocol* est un protocole cryptographique de chiffrement « de bout en bout » conçu par la *Signal Foundation* pour les communications interpersonnelles.

⁸ *WhatsApp, WhatsApp Encryption Overview*, 25 février 2026.

⁹ *Messaging Layer Security* est un protocole conçu pour les communications de groupe.

¹⁰ La clé publique est l'une des deux clés d'un système cryptographique dit « asymétrique », lequel repose sur deux clés distinctes mais mathématiquement liées. La clé publique peut être librement diffusée, tandis que la clé privée demeure connue de son seul

Il résulte de l'architecture technique propre au chiffrement « de bout en bout » que les opérateurs et fournisseurs de services numériques ne constituent plus le point de déchiffrement : c'est précisément la raison pour laquelle le E2EE s'est imposé comme un standard de confidentialité et de sécurité en contexte de massification des communications numériques.

Le chiffrement « de bout en bout » marque ainsi l'extension du domaine de la confidentialité, allant des entités stratégiques, institutionnelles et professionnelles jusqu'aux échanges de la vie quotidienne.

b) La diffusion du chiffrement à l'ensemble des communications numériques

La généralisation du chiffrement se manifeste par un double mouvement de fond : d'un côté, l'effondrement des modes classiques de communication ; de l'autre, l'extension du chiffrement au-delà des seuls services « *over the top* » (OTT)¹¹ qui en ont industrialisé les applications.

- ***L'effondrement des modes de communication accessibles aux enquêteurs***

La période récente se caractérise par le déplacement massif des usages traditionnels (appels téléphoniques, SMS, MMS) vers des applications de messagerie et d'appel dont la plupart chiffrent de « bout en bout » les communications au moyen des standards les plus avancés.

Cette mutation est particulièrement vraie pour les messages dits « textuels », ainsi que le documente l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), dans son dernier état du marché¹².

L'usage des SMS s'est réduit de 11 % en 2024, avec un nombre de messages envoyés (SMS ou MMS) de 11 par mois pour les particuliers (- 15 messages par an) et de 50 par mois pour les entreprises (- 12 messages en un an). Désormais, **64% de la population française utilise quotidiennement des services de messagerie instantanée** pour l'échange de messages textuels (+12 points en 3 ans). Dans le même temps, 43% des appels vocaux sont passés par l'intermédiaire d'applications numériques (+13 points en 3 ans). Très marqués chez les plus jeunes (79% des 12-17 ans échantent chaque jour des messages textuels par ce moyen), ces usages ont toutefois gagné toutes les générations (73% des 25-39 ans et 70% des 40-49 ans)¹³.

Au demeurant, l'essor récent des messages dits « vocaux » pourrait à l'avenir accentuer cette prépondérance de la communication par contournement des télécommunications

titulaire. Les données chiffrées avec la clé publique ne peuvent être déchiffrées qu'au moyen de l'autre clé. La clé publique ne permet donc pas, à elle seule, d'accéder au contenu en clair des données protégées.

¹¹ Les services OTT, tels qu'iMessage, Facebook Messenger, Instagram, Snapchat, Viber, WeChat, Line, WhatsApp, Signal ou encore Telegram, désignent les services de communication fournis par Internet sans être eux-mêmes opérateurs des infrastructures de télécommunication utilisées pour acheminer les échanges. L'expression « *over the top* », née dans l'industrie des télécommunications, désigne ainsi les services fournis « par-dessus » les réseaux des opérateurs, sans que ces derniers contrôlent le service lui-même.

¹² ARCEP, *Les services de communications électroniques en France*, 9 octobre 2025.

¹³ CREDOC, *Baromètre du numérique, édition 2026*, février 2026.

traditionnels. Le nombre de messages vocaux transmis par la seule messagerie *WhatsApp* était ainsi estimé à 9,4 milliards par jour en 2024, contre 7 milliards en 2022¹⁴.

Que sont les « messageries instantanées » ?

En droit, les messageries communément qualifiées d'« instantanées » recouvrent la catégorie des « *services de communications interpersonnelles non fondés sur la numérotation* ». Il y est aussi fait référence sous l'appellation de services ou messageries « *par contournement* » ou « *over the top* » (OTT) ; lorsque les fournisseurs utilisent le chiffrement, la notion générique de « *messagerie chiffrée* » est employée. Le présent rapport les qualifiera, le plus souvent, de « fournisseurs de services » pour les distinguer des opérateurs de communications électroniques (OCE) historiques.

Cette évolution des usages trouve, en toute logique, son prolongement parmi les populations ciblées par les services de renseignement et d'enquête judiciaire.

Pour les seules interceptions judiciaires, l'Agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ) constate, d'une part, l'inversion rapide du *ratio* entre les appels vocaux échangés par les modes classiques et par les messageries sécurisées¹⁵ et, d'autre part, la diminution des communications traditionnelles (SMS, appels). Ainsi, la Plateforme nationale des interceptions judiciaires (PNIJ) interceptait 87 millions de communications par appels et SMS en 2020, contre 61 millions en 2024, dont une partie – difficilement quantifiable – est de surcroît liée à des activités commerciales sans intérêt pour les enquêteurs¹⁶.

Au total, les SMS et MMS ne représentent plus que 3% du volume total des messages échangés. Les 97% restants transitent désormais par des applications de messagerie telles que *WhatsApp*, *Facebook Messenger* et *WeChat*. Or, **90% des communications dites OTT sont protégées par un chiffrement « de bout en bout »**¹⁷.

Il faut prendre toute la mesure de cette évolution. Lorsque, d'une part, 97% des messages échangés sur les réseaux mobiles empruntent des applications de messagerie et que, d'autre part, 90% d'entre elles sont chiffrées « de bout en bout », les réquisitions administratives et judiciaires sont réduites à un angle d'observation étroit, fragmentaire et lacunaire des échanges numériques.

¹⁴ Source : étude commandée par l'entreprise *Heineken*, fondée sur les données de l'entreprise allemande de production de données statistiques *Statista*, dans le cadre d'un sondage réalisé auprès de 14 000 personnes dans sept pays, décembre 2025.

¹⁵ 56% des appels détectés par la Plateforme nationale des interceptions judiciaires (PNIJ), en octobre 2025, étaient des appels classiques, contre 51% en février 2026.

¹⁶ Les interceptions centralisées par la PNIJ ne portent pas sur l'intégralité des interceptions judiciaires de données numériques. Les données produites par les fournisseurs de services de messageries, qui n'y sont pas raccordés, suivent des procédures judiciaires *ad hoc*.

¹⁷ HLEG, *Concluding Report of the High-Level Group on Access to Data for Effective Law Enforcement*, rapport final adopté le 15 novembre 2024.

Exemples de messageries instantanées chiffrées « de bout en bout »		
Service	Date de création	Caractéristiques
Dust	N.C.	- Chiffrement « de bout en bout » par défaut pour les données au repos (protocole TLS pour les données en transit) ; - Fonctionnalités de confidentialité avancées (autodestruction des messages, détection des captures d'écran).
iMessage (Apple)	2011	- Chiffrement « de bout en bout » par défaut ; - Fonctionnalités de confidentialité avancées (autodestruction des messages).
Line	2011	- Chiffrement « de bout en bout » sur paramétrage.
Signal	2013	- Chiffrement « de bout en bout » par défaut ; - Fonctionnalités de confidentialité avancées (autodestruction des messages) ; - Code source ouvert, protocole de chiffrement public et auditable ; - Stockage local des données ; - Aucune collecte de métadonnées.
Telegram	2013	- Chiffrement « de bout en bout » possible (fonctionnalité « échange secret ») - Fonctionnalités de confidentialité avancées (autodestruction des messages)
Threema	2012	- Chiffrement « de bout en bout » pour tous les types de messages ; - Limitation des données stockées/gérées sur le serveur de l'entreprise ; - Code source ouvert et auditable ; - Inscription sans numéro de téléphone ni adresse électronique ; - Vérification des contacts par QR code ; - Service payant (usage unique ou abonnement).
Viber	2010	- Chiffrement « de bout en bout » sur paramétrage.
Whatsapp (Meta)	2009	- Chiffrement « de bout en bout » par défaut ; - Sauvegarde des données dans les <i>clouds</i> associés aux systèmes d'exploitation ; - Nécessite un numéro de téléphone pour l'inscription.
Wickr Me¹⁸ (Amazon)	2012	- Chiffrement « de bout en bout » par défaut ; - Fonctionnalités de confidentialité avancées (autodestruction des messages, détection des captures d'écran) ; - Code source ouvert et auditable ; - Suppression automatique des métadonnées.
Wire	2014	- Chiffrement « de bout en bout » par défaut ; - Code source ouvert et auditable ; - Inscription avec une adresse électronique, sans numéro de téléphone.
(Source : mission, à partir de données publiques)		

- **Le chiffrement poursuit son extension vers les modes traditionnels de communication**

Le modèle du chiffrement est appelé à connaître une nouvelle accélération. Dans le domaine des messages textuels, la concurrence entre les services de contournement, tels que *WhatsApp*, *Signal* ou *Telegram*, et les opérateurs de télécommunication traditionnels, tels qu'*Orange*, *SFR*, *Bouygues Telecom* et *FreeMobile*, historiquement fournisseurs des services SMS et MMS, contribue à la diffusion du chiffrement « de bout en bout »¹⁹.

¹⁸ Application fermée au grand public en 2023, recentrée sur les usages professionnels et renommée *AWS Wickr*.

¹⁹ Les télécommunications traditionnelles avaient déjà engagé un renforcement de la sécurité et de la capacité d'authentification des communications lors du déploiement du standard 5G. L'architecture 5G inclut, en effet, le chiffrement des données et l'utilisation de certificats numériques d'authentification des terminaux. La norme 5G NR ne propose cependant pas de chiffrement « de bout en bout ».

Devant l'argument devenu central de protection des systèmes d'information, et donc de différenciation réputationnelle et commerciale, **les opérateurs traditionnels cherchent en effet à développer des services aux fonctionnalités comparables aux communications « over the top ».**

Cette stratégie de rattrapage se traduit par la mise en place du **Rich Communication Services** (RCS), en remplacement des *Short Message Services* (SMS). Outre les fonctionnalités d'interaction (*emoji*, par exemple), le RCS permet le chiffrement « de bout en bout » des messages, au même titre que les services *OTT*. L'entreprise *SFR* indique avoir été le premier opérateur, en juillet 2024, à activer le RCS dans l'Hexagone suivie, en décembre 2024, par *Bouygues Telecom* et *Free Mobile*, à la faveur de la mise à jour d'*iOS 18.2* d'*Apple*²⁰.

Selon les données publiées par l'Association française pour le développement des services et usages multimédias multi-opérateurs (AF2M), le déploiement du protocole RCS était effectif, à la fin du mois d'avril 2025, chez les quatre opérateurs historiques, dont *Orange*. 83% du parc de *smartphones* français est désormais compatible avec cette technologie, soit plus de 50 millions d'appareils à la fin de l'année 2025. AF2M, qui représente les principaux opérateurs de communications électroniques (OCE), souligne ainsi que « *le RCS est désormais le canal le plus universel du marché* »²¹.

L'usage du chiffrement « de bout en bout » se diffuse également sur d'autres fonctionnalités. L'application *Gmail*, sur *Android* et *iOS*, propose, depuis le mois d'avril 2026, une option de chiffrement *E2EE* pour ses clients professionnels, alors que la messagerie employait jusqu'ici, de façon transversale, un chiffrement « en transit ».

Au chiffrement des flux, s'ajoute le chiffrement des terminaux informatiques et téléphoniques. Sur les *smartphones*, le chiffrement traditionnellement assuré par le code PIN, associé à la carte SIM, peut être complété de mots de passe ou schémas de déverrouillage²².

Une étape supplémentaire est franchie avec la commercialisation de **téléphones intégralement cryptés**²³. Conçus pour réduire au minimum la surface d'attaque, ces terminaux éliminent les fonctionnalités non essentielles et ne conservent que les appels et la messagerie, eux-mêmes protégés par des mécanismes cryptographiques. Leur niveau de sécurité peut alors être renforcé par des serveurs dédiés, réservés à des appareils préalablement identifiés. Cette technologie a été utilisée à des fins criminelles dans l'affaire dite *EncroChat*.

D'autres ruptures technologiques, potentiellement déterminantes, pourraient encore renforcer la sécurité des communications numériques : **les capacités des technologies quantiques sont d'ores et déjà mobilisées pour consolider les mécanismes de chiffrement et la sécurité des clés cryptographiques**. *A contrario*, cette même technologie constitue, à moyen terme, une menace pour les mécanismes de chiffrement eux-mêmes. La puissance de calcul attendue des ordinateurs

²⁰ SFR Actus, 2025, *l'année de la fin du SMS ?*, 12 mars 2025.

²¹ AF2M, *Le RCS franchit le cap des 50 millions de smartphones compatibles en France*, 14 novembre 2025.

²² Bien que ces moyens de contrôle d'accès aux terminaux ne constituent pas du chiffrement cryptographique *stricto sensu*, ils participent du chiffrement des appareils. Ainsi, par une décision d'assemblée plénière du 7 novembre 2022, la Cour de cassation a considéré que lorsqu'un téléphone portable était équipé d'un « *moyen de cryptologie* », le code de déverrouillage de son écran d'accueil pouvait constituer une « *clé de chiffrement* », si l'activation de ce code avait pour effet de mettre au clair les données cryptées de l'appareil ou auxquelles il donnait accès.

²³ Les téléphones intégralement cryptés sont le plus souvent appelés « téléphones fantômes », « cryptophones » ou « téléphones PGP » pour « *Pretty Good Privacy* ».

quantiques à l'horizon 2030 pourrait compromettre une partie des algorithmes de chiffrement. Ce risque est pleinement identifié par les autorités compétentes en matière de cybersécurité. Dès 2022, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) publiait ainsi son premier avis consacré à la migration vers la cryptographie post-quantique (PQC)²⁴.

Au total, les avancées technologiques les plus récentes et les enjeux économiques adossés aux dizaines de millions d'utilisateurs concernés pour le seul marché français, conduisent à un chiffrement toujours plus robuste et étendu, accentuant la pression sur les services de renseignement et d'enquête.

Dès lors, si le docteur Queuille observait, dans une formule aussi mordante que rebattue, qu'« *il n'est pas de problème dont une absence de solution ne finisse par venir à bout* »²⁵, il serait illusoire, dans le domaine des communications numériques (comme dans beaucoup d'autres), de penser que le temps serait susceptible de faire une politique publique ... En d'autres termes, **espérer que le chiffrement finisse par céder naturellement sous l'effet du progrès technique reviendrait à méconnaître la dynamique des nouvelles technologies** qui ne cessent d'évoluer, précisément pour répondre aux innovations susceptibles d'en compromettre l'efficacité.

Chiffrement cryptographique et messageries chiffrées « de bout en bout »

Cryptographie et chiffrement

Le chiffrement est un procédé cryptographique qui permet de garantir la sécurité et la protection des données, qu'elles soient « au repos » (stockée de manière persistante), « en transit » (transmise sur un réseau de communication) ou « en traitement » (équivalente à l'état de la donnée lorsqu'un utilisateur y a accès). Fondé sur un algorithme²⁶, le chiffrement transforme les données dites « claires » en données dites « chiffrées ».

Deux grands mécanismes de chiffrement coexistent. Les « **cryptosystèmes symétriques** » permettent à deux utilisateurs d'utiliser une même clé pour chiffrer et déchiffrer les données partagées. La « **cryptographie asymétrique** » repose sur un couple de clés (bi-clé), l'une privée, l'autre publique. Dans ce cas, ce qui est chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée, qui reste rattachée à son propriétaire.

Les applications des procédés cryptographiques de chiffrement sont multiples :

- signature électronique, certificat numérique et vérification d'identité ;
- stockage de données sensibles dans des espaces de données ;
- gestion de droits numériques pour l'accès à des contenus ;
- flux financiers (ex. : achats en ligne), cryptomonnaies et autres données sensibles (santé, par exemple) ;
- communication électronique entre utilisateurs (messageries instantanées, emails).

Dans ce dernier domaine, le chiffrement garantit principalement la confidentialité de fichiers échangés par des interlocuteurs dits « légitimes ». Seul un utilisateur disposant de la clé de déchiffrement peut en théorie accéder aux données de manière intelligible. Les fonctions connexes de « hachage » et de signature numérique permettent de garantir l'intégrité (absence de modification) et l'authenticité (origine certifiée) des fichiers.

Le chiffrement « de bout en bout »

Parmi les moyens de chiffrement, le **chiffrement de « bout en bout » assure le niveau de sécurité le plus élevé**. Il se distingue des autres moyens en garantissant que seuls l'expéditeur et le destinataire de la communication sont techniquement en mesure d'y accéder en clair.

²⁴ ANSSI, *Avis scientifique et technique sur la migration vers la cryptographie post-quantique*, 2022.

²⁵ On rappellera qu'Henri Queuille, né en 1884, à Neuville, était en vérité pharmacien... Et nul ne semble pouvoir dater ni documenter cette formule, devenue un *gimmick* du débat politique, qui lui est pourtant, et si souvent, attribuée.

²⁶ Ex. : AES (*Advanced Encryption Standard*), RSA-OAEP, ECIES-KEM, DLIES-KEM.

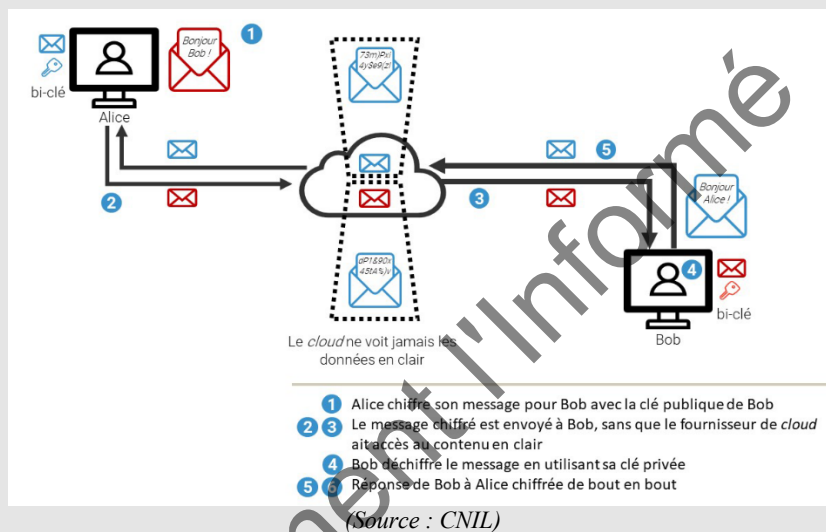
Cette différence est liée à l'**architecture « zero knowledge »** du service, qui garantit que les clés de chiffrement sont générées et stockées par le client. L'éditeur est en incapacité technique d'accéder aux données en clair.

A contrario, le chiffrement des données « en transit »²⁷ sécurise les données tout au long de leur voyage, mais il prévoit une étape de déchiffrement/(re)chiffrement lors du traitement par le serveur entre l'émetteur et le destinataire de la communication électronique. Le chiffrement « de bout en bout » maintient quant à lui les données chiffrées sans discontinuer de l'expéditeur au destinataire.

Le chiffrement « de bout en bout » connaît différents usages, dès lors qu'un échange de données entre une source et une destination peut nécessiter une parfaite confidentialité. C'est notamment le cas dans les différentes formes de services de communications électroniques : visioconférence, messagerie (instantanée ou courriel), partage de fichiers, services de travail collaboratif.

La plupart des applications de messageries instantanées utilisent le chiffrement « de bout en bout » pour tout ou partie de leurs fonctionnalités (messages textuels, appels).

Schéma de chiffrement « de bout en bout » (asymétrique)



2) Un standard encouragé par la puissance publique

La diffusion du chiffrement est d'autant plus inévitable qu'elle s'inscrit dans un mouvement plus large de recherche du niveau de sécurité le plus élevé face à l'élévation de la cybermenace. Le chiffrement apparaît ainsi comme un levier stratégique de protection des échanges numériques face aux risques élevés de compromission des données.

a) La complexité de la cybermenace justifie l'adoption de solutions robustes

La numérisation généralisée des économies comme des fonctions régaliennes, par exemple dans les domaines de la défense et de la santé, accentue le niveau de la menace. L'agence Europol

²⁷ Via notamment le protocole « *transport layer security* » (TLS), évoqué *supra*, ou « *SSH* », « *IPSec* » et « *MACSEC* ». Le terme « transit » ne prend pas la même signification selon qu'il s'applique aux données ou au chiffrement. Concernant les données, l'acception est littérale : sont en transit des données qui sont en circulation, elles peuvent l'être de manière non chiffrée ou chiffrée, et dans ce dernier cas avec un chiffrement « TLS » ou « E2EE », par exemple. Le chiffrement en transit, quant à lui, implique une rupture dans le canal de communication chiffrée, quand le standard « E2EE » assure une continuité du chiffrement entre la source et le destinataire de la communication en leur confiant la gestion des clés cryptographiques.

observe, à cet égard, dans son *Internet Organised Crime Threat Assessment* (IOCTA) pour 2026²⁸, la sophistication croissante du « cybercrime », notamment par l'emploi de technologies de pointe (intelligence artificielle, chiffrement « de bout en bout », *dark web*²⁹, ...).

- **Le contexte général de la montée de la cybermenace**

Ce mouvement n'épargne pas la France où **les incidents de cybersécurité portés à la connaissance de l'ANSSI sont passés de 831 en 2022, à 1112 en 2023 et 1366 en 2025**³⁰.

L'agence française constate, dans le même temps, une érosion continue des frontières entre acteurs étatiques et cybercriminels³¹. Celle-ci se manifeste par un rapprochement des capacités techniques (logiciels malveillants, techniques d'intrusion) : des groupes cybercriminels empruntent des modalités d'action historiquement associées aux opérations étatiques, quand des États (Russie, Chine, notamment) recourent à des modes opératoires proches de la criminalité organisée. Ces mécanismes d'hybridation de la menace sont fortement à l'œuvre.

Les applications de messagerie chiffrée constituent, elles aussi, des cibles privilégiées. Non parce que le chiffrement « de bout en bout » serait compromis, mais parce que les vulnérabilités des applications ou des systèmes d'exploitation peuvent offrir des brèches. En 2025, *WhatsApp* a ainsi corrigé une vulnérabilité susceptible d'avoir été exploitée conjointement avec une vulnérabilité d'*Apple* et affectant le traitement des images dans le cadre d'attaques sophistiquées³².

Plusieurs cas d'exploitation de failles de messageries instantanées, sans qu'elles aient trait au chiffrement lui-même, ont également été dénombrés et ont permis l'installation de logiciels espions sur des terminaux (logiciels *Pegasus* en 2019 et *Graphite* en 2024)³³. De même, dans le contexte de la guerre en Ukraine, de nombreuses campagnes d'hameçonnage, attribuées à des groupes liés aux intérêts russes, ont visé les utilisateurs de *Signal* et *WhatsApp* dans le but d'associer frauduleusement leur compte à un appareil contrôlé par l'attaquant, permettant l'accès aux conversations, sans toutefois compromettre le protocole de chiffrement³⁴.

²⁸ *The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026*, 2026.

²⁹ Le *dark web* désigne un ensemble de services numériques dissimulés et non accessibles par les moteurs de recherche ou les navigateurs internet classiques. Il repose sur des mécanismes d'anonymisation, destinés à masquer l'identité, la localisation et les échanges des utilisateurs. Les services qui y sont hébergés nécessitent généralement des logiciels dédiés, comme le réseau « *TOR* » (*the onion router*), « *I2P* » (*invisible internet project*) ou « *Freenet* ». Il est utilisé pour la vente de stupéfiants, le commerce de données volées, la diffusion de contenus pédocriminels ou encore le trafic d'armes. Le *dark web* et le chiffrement « de bout en bout » poursuivent un objectif commun : protéger la confidentialité des échanges. Ils interviennent toutefois à des niveaux différents : le chiffrement « de bout en bout » protège principalement le contenu d'une communication ; le *dark web* vise à dissimuler les acteurs impliqués dans une activité illicite. Ils se complètent néanmoins : le chiffrement intervient sur l'internet de « *surface* » et peut être coordonné avec des activités intervenant dans le *deep web*, dont le *dark web* est un sous-ensemble.

³⁰ ANSSI, *Panorama de la cybermenace 2025*, 2026. Quatre secteurs d'activité concentrent à eux seuls 76% des 1366 incidents portés à la connaissance de l'ANSSI en 2025 : l'éducation et la recherche (34%) ; les ministères et les collectivités territoriales (24%) ; la santé (10%) et les télécommunications (9%).

³¹ *Ibid.*

³² Références des vulnérabilités : CVE-2025-43300, CVE-2025-21043, CVE-2025-55117.

³³ ANSSI, *Téléphones mobiles, état de la menace depuis 2015*, 2025.

³⁴ ANSSI, *Ibid.*

- **Les exfiltrations de données, le ciblage des terminaux et les chocs futurs émergents**

Aux côtés des grandes cybermenaces (rançongiciels, attaques de « déni de service »³⁵), la France a été exposée à plusieurs actions spectaculaires d'exfiltrations ou fuites de données (fédérations sportives, ministères, agences de l'État, ...). L'ANSSI fait de ces incidents un élément marquant des années récentes, tout en soulignant que la motivation de ces attaques varie selon les opérations : notoriété, défi ou encore gain financier. Le Commandement du ministère de l'intérieur dans le cyberspace (COMCYBER-MI) confirme cette tendance et place le vol de données en deuxième position des cyberattaques, quand les campagnes « hacktivistes » s'en sont déportées pour privilégier des actions de « déni de service »³⁶. Selon la CNIL, **6 200 violations de données ont ainsi été constatées en 2025** (+ 10% en un an), avec une forte augmentation du nombre d'incidents sur des bases de données de plus d'un million de personnes³⁷.

Par ailleurs, le ciblage d'« environnements mobiles »³⁸, pour accéder aux données de communication et aux fonctionnalités des appareils, fait l'objet d'une attention particulière en ce qu'il met à la portée des cyberattaquants un large champ d'utilisateurs privés et professionnels. Le domaine de la cybermenace reflète, au demeurant, une capacité de recherche-développement sophistiquée de la part de sociétés privées spécialisées dans la lutte informatique offensive de portée (LIOP³⁹). La mise à disposition de ces techniques sur un « marché de la vulnérabilité » sert à la fois des commanditaires étatiques et criminels, tout en élevant le niveau de la cybermenace.

Les marchés de la vulnérabilité : du repérage de failles à la commercialisation des capacités d'intrusion

La vulnérabilité désigne une faiblesse affectant un logiciel, un système d'exploitation ou un équipement numérique. Tant qu'elle est inconnue de son éditeur et qu'aucun correctif n'est disponible, elle est qualifiée de **vulnérabilité « zero day »**. Son identification n'est toutefois pas, à elle seule, exploitable. Encore faut-il développer un « **exploit** » ou **outil d'exploitation**, c'est-à-dire un programme, une séquence d'instructions ou une méthode technique permettant de tirer parti de cette faiblesse.

Les « exploit » revêtent une valeur économique potentiellement très forte : le marché de la vulnérabilité rémunère ainsi moins la simple connaissance d'une faille que la capacité de la convertir en outil opérationnel puis, le cas échéant, en une chaîne d'exploitation, voire une chaîne complète de cyber-intrusion. Les études conduites par l'organisme de recherche *RAND Corporation*, dont les liens sont étroits avec le Département de la Défense américain, décrivaient, en 2017, des « exploits » échangés à hauteur de **50 000 à 300 000 dollars**.

L'ANSSI relève ainsi que « *de nombreuses entreprises se sont spécialisées dans le développement et la vente de vulnérabilités jour-zéro à des acteurs offensifs* » et que des intermédiaires, « *moins visibles, sont pourtant essentiels dans la chaîne d'approvisionnement de la surveillance numérique* »⁴⁰. Interviennent alors des chercheurs, développeurs, courtiers, intégrateurs, revendeurs, investisseurs, opérateurs et clients finaux.

Il n'existe toutefois pas un marché unique de la vulnérabilité mais des circuits concurrents ou complémentaires.

³⁵ Les attaques par « déni de service » ou « DoS » pour « *denial of service* » visent à rendre un service numérique indisponible pour ses utilisateurs, soit en saturant ses capacités de traitement, soit en exploitant une vulnérabilité.

³⁶ COMCYBER-MI (CECyber), *Rapport annuel sur la cybercriminalité 2026*, 2026.

³⁷ Audition du 19 février 2026.

³⁸ L'environnement mobile désigne l'ensemble formé par les logiciels et le matériel de fonctionnement des terminaux mobiles (smartphone, tablettes, principalement) : systèmes d'exploitation, applications et interfaces de programmation, ...

³⁹ Le terme LIOP regroupe des entreprises qui développent et commercialisent des capacités informatiques offensives (logiciels espions, chaînes d'exploitation de vulnérabilités, ...). V. à ce propos l'encadré sur le « marché de la vulnérabilité ».

⁴⁰ ANSSI, *Téléphones mobiles : état de la menace depuis 2015*, 2025.

L'Agence européenne pour la cybersécurité (ENISA) distingue en effet des **circuits « organisés »**, dans lesquels les divulgations interviennent selon des règles définies : diffusion coordonnée auprès de l'éditeur, programmes de récompense (*bug bounty*) ou marchés captifs. À côté de ces circuits, se développent des **marchés « gris »**, structurés autour de courtiers spécialisés, qui achètent des vulnérabilités ou des « *exploits* » pour les revendre, par exemple à des acteurs gouvernementaux. Enfin, les **marchés « noirs »** se caractérisent par l'anonymat de la relation client-acheteur et le recours à des plateformes clandestines ou au *dark web*⁴¹. Une même vulnérabilité peut d'ailleurs emprunter différents circuits selon la stratégie de valorisation retenue par son découvreur.

NSO Group, présent sur le marché « gris », parfois qualifié de « *Commercial Spy Market* » ou encore de « *government hacking market* », et son produit phare, *Pegasus*, illustre l'aboutissement industriel de cette chaîne de valorisation des vulnérabilités. Les analyses forensiques produites par le *Security Lab* d'*Amnesty International*⁴², montrent en effet que le logiciel espion repose à la fois sur **une chaîne intégrée de capacités d'identification des failles, d'exploitation (compromission de navigateurs, déclenchement sans action ou « zero clic », ...) et d'infection cyber** (serveurs de validation ou d'installation, par exemple). Plusieurs sources citent des montants d'acquisition et de maintenance de *Pegasus*, au bénéfice d'États, à hauteur de plusieurs millions d'euros.

Par ailleurs, **les cyberattaquants ne renoncent pas à s'approprier des données aujourd'hui protégées par le chiffrement**. Cette stratégie, connue sous l'appellation « *Harvest Now, Decrypt Later* » (HNDL) ou encore « *Store Now, Decrypt Later* » (SNDL), consiste à **intercepter et conserver des données chiffrées dans l'attente de capacités futures permettant d'en compromettre la confidentialité**, par exemple grâce aux progrès attendus de l'informatique quantique. Ces « **attaques rétroactives** »⁴³ concernent tout particulièrement les informations dont la valeur stratégique ou économique suppose une protection durable (données des administrations, des opérateurs d'importance vitale, des entreprises ou des particuliers)⁴⁴. Elle justifie d'engager, sans délai, la transition vers des solutions de « cryptographie post-quantique », plus résistantes, afin de préserver, dans la durée, la confidentialité des informations les plus sensibles⁴⁵.

Enfin, **l'émergence de modèles d'IA capables d'identifier en un temps record et à grande échelle des failles de cybersécurité**⁴⁶, dont certaines présentent un niveau de criticité élevé, rend encore plus prégnant l'objectif de sécurisation des systèmes d'information dans leur ensemble

b) Le chiffrement, une garantie pour la sécurité numérique et les libertés

Dès 1997, dans le contexte d'émergence de la cryptographie à l'échelle mondiale, l'Organisation de coopération et de développement économique (OCDE) publiait une recommandation reconnaissant la criticité du chiffrement cryptographique pour le développement et l'emploi des technologies numériques⁴⁷. Les principes posés visaient à encourager la coordination

⁴¹ European Union Agency for Cybersecurity (ENISA), *Economics of Vulnerability Disclosure*, 2018.

⁴² Amnesty International Security Lab, *Forensic Methodology Report : How to Catch NSO Group's Pegasus*, Londres, 2021.

⁴³ ANSSI, *Cryptographie post-quantique*, 8 octobre 2025.

⁴⁴ V. sur ce point : Europol, *The changing DNA of Serious and Organised Crime (SOCTA) 2025*, 2025.

⁴⁵ V. en ce sens : ANSSI, *Analyse de risque de haut niveau sur le chiffrement et autres usages de la cryptographie*, 27 mai 2026.

⁴⁶ À titre d'exemple, le modèle *Claude Mythos* de la société américaine *Anthropic* n'est pas accessible au grand public en raison des risques anticipés s'il était exploité par des cyberattaquants. Un partenariat a été noué entre *Anthropic* et plusieurs grandes entreprises afin de tester l'impact du modèle sur la sécurité de leurs systèmes (projet dit *Glasswing* avec *Amazon Web Services*, *Apple*, *Broadcom*, *Cisco*, *CrowdStrike*, *Google*, *JPMorganChase*, *Linux Foundation*, *Microsoft*, *Nvidia*, et *Palo Alto Networks*). La fondation *Mozilla*, qui développe le navigateur *Firefox*, a, elle aussi, pu tester les capacités des modèles d'*Anthropic*. Si *Claude Opus 4.6*, modèle antérieur, lui avait permis d'identifier une centaine de vulnérabilités, dont 14 critiques, *Claude Mythos* a, quant à lui, détecté 271 failles.

⁴⁷ OCDE, *Recommendation of the Council concerning guidelines for cryptography policy*, 1997.

des politiques nationales pour assurer un développement homogène des services numériques. Ce faisant, l'organisation internationale admettait la nécessité de renforcer la confiance numérique au moyen de la cryptographie, tout en plaidant, déjà, pour le maintien de la capacité des autorités publiques à protéger les intérêts nationaux et l'ordre public.

- **Une priorité pour la cybersécurité et la souveraineté technologique**

Dans le cadre de l'Union européenne, la stratégie de cybersécurité et le déploiement du marché unique numérique reposent également sur l'affirmation du chiffrement cryptographique.

L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) incite au développement d'un chiffrement robuste, alors même que l'accroissement des transferts d'information par Internet multiplie les risques *cyber* et invite à renforcer la confiance numérique⁴⁸. Cet objectif est endossé au plus haut niveau de pilotage politique. Le Conseil de l'Union européenne affirme, ainsi, « *son soutien au développement, à la mise en œuvre et à l'utilisation du chiffrement fort, qui est un moyen nécessaire pour protéger les droits fondamentaux et la sécurité numérique des citoyens, des pouvoirs publics, des entreprises et de la société (...)* »⁴⁹.

Dans le même temps, le *programme pour une Europe numérique 2021-2027*, établi dans le cadre du règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021⁵⁰, consacre 1,6 milliard d'euros à des investissements dans la cybersécurité des administrations publiques, des entreprises et des particuliers, pour renforcer les capacités de réaction aux incidents, et déployer des infrastructures et des outils adaptés. De son côté, le *programme-cadre Horizon Europe 2021-2027*, porté par le règlement (UE) 2021/695 du 28 avril 2021⁵¹, anticipe un effort de financement à hauteur de 472 millions d'euros pour la recherche-innovation dans le domaine de la cybersécurité et des systèmes de protection de la vie privée.

En France, la *Stratégie nationale de cybersécurité 2026-2030*⁵², élaborée à la demande du Président de la République par le SGDSN, fait de la cybersécurité un objectif à part entière et le rattache, notamment, à l'enjeu de souveraineté technologique : « le chiffrement est un composant essentiel du socle de sécurité permettant d'assurer la confidentialité et l'intégrité des communications ou du stockage des données. La France investira massivement pour conserver la maîtrise des technologies critiques dans le domaine de la cryptographie. Elle soutiendra également les travaux relatifs aux technologies de protection des données, sur l'ensemble de leur cycle de vie ». Dès l'année 2018, le SGDSN appelait d'ailleurs, dans sa *Revue stratégique de cyberdéfense*, premier grand exercice de synthèse stratégique dans ce domaine, à sécuriser les communications par le développement des techniques de chiffrement et à maintenir une industrie nationale de pointe dans ce domaine⁵³.

⁴⁸ ENISA, *Strong Encryption Safeguards our Digital Identity*, décembre 2016.

⁴⁹ *Conclusions du Conseil sur la stratégie de cybersécurité de l'Union européenne pour la décennie numérique*, mars 2021.

⁵⁰ JOUE du 11 mai 2021.

⁵¹ JOUE du 12 mai 2021.

⁵² Commandée par le Président de la République, la *Stratégie nationale de cybersécurité 2026-2030*, rendue publique le 29 janvier 2026, prolonge les ambitions de la *Revue nationale stratégique* et fixe la trajectoire française en matière de résilience cybernétique, de souveraineté numérique et de cyberdéfense. Élaborée sous l'égide du SGDSN, elle a été construite avec l'ensemble des ministères, ainsi qu'un panel d'experts du monde industriel, scientifique et académique.

⁵³ SGDSN, *Revue stratégique de cyberdéfense*, 12 février 2018.

Nous verrons, dans la suite du présent rapport, **qu'à l'heure d'évoquer des « solutions techniques » visant à rendre les données chiffrées accessibles aux services d'investigation, à la double condition de protéger l'intégrité du chiffrement et le secret des correspondances, ces compétences nationales pourraient utilement être mobilisées.**

Au-delà de ces objectifs généraux, le chiffrement constitue une brique fondamentale de la sécurité numérique dans plusieurs secteurs sensibles, à l'image de la santé et des activités bancaires. Dans ce dernier cas, le chiffrement irrigue déjà la protection des flux, des données stockées, des connexions et des environnements mobiles. Le service de renseignement financier TRACFIN⁵⁴ relève également « *la diffusion du chiffrement à des usages spécifiques* », par exemple le recours à des messageries intégrées à des applications bancaires, proposées aux particuliers et offrant des espaces conversationnels difficilement contrôlables⁵⁵.

Ces orientations se traduisent par **l'incitation, au sein de la sphère publique, à recourir à des messageries sécurisées** pour les communications sensibles. Aux États-Unis, la *Cybersecurity and Infrastructure Security Agency* (CISA) recommande aux « officiels » de ne plus utiliser les communications traditionnelles mais d'employer des messageries OTT chiffrées « de bout en bout »⁵⁶, à la suite du piratage attribué à « *Salt Typhoon* » sur les principales entités du secteur des télécommunications, dont plusieurs auraient été compromises à des fins d'espionnage⁵⁷.

Incident de sécurité sur Tchap : un compte utilisateur compromis, sans casser le chiffrement

Le 17 juin 2026, *Tchap*, la messagerie instantanée utilisée par les administrations et les agents publics françaises, a été affectée par un incident de sécurité résultant de la compromission d'un compte utilisateur. Développée et opérée par la *direction interministérielle du numérique* (DINUM), placée sous l'autorité conjointe du Premier ministre et de la ministre chargée du numérique, **la plateforme Tchap repose sur le protocole de messagerie Matrix et intègre un mécanisme du chiffrement « de bout en bout » pour certaines catégories d'échanges.**

Selon le communiqué publié le 8 juin 2026 par la DINUM, le compte compromis a été utilisé pour réaliser des **requêtes malveillantes** avant d'être identifié puis bloqué. L'incident a été traité en coordination avec l'ANSSI. Selon la DINUM, **l'incident a concerné les seuls forums publics et non chiffrés, accessibles sur la messagerie, à l'exclusion des conversations privées chiffrées**, précisant que « *même dans le cas d'une usurpation de compte, l'historique des conversations privées et chiffrées n'est pas accessible* ». Les échanges susceptibles d'avoir été consultés se limitent donc aux conversations publiques de la plateforme.

Cet incident met toutefois en lumière la question du **contrôle des accès et des habilitations** pour l'accès à la messagerie *Tchap*. *Tchap* distingue, en effet, les conversations privées, protégées par chiffrement, des salons publics, accessibles à tout utilisateur authentifié de la plateforme. Les salons publics peuvent ainsi être recherchés et rejoins par l'ensemble des utilisateurs, leurs contenus ne sont pas chiffrés. La compromission d'un compte autorisé a donc, en l'espèce, permis d'accéder aux informations diffusées dans ces espaces ouverts.

73 467 agents auraient été concernés par l'incident, sur 825 000 utilisateurs inscrits. Les données potentiellement exposées comprennent toutefois les noms, prénoms, adresses électroniques, entités d'appartenance et avatars des utilisateurs concernés. L'incident a fait l'objet d'une notification à la CNIL.

⁵⁴ Créé en 1990, le service de Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) est rattaché au ministère chargé de l'économie, des finances et du budget.

⁵⁵ Audition de TRACFIN, le 10 février 2026.

⁵⁶ CISA, *Mobile communications best practice guidance*, 18 décembre 2024.

⁵⁷ ANSSI, *Panorama de la cybermenace 2024*, 11 mars 2025.

Dans le même esprit, aux termes de sa circulaire du 22 novembre 2023⁵⁸, remplacée par une circulaire du 25 juillet 2025⁵⁹, **le Gouvernement français recommande le renforcement de la sécurité des communications électroniques au sein de la sphère publique** et des cabinets ministériels, par l'usage de messageries instantanées sécurisées.

Plusieurs mesures, plus structurelles, ont d'ailleurs été prises par l'État pour protéger ses activités, à l'image de la messagerie instantanée interministérielle des agents publics *TCHAP*, d'outils collaboratifs sécurisés tels que « France Transfert » ou encore de l'important « réseau radio du futur » (RRF) pour les forces de sécurité intérieure, intégré à la trajectoire budgétaire de la loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur 2022-2027 à hauteur de 700 millions d'euros par an, pour un investissement total de l'ordre de 2 milliards d'euros⁶⁰.

Ce bref tour d'horizon démontre que le renforcement de la sécurité numérique est endossé à toutes les échelles d'action – internationales, européennes et nationales – et que le chiffrement « de bout en bout » en est, en l'état des technologies disponibles, le standard le plus élevé. Au demeurant, selon les informations dont dispose la mission, aucune attaque n'a à ce jour permis de compromettre le chiffrement des messageries instantanées utilisant les protocoles les plus aboutis.

La politique de diffusion du chiffrement poursuit ainsi une double finalité. Destinée, on vient de le voir, à renforcer la résilience des systèmes d'information, elle répond tout autant à l'exigence de protection des données personnelles et des droits fondamentaux.

- ***Un instrument de protection des droits fondamentaux***

Les prises de position de l'Organisation des Nations Unies (ONU) soulignent le rôle du chiffrement dans l'exercice des libertés à l'heure où de nombreux régimes basculent dans l'autoritarisme. Le Bureau du Haut-Commissariat des Nations Unies aux droits de l'homme associe ainsi le *E2EE* à la préservation des droits essentiels (liberté d'opinion, d'expression et d'association) et recommande à ses membres de « *promouvoir et protéger un chiffrement robuste et [d']éviter toute restriction directe ou indirecte, générale et indiscriminée, à l'utilisation du chiffrement* »⁶¹. Le rôle des plateformes chiffrées est d'ailleurs très documenté dans l'expression des oppositions, leur structuration et leur mobilisation dans plusieurs pays autoritaires⁶². L'accès à des réseaux privés, en parallèle des réseaux hélas détenus et contrôlés par des structures étatiques, permet aux opposants d'accéder à des communication protégées de la répression.

Par ailleurs, le **règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (RGPD)** favorise *de facto* le chiffrement

⁵⁸ Circulaire n° 6428/SG du 22 novembre 2023 relative au déploiement de l'application *Olvid* sur les téléphones et ordinateurs des membres du Gouvernement et des cabinets ministériels.

⁵⁹ Circulaire n° 6497/SG du 25 juillet 2025 relative au renforcement des communications électroniques par messagerie instantanée au sein de la sphère publique et des cabinets ministériels.

⁶⁰ Le Réseau radio du futur (RRF) est un réseau national de communications mobiles sécurisées, destiné aux acteurs publics de sécurité, de secours et de gestion de crise. Il vise à remplacer les anciens réseaux séparés et utilisés par la police nationale, la gendarmerie nationale, les SDIS ou encore le SAMU par une architecture numérique commune.

⁶¹ Haut-Commissariat des Nations Unies aux droits de l'homme, *The right to privacy in the digital age*, 4 août 2022.

⁶² *Entre la rue et les réseaux : les printemps arabes, laboratoire d'un numérique politique*, Fondation Jean Jaurès, 2025.

« de bout en bout » en orientant les politiques publiques vers les solutions techniques de sécurité numérique les plus avancées. Son article 32 est éclairant qui précise que toute entité responsable ou sous-traitante d'un traitement de données se doit de mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* », y compris « *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitements* ». Si le RGPD n'impose évidemment par le chiffrement « de bout en bout, celui-ci en est un « allier objectif ».

Sur le plan national, le chiffrement des données est également promu par les acteurs publics comme un levier de protection de la vie privée. Dès son rapport d'activité 2016, la CNIL soulignait que « *le chiffrement est devenu une mesure essentielle de protection de la vie privée et de sécurité des données* »⁶³ et l'a rappelé dans le cadre des travaux conduits par la mission⁶⁴. Sa présidente, Mme Marie-Laure Denis, l'explicitait à l'occasion du *Privacy Symposium 2024* de Venise⁶⁵ : « (...) en ce qui concerne la tentation de s'attaquer au chiffrement de bout en bout de nos communications électroniques quelles que soient les causes, parfois très légitimes, poursuivies (...), il faut prendre garde qu'en affaiblissant la possibilité de communiquer de façon confidentielle, pour lutter contre tel ou tel type de délit ou de crime, on repousse parfois les délinquants tout en dégradant la situation du plus grand nombre et en portant atteinte à la liberté de communication. (...) J'observe que la protection de la vie privée et la démocratie forment un couple en tension dans le monde numérique ».

Cette position est bien sûr unanimement défendue par les structures associatives intervenant dans le domaine numérique et rencontrées par la mission. Toutes soulignent la place du chiffrement « *dans la confiance et la confidentialité* », tout en observant que « *la cryptographie évolue pour répondre aux enjeux de sécurité numérique* »⁶⁶.

Au demeurant, l'ensemble des administrations rencontrées par la mission souligne le caractère déterminant de la sécurité numérique pour la protection de la vie privée, dans un environnement où les échanges numériques atteignent toutes les étapes de la vie : intime, publique et professionnelle. Avec une sensibilité plus marquée encore, les représentants de l'autorité judiciaire ont rappelé à la mission leur attribution constitutionnelle de « *gardienne de la liberté individuelle* »⁶⁷, et attiré l'attention de la mission sur les « *risques frauduleux* », de « *cybersécurité* » et « *d'atteintes aux libertés publiques* »⁶⁸, si l'intégrité du chiffrement devait être atteinte.

La conciliation entre, d'une part, l'exercice des droits et libertés constitutionnellement garantis et, d'autre part, les exigences d'ordre public, qu'elles relèvent de la police administrative ou de la police judiciaire, revêt ainsi une acuité – et une complexité – toute particulière dès lors que **les garanties de confidentialité offertes par le chiffrement sont mises au service d'activités illicites.**

⁶³ *Ibid.* p. 47.

⁶⁴ Audition du 19 février 2026.

⁶⁵ *Colloque Privacy Symposium 2024*, Venise, 10 juin 2024.

⁶⁶ Audition de *La Quadrature du Net* et de l'association établie à Bruxelles *European Digital Rights* (EDRI), le 19 février 2026.

⁶⁷ Article 66 de la Constitution : « *L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi* ».

⁶⁸ Audition de la procureure de la République près le tribunal judiciaire de Paris, du PNAT et du PNACO, le 10 mars 2026.

Devenu un standard des communications numériques, le chiffrement bénéficie, en effet et en toute logique, à tous les utilisateurs, quelles que soient leurs finalités d'emploi, y compris les plus répréhensibles.

B) Le recours au chiffrement a gagné l'ensemble du spectre infractionnel

Longtemps circonscrit à des usages spécialisés – militaires, diplomatiques ou gouvernementaux – le chiffrement pénètre désormais les principaux services de communication électronique et accompagne par conséquent tous les usages, y compris délinquants et criminels.

Ce constat recouvre toutefois des réalités distinctes : d'un côté, l'usage des communications chiffrées s'est banalisé dans la commission d'infractions de droit commun et donc « de masse » ; de l'autre, et à un niveau supérieur, l'émergence d'écosystèmes criminels numériques se structure autour de services, plateformes et infrastructures utilisés, voire conçus, dans le but parfois exclusif de garantir l'opacité et la résilience des activités illicites les plus graves.

Les services de l'État témoignent ainsi du **risque « d'asymétrie des moyens »** dans un contexte de *« compétition stratégique entre des structures criminelles dotées d'importantes capacités financières et les autorités détentrices du monopole de la puissance publique »*⁶⁹.

1) Un outil désormais banalisé dans la délinquance dite « de masse »

L'analyse conduite par la mission met en évidence deux phénomènes complémentaires.

Le premier tient à la numérisation des activités humaines qui accroît, mécaniquement, la part des données probatoires protégées par le chiffrement et ce dans un large champ d'infractions.

Le second se traduit par l'usage massif des propriétés de confidentialités dans le but de limiter les possibilités d'identification et d'exploitation des données par les services d'investigation.

a) L'omniprésence des données numériques dans toutes les formes de délinquance

La Direction nationale de la police judiciaire (DNPJ) a relevé devant la mission que l'usage des échanges chiffrés *« s'étend sur le haut du spectre mais aussi sur le bas et le moyen du spectre »*⁷⁰. La Direction des affaires criminelles et des grâces (DACG) décrit, quant à elle, un puissant mouvement de *« démocratisation »* des usages, *« y compris en matière de petite délinquance, par exemple dans des affaires de cambriolage ou de violences intra-familiales »*⁷¹. L'ANTENJ, chef de file des techniques d'enquête numérique ajoute que **« le développement du chiffrement s'étend**

⁶⁹ Audition de la Direction nationale du renseignement et des enquêtes douanières (DNRED), le 4 février 2026.

⁷⁰ Audition du 6 février 2026.

⁷¹ Audition du 17 février 2026.

jusque dans la délinquance du quotidien, qu'il s'agisse de violences ou encore de tentatives d'homicides »⁷².

Dans le même esprit, la Direction générale de la gendarmerie nationale (DGGN) observe que « *les systèmes applicatifs et les messageries sécurisés sont utilisés dans la délinquance de masse : 100 % des délinquants les utilisent* »⁷³. La Direction générale de la police nationale (DGPN) alerte, quant à elle, sur « *une accélération, ces 12 derniers mois, de l'utilisation du chiffrement dans le champ de la délinquance de masse* »⁷⁴.

Signe d'une transformation en profondeur des modes opératoires, **les procédures judiciaires relevant des violences intrafamiliales confrontent de plus en plus les enquêteurs à de nombreuses traces numériques.**

- ***Le révélateur des violences intrafamiliales***

La Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains (MIPROF) fait état de l'étude, certes déjà ancienne (2017/2018) et conduite par le Centre Hubertine Auclert, démontrant que 9 femmes sur 10 victimes de violences au sein du couple déclarent avoir subi des cyber-violences de la part de leur partenaire ou ex-partenaire, dont 1 femme sur 3 a été menacée de diffusion de contenus intimes⁷⁵.

Selon la MIPROF, les cyber-violences au sein du couple se déploient sur des modes opératoires très larges : le **cybercontrôle** (vérification au moyen d'outils numériques des déplacements et des relations sociales de la victime) ; le **cyberharcèlement** (envahissement du quotidien par appels, SMS ou *via* les réseaux sociaux, qui peuvent prendre la forme d'insultes, injures et menaces) ; la **cybersurveillance** (l'agresseur met en place des outils de traçage ou impose de la victime de connaître ses identifiants, mots de passe, etc.) ; les **cyberviolences économiques ou administratives** (utilisation des outils numériques pour réduire l'autonomie financière ou contraindre les démarches de la victime) ; les **cyberviolences sexuelles** (menaces de diffusion de contenus intimes) ; ou encore la **cyberviolence exercée à travers les enfants**. Le tout en contexte d'échanges chiffrés.

Le seul champ des violences intrafamiliales suffit ainsi à mesurer l'ampleur de la difficulté pour les services d'investigations dans des affaires qui relèvent, hélas, du quotidien : avec 256 000 affaires de violences physiques dans le cadre familial enregistrées en 2025 par les services de police et de gendarmerie⁷⁶, **la présence croissante de données issues d'échanges chiffrés confronte les victimes et les enquêteurs à des obstacles probatoires massifs.**

En délinquance générale, une étude plus récente commandée par le *Home Office* britannique, et fondée sur le recoupement de plusieurs milliers de décisions judiciaires, élargit ce constat. La part des preuves numériques dans les affaires pénales y est notée dans 21% des cas en 2010 contre 34% en 2018, tandis que les données provenant des réseaux sociaux et des messageries, notamment

⁷² Audition du 18 février 2026.

⁷³ Audition du 24 février 2026.

⁷⁴ Audition du 26 février 2026.

⁷⁵ *Recherche action « Cyber-violences conjugales »*, 2018, Centre Hubertine Auclert. L'étude portait sur 302 femmes victimes de violences au sein du couple et 73 professionnels des accompagnant dans le périmètre de la région Île-de-France.

⁷⁶ *Insécurité et délinquance*, ministère de l'intérieur, édition de juillet 2026.

Facebook et *WhatsApp*, sont passés, sur la même période, de 3 à 14% des affaires jugées. L'étude mentionne l'existence de preuves numériques dans 45% des affaires de viol et 28% des violences contre les personnes⁷⁷.

b) La confidentialité est un critère d'usage prioritaire pour les auteurs d'infractions

Le second phénomène observé en délinquance dite « de masse » résulte du choix des auteurs d'infractions de recourir à des services protégés dans le but d'échapper aux investigations. **Les messageries chiffrées constituent alors un mode opératoire en tant que tel.** De la simple coordination de groupes locaux en vue de commettre des violences collectives, à la vente au détail de stupéfiants, en passant par les « *sextorsions* »⁷⁸, les échanges chiffrés constituent l'outil privilégié pour commettre une variété toujours plus étendue d'infractions.

S'agissant des **violences collectives**, le rapport d'information du Sénat relatif aux émeutes de juin 2023⁷⁹ relevait ainsi que les « *messageries interpersonnelles* » ont joué « *un rôle important dans l'organisation des actions de pillages à grande échelle* ». Il cite, en particulier, l'usage de plusieurs plateformes de messageries, telles que *WhatsApp*, *Snapchat* et *Telegram*. Le rapport sénatorial documente l'usage de « *boucles* » de proximité, recourant aux messageries sécurisées et constituées à l'échelle très locale (ville, quartier), pour diffuser, coordonner et valoriser les appels de préparation à la violence dans un cadre confidentiel.

Plusieurs études, essentiellement étrangères, décrivent l'usage intensif des applications chiffrées dans les **trafics de stupéfiant de faible à moyenne intensité**.

• **Le cas emblématique des « petites mains » du trafic de stupéfiants**

À titre d'illustration, en dehors de l'espace européen, l'enquête conduite en Argentine par MM. Matías Dewey et Andrés Buzzetti, consacrée à *Telegram*, décrit le déplacement d'une partie du marché de détail des stupéfiants vers les applications de messageries chiffrées, facilitant l'accès aux vendeurs, l'anonymisation des interactions ainsi que la rapidité des livraisons⁸⁰. Un double objectif est alors atteint : la discrétion et l'abaissement du coût – financier mais également physique, au sens de la moindre exposition à des actes de violence entre bandes – d'organisation des échanges illicites.

Ce phénomène de numérisation du trafic, parfois appelé « *ubershit* », a pris de l'ampleur en France avec la période du Covid-19 et des confinements. Il s'est imposé comme une façon de déjouer les contrôles de police et d'éviter les tensions sur les points de « *deal* » traditionnels, tout en proposant une gamme toujours plus étendue de services aux consommateurs de stupéfiants.

⁷⁷ V. Richardson, P. Hanway, R. Baxter et J. McMillan, *Using Appeal Judgement Transcript to Assess Changes in The Presence of Digital Evidence in Police Investigation*, Home Office, Research Report, 19 mai 2022.

⁷⁸ Le terme de « *sextorsion* » désigne les extorsions fondées sur la menace de diffusion d'images, de vidéos ou d'informations à caractère sexuel ou intime.

⁷⁹ F.-N. Buffet, *Émeutes de juin 2023 : comprendre, évaluer, réagir*, Rapport d'information fait au nom de la Commission des lois, Sénat, 9 avril 2024.

⁸⁰ *Easier, faster and safer : the Social organisation of drug dealing through encrypted messaging apps*, Sociology Compass, 2024.

Les services de police observent d'ailleurs que la numérisation du commerce de détail s'accompagne de la baisse du nombre de points de vente physiques. Les vendeurs s'appuient ainsi sur les applications de messageries les plus populaires, en particulier *Snapchat*, considéré comme une « vitrine » commerciale »⁸¹. Ces « marchés souterrains », ou points de « *deal* » numériques, comptabiliseraient entre 100 000 et 300 000 membres actifs sur l'ensemble du réseau de vente de stupéfiants établi sur le territoire national⁸².

L'étude conduite en 2017 auprès de 350 consommateurs australiens, canadiens, britanniques et américains, par Mme Leah Moyle, professeure au *Royal Holloway College* de l'Université de Londres, renseigne sur la portée du chiffrement : « *historiquement, les dealers ont toujours tiré profit des progrès technologiques pour accroître leurs bénéfices et minimiser les risques (...). Ils migrent aujourd'hui vers des applications de messageries sécurisées. Quant aux acheteurs (...), ce sont des consommateurs avertis et soucieux de la sécurité de leurs échanges, sans pour autant avoir le niveau technique pour acheter sur le Darknet avec des cryptomonnaies* ». Elle ajoute : « *s'il est clair que ces applications rendent l'achat de drogue plus accessible, le risque le plus important se trouve dans le plus grand nombre de substances rendues disponibles* »⁸³.

Illustrations de l'usage criminel des messageries instantanées chiffrées

Plusieurs cas d'investigations partagés à la mission par les forces de sécurité intérieure françaises révèlent la criticité de certaines données de contenu des échanges sur messageries chiffrées.

Dans chacun des exemples fournis, les données de communication ont finalement été obtenues par les services d'enquête et de renseignement indépendamment de la coopération des fournisseurs de messageries. Dans certains cas, les données ont été révélées à posteriori, dans le cadre d'enquêtes faisant suite à un crime mobilisant des outils de forensique numérique. Les obtenir plus tôt dans les investigations aurait permis de détecter et élucider plus rapidement les affaires en cours. Lorsqu'elles ont été obtenues avant un passage à l'acte, cela s'est fait dans des délais prolongés et par des moyens coûteux, risqués et incertains.

Sans prétendre à l'exhaustivité, la mission a choisi de mettre en exergue ces affaires réelles documentées par ses interlocuteurs, portant sur des champs d'investigation variés des forces de sécurité intérieure, afin d'illustrer la variété et la sensibilité des cas auxquels sont confrontés les services de l'État :

[Affaire 1] **Enlèvement-séquestration** : les contenus de messagerie chiffrée prouvaient l'implication direct du détenteur de l'appareil saisi dans un enlèvement-séquestration avec demande de rançon. L'exploitation des données a pu mettre au jour un autre fait criminel de même nature commis avec actes de torture et de barbarie (échanges textuels et de photos/vidéos).

[Affaire 2] **Pédocriminalité** : plusieurs personnes impliquées dans des actes pédocriminels et/ou la détention et la communication de contenus de cette nature sont en lien sur une messagerie chiffrée « de bout en bout ». La messagerie leur sert de forum de discussion et de lieu d'échange de leurs productions de contenus.

[Affaire 3] **Prolifération des armes** : un individu situé en France est suspecté de prendre une part active à la livraison d'armes entre deux pays proliférants, en lien avec les autorités politiques et militaires de son pays d'origine.

[Affaire 4] **Terrorisme** : deux individus, l'un en France, l'autre à l'étranger, échangent au sujet d'un lieu de culte identifié pour être la cible d'un potentiel attentat. Les échanges portent sur sa localisation, ses horaires d'ouverture, sur des envois d'argent et sur la possibilité de recruter des personnes en appui à l'action envisagée.

⁸¹ « *Sur Snapchat, WhatsApp ou Telegram, les trafiquants de drogue misent sur la livraison à domicile* », *Le Monde*, 4 août 2025.

⁸² *Ibid.* citant une « note de police » datée du 30 juillet 2025.

⁸³ Citée in « *Les applications offrent une plus grande visibilité à certaines drogues* », *Le Monde*, 12 octobre 2019.

[Affaire 5] **Trafic de stupéfiants** : les messageries chiffrées servent à la tête de réseau d'outil de gestion en « groupes de discussion » du trafic opéré entre la métropole et la zone caribéenne. Les contenus des échanges concernent l'identité des participants au trafic, les prix des marchandises, des lieux et dates relatifs aux opérations, et des voies de blanchiment des recettes des ventes.

[Affaire 6] **Traite d'êtres humains et proxénétisme en bande organisée** : les victimes du réseau de proxénétisme recevaient leurs instructions (lieu, tarification, clients) sur des salons dédiés en boucles restreintes avec les proxénètes. Ces derniers échangeaient entre eux, dans un groupe distinct, sur la gestion et la comptabilité du réseau.

(Source : mission, à partir des données de la Police nationale)

Une enquête française conduite en 2023 sur les usages numériques par les trafiquants de drogues⁸⁴ observe également que les commandes de drogues *via* les outils numériques permettent aux trafiquants de disposer d'une relation permanente à leur clientèle, dans une logique de fidélisation, en contexte fortement concurrentiel. L'enquête souligne que « *le cloisonnement des relations entre les acteurs du réseau vise à limiter (...) le risque de démantèlement policier. Des personnes sont ainsi recrutées de manière occasionnelle ou plus régulière par les trafiquants, pour réaliser des tâches spécifiques, comme la gestion de supports de communication et de l'environnement visuel de comptes numériques ou la livraison des produits au domicile des clients, sans autre lien avec le reste de l'organisation du trafic* ». Le livreur ne connaît pas forcément le fournisseur et, en cas d'arrestation, ne sera pas en mesure de livrer le « haut de la chaîne ». Ces « petites mains » entendent elles-mêmes limiter l'accumulation des preuves de leur implication, par exemple en recourant à des messages s'autodétruisant.

- **Un facteur de convergences inédites entre délinquance du quotidien et crime organisé**

Là où délinquance du quotidien et criminalité organisée évoluaient dans des sphères plutôt cloisonnées, le numérique chiffré multiplie désormais les points de contacts et facilite leur convergence dans un environnement où chacun peut avancer masqué.

La DGGN souligne ainsi un phénomène qu'elle estime compter parmi les « *spécificités françaises* » et qu'elle décrit comme « *une hybridation de la criminalité organisée et de la cybercriminalité* », au point d'évoquer une « **cybérisation de la criminalité organisée** », parfois associée, dans ses manifestations les plus sophistiquées, à des entités étatiques hostiles.

Si ce constat rejoint ceux, précités, de l'ANSSI, la DGGN attribue ce caractère spécifique à des considérations territoriales, « *des communautés de hackers et de gamers, issus de quartiers, se rapprochant de la criminalité organisée, par exemple dans le secteur des cryptoactifs* ». Elle estime à cet égard que « *80% des crypto-rapts sont réalisés en France* »⁸⁵.

L'année 2025 a en effet été marquée par plusieurs « **crypto-rapts** » retentissants, visant en particulier des investisseurs en cryptoactifs⁸⁶. Le Parquet national anticriminalité organisée (PNACO) évoque à cet égard « *un volume significatif de mis en cause* », alors que « *135 faits* [d'enlèvements

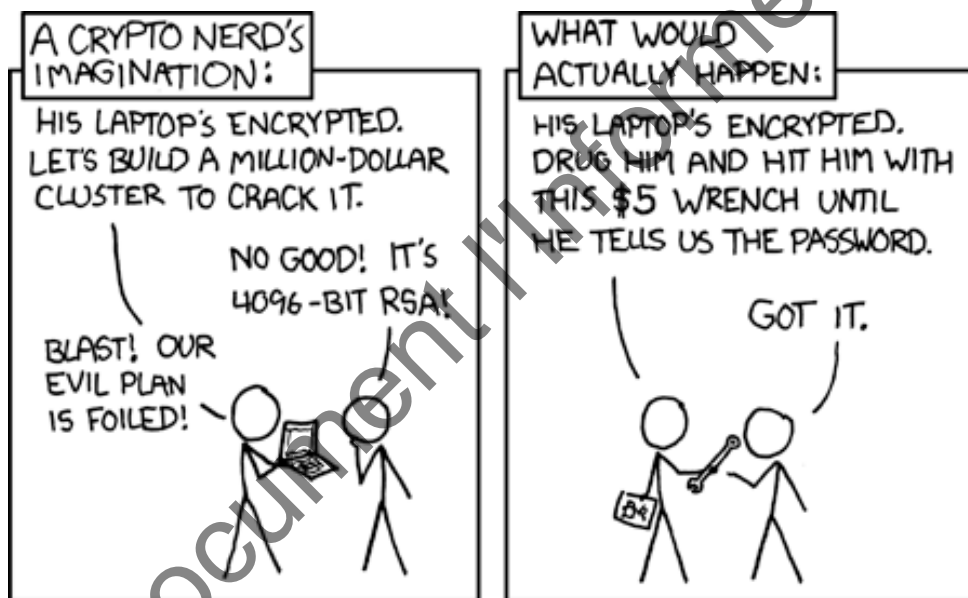
⁸⁴ Clément Gérôme, « *Fidéliser la clientèle et déjouer l'intervention policière : les usages du numérique par les trafiquants de drogues* », Enjeux numériques, Annales des Mines, décembre 2023.

⁸⁵ Audition du 24 février 2026.

⁸⁶ Pour une illustration des techniques employées par les malfaiteurs : « *Après l'enlèvement de David Balland, la crainte se répand dans le secteur des cryptomonnaies* », *Le Monde*, 6 février 2025.

liés aux cryptomonnaies] *ont été recensés depuis 2023 par les forces de l'ordre* »⁸⁷. Enlèvements, séquestrations, usage de la violence, demandes de rançon ou de remise de valeurs en cryptoactifs, la procureure de la République anticriminalité organisée souligne « *l'identification de personnes impliquées de manière récurrente dans plusieurs dossiers, révélant (...) l'existence de réseaux structurés* » mobilisant, en particulier, l'Office central de lutte contre le crime organisé (OCLCO) de la Direction nationale de la police judiciaire (DNPJ), ainsi que l'Unité nationale de police judiciaire (UNPJ) de la Gendarmerie nationale⁸⁸.

Le chiffrement n'est toutefois au cœur des infractions de crypto-rapts qu'en ce qu'il protège l'accès aux cryptoactifs dont l'efficacité conduit des groupes criminels à privilégier, non l'attaque des systèmes d'information eux-mêmes, mais la contrainte exercée sur leurs détenteurs⁸⁹. Ces « *wrench attacks* », ou « *attaques par coercition physique* », répondent à cette formule, devenue un classique de la communauté de la cybersécurité : « *son ordinateur portable est chiffré ; administrez-lui un sédatif puis contraignez-le avec une clé anglaise à 5 dollars, jusqu'à ce qu'il vous révèle son mot de passe* ».



(Source : dessin de Randall Munroe, <https://xkcd.com/538/>)

Dans un autre champ de la délinquance, la Direction nationale du renseignement et des enquêtes douanières (DNRED) ajoute, au profilage des usages criminels des messageries chiffrées, sa forte représentation dans le domaine de la « **criminalité en col blanc** »⁹⁰. Le constat est bien sûr confirmé à une échelle plus large que le seul cadre national : le rapport établi par les membres⁹¹ du Pôle européen d'innovation pour la sécurité intérieure⁹² constate le recours au chiffrement dans

⁸⁷ Communiqué du PNACO, 24 avril 2026.

⁸⁸ V. en ce sens : « Enlèvements dans le secteur des cryptomonnaies : 88 mises en examen dans les enquêtes en cours, selon le PNACO », *Le Monde*, 24 avril 2026.

⁸⁹ Pour consulter l'une des rares études disponibles sur le phénomène des « crypto-rapts » : M. Ordekian, G. Atondo-Siu, A. Hutchings et M. Vasek, *Étude des « wrench attacks » : les agressions physiques visant les détenteurs de cryptoactifs*, Actes de la 6^e Conférence sur les avancées des technologies financières, Leibniz International Proceedings in Informatics, 2024.

⁹⁰ Audition du 4 février 2026.

⁹¹ Europol, Eurojust, la direction générale de la migration et des affaires intérieures (DG HOME), le Centre commun de recherche de la Commission européenne (Join Research Centre – JRC), le coordinateur de la lutte contre le terrorisme du Conseil de l'Union européenne et l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information (eu-LISA).

⁹² UE Innovation Hub for Internal Security.

plusieurs affaires de fraudes aggravées et observe que « *les cryptoactifs sont largement utilisés pour blanchir les produits d'activités criminelles* » et dissimuler les transactions⁹³.

Certes, il ne saurait être conclu de ces observations convergentes, qui débordent du seul contexte national, que les messageries instantanées seraient intrinsèquement criminogènes, ni d'ailleurs que les techniques administratives et judiciaires d'interception disponibles dans notre droit positif, auraient vocation à s'élargir à l'ensemble du champ infractionnel. **Ces constats attestent en revanche l'existence d'un monde souterrain, entretenu par la totale confidentialité garantie par le chiffrement « de bout en bout ».**

Une observation, toutefois : en dépit des informations recueillies sur la place des communications chiffrées dans la délinquance dite « de masse », la mission constate que ce phénomène demeure imparfaitement documenté sur le territoire national. Les connaissances disponibles reposent encore largement sur des observations empiriques et dispersées selon les catégories d'infractions, ne permettant pas de distinguer les différentes fonctions assignées aux outils numériques dans la préparation, la commission, la réitération ou la dissimulation des faits.

Cette lacune n'est pas sans poser problème dès lors que toute évolution du champ pénal suppose, pour viser juste, une connaissance fine des activités criminelles qui s'affirment dans la société. La mission estime par conséquent que des travaux de recherche devraient pouvoir être encouragés sur ce thème, associant notamment les services statistiques des ministères de l'intérieur et de la justice, les services d'enquête, les juridictions, les associations de victimes ainsi que les opérateurs de communications et les fournisseurs de services numériques.

Recommandation n° 1 : Favoriser l'émergence d'un programme pluridisciplinaire de recherche pour documenter la transformation des activités criminelles à l'heure du numérique et des communications chiffrées.

Enfin, un point mérite d'être précisé : les services compétents en matière de lutte contre le **terrorisme** ont indiqué à la mission que la problématique du chiffrement des échanges d'informations y était moins prégnante qu'en criminalité organisée. Les usages y reposeraient encore fréquemment sur des services « grand public » et s'accompagneraient d'un niveau très inégal de sécurité opérationnelle, et donc d'une « professionnalisation » moindre des mesures de confidentialité. Cet état de fait n'atténue évidemment en rien la vigilance exercée par les forces de sécurité intérieure et les services enquêteurs quant à l'évolution des modes opératoires.

2) Le chiffrement comme infrastructure d'écosystèmes criminels intégrés

La diffusion massive des communication chiffrées en population générale produit, sans surprise, un **effet de normalisation** : les mêmes outils servent indifféremment aux usages légitimes de protection de la vie privée comme à des usages délinquants et, à un niveau d'intensité plus élevé, à la structuration d'écosystèmes numériques criminels, d'ampleur régionale ou transnationale, spécialisés ou généralistes.

⁹³ Europol, *First Report on Encryption by the EU Innovation Hub for Internal Security*, Publications Office of the European Union, 2024.

Cette évolution conduit à la mutation des activités illicites autour des services numériques, le plus souvent sécurisés. **La mission fait à cet égard le constat préoccupant que deux niveaux de structuration des activités criminelles sont à l'œuvre : le premier porte sur l'intégration des services numériques « grand public » dans des chaînes criminelles complètes ; le second porte sur la spécialisation d'infrastructures numériques dédiées et/ou commercialisées à la destination exclusive d'activités criminelles.**

a) L'intégration de services numériques dans une chaîne criminelle complète

À une échelle plus large que la France, Europol, dans son rapport intitulé *Serious and Organised Crime Threat Assessment (SOCTA)* pour 2025, observe que « les réseaux criminels exploitent les infrastructures numériques à leur plein potentiel, en utilisant les technologies et les systèmes en ligne afin de faciliter les activités illégales, d'échapper aux forces de l'ordre et de maximiser leurs profits »⁹⁴. Elle ajoute qu'« avec un haut degré d'organisation, les criminels font la publicité de biens et de services illicites, identifient les cibles, utilisent des messages chiffrés et codés pour communiquer et recruter des individus, y compris des mineurs, sur ces plateformes. Les réseaux criminels travaillent souvent avec des spécialistes techniques afin de mener ces activités »⁹⁵.

À titre d'illustration, dans le champ des **infractions sexuelles** et des **atteintes aux mineurs**, les enquêtes disponibles ne cessent de documenter l'utilisation accrue des messageries chiffrées : chantage à la diffusion d'images intimes, « *grooming* »⁹⁶ ou échanges massifs et monétisés de contenus pédocriminels. À cet égard, le Groupe d'action financière (GAFI), organisation intergouvernementale créée en 1989 à l'initiative du G7 afin d'élaborer des standards internationaux de lutte contre certains phénomènes criminels, souligne, dans son rapport pour 2025, que l'exploitation sexuelle des enfants en ligne est aggravée par « l'augmentation de l'utilisation et la prolifération de la technologie de communications cryptées ».

La structuration numérique des activités criminelles s'accompagne d'un mouvement d'intégration et d'externalisation de fonctions ciblées, une part significative des réseaux les plus menaçants exerçant un « *contrôle de bout en bout* » du processus criminel⁹⁷.

- **L'internalisation de fonctions criminelles numériques**

Dans cet environnement, les services numériques remplissent plusieurs fonctions intégrées : **fonctions commerciales**, à des fins *marketing* et de mise en relation ; **fonctions opérationnelles** par la coordination des intervenants ; **fonctions financières** par l'organisation des paiements et des opérations de blanchiment. Plusieurs **fonctions transversales** sont également supportées par la voie numérique, dans le domaine du recrutement et de la dissimulation, dont le chiffrement « de bout en bout » est le principal point d'appui technologique.

⁹⁴ Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA)*, 2025.

⁹⁵ V. également en sens : Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2024, et Eurojust/Europol, *Common challenges in cybercrime*, 2024.

⁹⁶ Le « *grooming* » ou « *cyberprédation* » désigne le procédé par lequel un adulte établit progressivement une relation de confiance avec un mineur, par l'intermédiaire de services numériques, afin de commettre une infraction sexuelle ou de faciliter son exploitation.

⁹⁷ Europol, *Decoding the EU's most threatening criminal network*, 2024.

Les infrastructures numériques sont, de surcroît, utilisées à des fins logistiques afin d'obtenir frauduleusement des informations, par exemple sur les cargaisons dans lesquelles des produits illicites sont dissimulés. Cette exploitation peut alors donner lieu à des actions de piratage de systèmes informatiques, à la corruption de personnels disposant d'accès numériques ou encore à l'exploitation d'informations logistiques dématérialisées.

Une multitude de « couches numériques » sécurisées est ainsi mobilisée et fait système : les messageries chiffrées pour la mise en relation, la diffusion, la coordination opérationnelle et la sécurisation des échanges textuels et vocaux ; les outils de pseudonymisation, à l'image des cryptoactifs, pour la sécurisation des transactions financières.

La mobilisation des leviers numériques par la criminalité couvre l'ensemble des outils du numérique. Les outils « grand public » servent de « vitrine » et offrent un premier point de contact et d'entrée, par exemple pour la proposition de biens illicites. Le **dark web** accueille ensuite des « places de marché » virtuelles qui mettent en relation l'offre et la demande. En 2025, une opération conduite par Europol et Eurojust a ainsi permis le démantèlement de la « place de marché » dédiée aux produits stupéfiants « *Archtyp Market* », qui, depuis sa création en 2020, avait enregistré 600 000 utilisateurs pour un total de transactions d'au moins 250 millions d'euros. En parallèle, les paiements en **cryptomonnaie** se développent, gages d'anonymat et de transactions sans frontières. Les services de police relèvent, à cet égard, une tendance à l'emploi de monnaie à degré d'opacité élevée, leur permettant de résister aux outils de traçage de la *blockchain*⁹⁸. Enfin, les services localisés dans des zones géographiques plus permissives en matière de lutte contre le **blanchiment** sont privilégiés sachant, selon Europol, que 96% des réseaux criminels les plus menaçants blanchissent eux-mêmes leurs produits criminels⁹⁹. **Les activités les plus sophistiquées font donc un usage hybride des échanges chiffrés « de bout en bout ».**

Les témoignages recueillis par la mission montrent, par ailleurs, que les acteurs criminels basculent systématiquement leurs échanges vocaux sur des messageries chiffrées, dès lors qu'ils sont appelés à traiter de leurs activités¹⁰⁰. Ils ne se bornent au demeurant pas à utiliser une plateforme de messagerie chiffrée en particulier mais sollicitent, pour « *brouiller les pistes des enquêteurs* », « **un cocktail de messageries cryptées** »¹⁰¹.

Ainsi, en facilitant l'organisation et la dissimulation des activités délictuelles et criminelles, les messageries chiffrées permettent à leurs utilisateurs d'échanger rapidement des informations, en protégeant l'anonymat des interactions au sein d'espaces fermés, en grande partie inaccessibles aux services de renseignement et d'enquête judiciaire. L'importance du chiffrement pour les activités illicites de grande ampleur se mesure d'ailleurs à l'intérêt que les réseaux criminels portent aux ingénieurs cryptographes et aux fournisseurs de technologie de chiffrement. Ces derniers sont identifiés comme des « **cibles de grande valeur** » pour l'organisation des processus criminels, au même titre que les compétences en courtage, comptabilité, droit et falsification¹⁰².

⁹⁸ On rappellera que la « *blockchain* » est une technologie dans laquelle les données sont enregistrées au sein de bloc successifs, reliés entre eux par des procédés cryptographiques.

⁹⁹ Europol, *Decoding the EU's Most Threatening Criminal Networks*, 2024.

¹⁰⁰ Audition de la DGGN, le 24 février 2026.

¹⁰¹ Audition de la DNPI, le 6 février 2026.

¹⁰² Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA)*, 2021. Les cibles de « grande valeur » sont, dans la définition donnée par Europol, des acteurs clés permettant ou facilitant le déroulement des processus criminels.

- **L'externalisation de fonctions criminelles numériques**

Les organisations criminelles les plus structurées, parce qu'elles sont dotées d'une puissante surface financière, ont la capacité de déployer des stratégies d'externalisation de fonctions spécialisées. Cette stratégie, parfois appelée « **crime as a service** », désigne la fourniture, à titre marchand, de prestations criminelles hautement spécialisées, conçues pour d'autres acteurs criminels : vente de logiciels malveillants ou de données volées ; prestations de « *phishing* »¹⁰³ ou de rançongiciels ; et mise en relation entre offreurs et demandeurs.

Europol identifie ainsi plusieurs catégories de « prestataires » : « *hommes de paille, experts techniques, prestataires de transport, agents corrompus, conseillers ou experts financiers, faussaires de documents et d'identité, vendeurs de rue et coursiers* »¹⁰⁴. **Les potentialités offertes par le numérique favorisent une division des tâches qui, dès lors que le contenu des échanges est chiffré « de bout en bout », échappe aux capacités d'interception des services d'investigation.**

Enfin, l'usage des services chiffrés entraîne **un changement d'échelle des activités criminelles** : leurs utilisateurs, même lorsqu'ils disposent de moyens limités, peuvent organiser, en toute sécurité, un espace confidentiel tout à la fois intégré (unité de commandement) et segmenté (en une multitude de fonctions externalisées), et ce depuis un territoire différent des marchés domestiques sur lesquels ils opèrent.

Ces pratiques déterminent directement les conditions dans lesquelles travaillent désormais les services d'investigation : il ne font plus face aux ramifications propres à toute forme de crime organisé, ils enquêtent dans un environnement où une même affaire se compose de branches et sous-branches – duplices, masquées et protégées – d'une redoutable complexité.

Annonce de recrutement pour d'un homicide sur une messagerie chiffrée



(Source : Police nationale)

¹⁰³ Le « phishing » ou « hameçonnage » désigne une technique frauduleuse consistant à tromper une personne afin qu'elle communique des informations confidentielles, ouvre un accès à un système informatique ou réalise une opération au profit de l'auteur de la fraude. En France, le site cybermalveillance.gouv.fr indique que l'hameçonnage demeurerait, en 2024, une menace prédominante, tout public confondu, avec une progression de l'ordre de 70% en 2025.

¹⁰⁴ Europol, *Decoding the EU's Most Threatening Criminal Networks*, 2024.

b) La création de services numériques à vocation spécifiquement criminelle

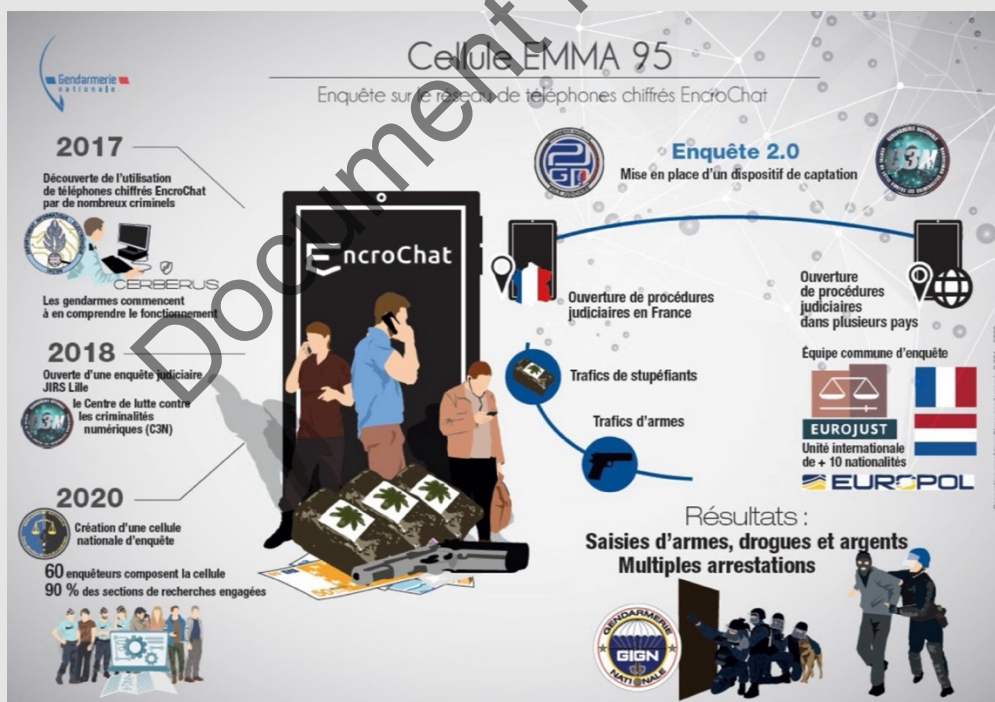
Un degré plus élevé de structuration recouvre les infrastructures numériques conçues, commercialisées et configurées pour offrir aux acteurs criminels un service d'échange protégé : terminaux dédiés, abonnements et serveurs spécifiques, chiffrement renforcé, ... Les affaires dites *EncroChat*, *Sky ECC* ou encore *Ghost* relèvent de cette catégorie.

• L'affaire *EncroChat*, un succès français éclairant les nouveaux modes opératoires

Dans le cadre de l'enquête judiciaire confiée à la DGGN¹⁰⁵, conduite par le parquet de la Juridiction interrégionale spécialisée (JIRS) de Lille, puis par les juges d'instruction saisis d'une information judiciaire¹⁰⁶, les investigations ont permis d'identifier une solution de communication chiffrée, distribuée sous le nom d'*EncroChat*, mise en œuvre depuis la France et destinée à des organisations criminelles¹⁰⁷.

« Dès 2017 », rappellent les services, « des téléphones utilisant le moyen de communication sécurisée *EncroChat* [ont été] détectés par le département Informatique Électronique (INL) de l'Institut de recherche criminelle de la Gendarmerie Nationale (IRCGN). (...) Début 2019, le projet *CERBERUS*, piloté par la gendarmerie et financé par des fonds européens, permettait l'accélération (...) des recherches sur ces téléphones »¹⁰⁸.

L'enquête sur le réseau de téléphones chiffrés *EncroChat*



(Source : Gendarmerie Nationale)

¹⁰⁵ Et son Centre de lutte contre les criminalités organisées (C3N).

¹⁰⁶ Le 28 mai 2020.

¹⁰⁷ L'ouverture d'une enquête préliminaire par le C3N datait du 15 novembre 2018.

¹⁰⁸ Note des autorités judiciaires françaises relative à l'enquête *EncroChat*, diffusée sur le site Internet d'Eurojust le 2 juillet 2020 à l'occasion de la conférence de presse conjointe Eurojust-Europol du 2 juillet 2020, document ID 2020/00035.

Cette opération¹⁰⁹ – nom de code *EMMA 95* – a démontré l'existence de services numériques conçus pour offrir une prestation complète, associant une fonctionnalité de messagerie cryptée et des terminaux *ad hoc*, conçue pour dissimuler l'activité de criminels du « haut du spectre ».

Un service français de renseignement du premier cercle observe qu'« **EncroChat relevait d'une véritable offre marketing consistant à offrir une solution de protection adaptée à des activités criminelles** »¹¹⁰, tandis que la DGGN, évoque « *une solution de terminaux chiffrés créée pour un usage spécifiquement criminel* »¹¹¹. Le crime « *by design* », en quelque sorte ... Les données issues d'*EncroChat* et *Sky ECC* ont ainsi permis d'éclairer les modes opératoires des réseaux criminels pour l'organisation d'activités violentes ou encore le transport de stupéfiants à grande échelle.

L'importance des données révélées par le démantèlement de services chiffrés dédiés aux activités criminelles

Des affaires récentes ont conduit au démantèlement de réseaux et à l'exploitation de messageries principalement utilisés par des organisations criminelles (*EncroChat*, *Sky ECC*, *ANOM*). L'exploitation des conversations a confirmé l'importance des contenus pour la prévention de crimes et délits et l'incrimination des personnes responsables.

EncroChat

La solution de communication numérique chiffrée *EncroChat* est ciblée dès 2018 par la Gendarmerie nationale française. Une solution technique d'accès aux communications en clair est développée et mise en place courant 2020. Les investigations révèlent une large diffusion de la solution de téléphonie cryptée dans des réseaux criminels répartis dans le monde. Des partenariats sont mis en place au sein d'Eurojust et Europol pour superviser le recueil de données et exploiter les contenus. Les investigations se concentrent sur un niveau de danger particulièrement élevé (atteinte à la vie, flagrant délit, identification d'organisations criminelles). Entre 2020 et 2023, les investigations conduites sur le réseau *EncroChat* ont conduit à 6 500 interpellations, à la prévention d'une centaine d'assassinats ou enlèvements et à la saisine ou le gel de 900 millions d'euros d'avoirs criminels.

(Source : bilans *EncroChat* réalisés par la Gendarmerie nationale, Europol, Eurojust, et les parquets français et néerlandais)

Sky ECC

Fin 2018, la police belge découvre l'emploi de cryptophones chez des membres d'organisations criminelles. Ces appareils sont uniquement équipés du logiciel de chiffrement *Sky ECC* commercialisé par une organisation basée au Canada et aux Etats-Unis. L'application permet d'envoyer des messages textuels ou vocaux, ainsi que des photos, avec un haut niveau de chiffrement. Une solution de déchiffrement est mise au point fin 2020 dans un cadre partenarial. A compter de début 2021, les enquêteurs et magistrats sont en mesure de prendre connaissance, de façon ciblée, de données de contenu de l'application en direct.

Sur la seule exploitation des flux en direct pendant 3 semaines, 34 atteintes à la vie et 73 faits criminels de très grande importance ont été détectés. Pour la Belgique seule, l'opération a permis d'ouvrir 470 nouveaux dossiers judiciaires en 5 ans et d'enrichir 203 dossiers déjà en cours. Près de 5 000 suspects ont été identifiés dans ce cadre. La plupart des condamnations conséquentes relevaient du trafic de stupéfiants, d'actes de violence, de corruption, de blanchiment, de possession illégale d'armes et de violation du secret professionnel.

¹⁰⁹ Il convient de rappeler qu'une équipe européenne commune d'enquête a également été constituée sur la base de l'article 13 de la Convention européenne d'entraide judiciaire en matière pénale du 29 mai 2000 conclue entre les États membres de l'Union européenne. Prévu aux articles 695-2 à 695-3 du CPP, le cadre des équipes communes d'enquête permet de développer entre les États des stratégies communes d'enquête et de partager des objectifs de lutte contre la criminalité organisée transfrontalière. La souplesse de ce mécanisme permet aux autorités judiciaires et aux services concernés d'échanger des renseignements, de mener des opérations conjointes et de coordonner les poursuites pénales.

¹¹⁰ Audition du 24 février 2026.

¹¹¹ Audition du 24 février 2026.

(Source : bilan Sky ECC réalisé par la Police fédérale belge en février 2026)

ANOM

Une opération de coopération policière internationale a conduit au développement et à la diffusion dans des réseaux criminels des téléphones cryptés dotés d'une messagerie chiffrée dissimulée derrière une application de calcul. L'application de messagerie incluait des paramètres avancés de confidentialité (autodestruction des messages, stockage sécurisé des données). Au plus haut de l'opération, l'application avait été installée sur près de 12 000 appareils, actifs dans 300 réseaux criminels situés dans environ 100 pays. L'opération de surveillance conduite entre 2018 et 2021 a permis à aux services de police de 16 pays d'arrêter 800 personnes impliqués dans des activités criminelles.

(Source : « Policing Futures / strataTalks future networks / Interpol global horizon scan », novembre 2021)

• **L'émergence de criminels « digital natives »**

Les services de l'État l'ont observé devant la mission : nous sommes progressivement entrés dans une nouvelle ère. À la génération de délinquants optimisant leurs activités en recourant aux outils numériques a succédé une génération de véritables criminels « digital natives »¹¹². **La numérisation du crime fait alors place à la criminalisation du numérique** : il s'agit là de la définition la plus authentique qui soit de la cybercriminalité. Le crime organisé recherche particulièrement ces profils, souvent jeunes et accoutumés aux bouquets de fonctionnalités protégées. La Direction générale de la sécurité intérieure (DGSI) observe, à cet égard, que certaines de ses cibles « *se servent de façon privilégiée de jeunes utilisateurs des nouvelles technologies* »¹¹³.

Ces profils sont également rompus à une forme d'ascèse ou **hygiène numérique** exigeante, méthodique, disciplinée¹¹⁴. Les paramètres applicatifs d'anonymat et de confidentialité sont activés, leurs activités et leur présence en ligne rigoureusement « nettoyées ». Ils procèdent à des renouvellements réguliers de terminaux, de cartes SIM ou à des mesures de contre-piégeage anticipées pour contourner les techniques d'interception.

Le numérique chiffré n'est donc pas un simple outil d'appui à l'activité criminelle, il en devient la composante centrale, offrant à la fois une infrastructure technique performante et un environnement opérationnel intégré. **Le centre de gravité des activités illicites demeure dans le monde physique, mais il s'appuie, en France et partout ailleurs, sur des services numériques la plupart du temps chiffrés.**

Les services enquêteurs font alors face à **une criminalité liquide** – frappée de mobilité, d'instantanéité, de « défrontiarisation » – dont les conséquences économiques, sociales et bien sûr sécuritaires n'en demeurent pas moins tangibles. La Délégation parlementaire au renseignement (DPR) en conclut, dans son rapport public pour l'année 2025, que « *les organisations criminelles (...) disposent désormais de capacités qui ont longtemps relevé d'un monopole de la puissance publique (...)* »¹¹⁵.

¹¹² La formule est employée par Europol dès 2021, v. à cet égard : Europol, *Serious and Organized Crime Threat Assessment (SOCTA)* 2021, 2021.

¹¹³ Audition du 24 février 2026.

¹¹⁴ Audition du DGP, le 26 février 2026.

¹¹⁵ Rapport de l'activité de la délégation parlementaire au renseignement pour l'année 2025, tome 1, « La transformation du renseignement français face aux ruptures du monde », 16 décembre 2025.

II) Un défi opérationnel pour les services : adapter les capacités d'accès aux données

L'histoire récente offre plusieurs illustrations de ruptures technologiques ayant affecté les capacités d'investigation des services de renseignement et des enquêteurs judiciaires. Il suffit pour s'en convaincre de convoquer le souvenir de l'attaque de la *Société Générale*, le 22 décembre 1911, rue Ordener, à Paris, où la célèbre « Bande à Bonnot » commit le premier braquage armé à l'aide d'une automobile. La presse de l'époque et les responsables politiques déplorèrent alors l'avantage tactique procuré par la vitesse des automobiles sur les forces de l'ordre¹¹⁶.

Mais les mutations introduites par les technologies de la communication se singularisent par leur ampleur et par le rythme des adaptations qu'elles imposent aux services de l'État.

Dès le tournant des années 1990, l'essor des téléphones portables et le développement du *Global System for Mobile Communications* (GSM) avaient certes frappé d'obsolescence les techniques d'interception des téléphones fixes. De la même façon, l'apparition des SMS, la généralisation des accès Internet fixes par « box », puis le déploiement des réseaux mobiles de Cinquième Génération (5G), imposèrent de prendre des mesures d'adaptation. La transition attendue à l'horizon 2030 de la 6G devrait produire les mêmes effets.

À la différence toutefois de ces évolutions récentes, le chiffrement « de bout en bout » déplace l'enjeu vers l'existence même de l'information « en clair ».

À l'ère du chiffrement « de bout en bout », si l'intermédiaire technique peut détenir des métadonnées et des informations de signalisation, il ne dispose en effet plus, par construction technique, de la clé permettant de restituer l'échange. **Le défi auquel font face les services d'investigation change ainsi radicalement de nature : il est désormais systémique.**

Aux « *bandits tragiques* » de 1911 – le mot est parfois attribué à Jules Romain – l'État pouvait répondre en motorisant la police mobile, fondée par Clémenceau quelques années auparavant¹¹⁷. Face au chiffrement « de bout en bout », la tâche est d'une toute autre ampleur : elle consiste à contourner une architecture standardisée, de dimension mondiale, déployée par des entreprises le plus souvent étrangères et pour certaines sans existence légale en France, spécifiquement conçue pour que nul tiers, y compris les opérateurs de communications électroniques eux-mêmes, ne puisse détenir l'information. Autrement dit : un *Everest* technologique. Dès lors, **le chiffrement déstabilise les fondements mêmes du modèle français d'accès aux communications électroniques.**

¹¹⁶ « Face à l'intrépidité et à la vitesse des malfaiteurs en automobile, le retard de militaires se déplaçant à bicyclette, et encore largement à cheval, apparaît criant », Luis Miguel Lopez, « 1912, l'affaire Bonnot : les effets contradictoires d'une crise anarchiste », *Socio-Logos*, n°2, 2007.

¹¹⁷ En 1907.

A) Le modèle d'accès légal aux communications à l'épreuve du chiffrement

Depuis la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie de communications électroniques, premier cadre légal des interceptions judiciaires et de sécurité, le législateur n'a cessé d'intégrer l'essor du numérique. Il s'est appliqué à adapter, au gré des virages technologiques, le cadre juridique national. Il a fait entrer dans le champ du droit des notions et des acteurs qui, jusque-là, lui étaient étrangers, à l'instar des « *systèmes d'exploitation* », des « *données relatives au trafic* »¹¹⁸ ou encore des « *fournisseurs de services de communications interpersonnelles* ». Il faut d'ailleurs lire l'article 32 du code des postes et des communications électroniques (CPCE), introduit par l'ordonnance du 28 avril 2016¹¹⁹, en qu'il constitue un véritable glossaire des procédés technologiques les plus innovants et, parfois, les plus complexes.

Le législateur s'est également attaché, sous l'impulsion notamment du droit de l'union européenne, à faire le tri parmi les informations échangées par la voie numérique : celles qui relèvent du contenu des communications (données de correspondance) ; celles qui permettent d'identifier les utilisateurs, d'assurer l'acheminement des échanges, leur facturation ou la localisation des terminaux (données techniques de connexion ou métadonnées). **En deux décennies, un cadre juridique complexe, sédimenté, s'est ainsi construit et enrichi au gré des exigences constitutionnelles et conventionnelles, et des besoins opérationnels des services.**

Pour comprendre cette évolution et éclairer les arbitrages auxquels les pouvoirs publics sont confrontés, il est indispensable de rappeler l'économie générale et les principes qui organisent le régime des interceptions administratives et judiciaires. C'est en effet la maîtrise du droit positif, des procédures existantes et des capacités offertes par celles-ci, qui permettront d'identifier les brèches ouvertes par le chiffrement comme les voies d'action envisageables.

Sans altérer sa complexité, le droit de l'accès aux communications électroniques peut être représenté selon une architecture à quatre niveaux :

- les obligations de coopération technique imposées aux opérateurs pour les besoins des services enquêteurs : elles relèvent du CPCE ;
- les finalités définies pour la mise en œuvre des techniques de renseignement et des techniques d'enquête numérique judiciaire qui relèvent respectivement du code de la sécurité intérieure (CSI) et du code de procédure pénale (CPP) ;
- la nature des informations, en flux ou stockées, susceptibles d'être obtenues, qu'elles visent les correspondances proprement dites ou les métadonnées qui y sont associées ;

¹¹⁸ L'article 32, 18°, du CPCE définit les « *données relatives au trafic* » comme celles « *traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* ». Cette catégorie recouvre notamment les numéros appelés et appelants, les adresses IP, les horodatages, la durée des connexions, les protocoles utilisés. La notion de « *fadette* », ou facturation détaillée des opérateurs, héritée de la téléphonie classique et encore utilisée dans le vocabulaire des services de renseignement et d'enquête, vise précisément des données trafic (numéros, horaires, durées, acheminement), sans porter sur le contenu des échanges.

¹¹⁹ Ordonnance n° 2016-526 du 28 avril 2016 portant transposition de la directive 2014/61/UE du Parlement européen et du Conseil du 15 mai 2014 relative à des mesures visant à réduire le coût de déploiement des réseaux de communications électroniques à haut débit.

- enfin, les catégories de métadonnées auxquelles le législateur et la jurisprudence attachent, au regard du respect de la vie privée, des régimes d'accès et de conservation différenciés.

1) L'obligation de coopération imposée aux opérateurs de communication électroniques

L'effectivité de l'accès aux communications électroniques suppose que les opérateurs soient en mesure de répondre aux injonctions de la puissance publique. À cette fin, le CPCE leur impose deux séries d'obligation : d'une part, la mise en œuvre de moyens techniques permettant l'exécution des interceptions, réquisitions et autres mesures d'accès prévues par le CSI et le CPP ; d'autre part, la conservation de données dont la communication peut être requise par les autorités¹²⁰.

a) Les obligations imposées pour l'interception et la conservation des données

Si l'article L. 33-1 du CPCE affirme le principe de la liberté de l'établissement, de l'exploitation des réseaux ouverts au public et de la fourniture de services de communications électroniques, il subordonne néanmoins son exercice à l'obligation de mettre en œuvre les « *prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique* », ainsi que les mesures « *nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique* ».

- **Les obligations techniques mises à la charge des opérateurs et des fournisseurs**

Les opérateurs de communications électroniques et les fournisseurs de services numériques sont ainsi contraints de « *mettre en place et [d']assurer la mise en œuvre des moyens nécessaires* »¹²¹ pour répondre aux demandes formulées dans le cadre des techniques de renseignement et d'enquête numérique. Il n'y est dérogé que « *lorsque des obstacles techniques le justifient ou lorsque les coûts à exposer pour satisfaire à ces conditions sont disproportionnés au regard du nombre d'interceptions susceptibles d'être demandées* » à l'opérateur¹²².

¹²⁰ La mise en œuvre de ces obligations relève du Commissariat aux communications électroniques de défense (CCED), service à compétence nationale, rattaché à la direction générale des entreprises (DGE). L'arrêté du 29 décembre 2017 lui confie, sous réserve des attributions de l'ARCEP, la mission de coordonner les relations avec les opérateurs en matière de déploiement d'équipements d'interception et de mise à disposition de données, de définir les interfaces entre les équipements des opérateurs et ceux des autorités publiques ou des responsables d'établissements publics chargés d'une mission d'intérêt public, et d'établir les référentiels de prestations pouvant être demandées aux opérateurs. Il participe, en lien avec l'ANTENJ et le Groupement interministériel de contrôle (GIC), aux travaux interministériels relevant de sa compétence, ainsi qu'aux travaux de normalisation et de standardisation dans son domaine.

¹²¹ Article D. 98-7, III du CPCE.

¹²² Article 98-7, III, du CPCE : « À titre exceptionnel, il peut être dérogé à ces conditions lors de la validation par le ministre chargé des communications électroniques des choix opérés par l'opérateur et les personnes mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en application du IV après avoir recueilli l'avis de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse et de l'Agence nationale de la sécurité des systèmes d'information lorsque des obstacles techniques le justifient ou lorsque les coûts à exposer pour satisfaire à ces conditions sont disproportionnés au regard du nombre d'interceptions susceptibles d'être demandées à cet opérateur et aux personnes mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ».

Les obligations instituées par le CPCE en matière d'interceptions légales	
Opérateurs concernés par les obligations <i>15° de l'article L. 32 du CPCE</i>	Nature des obligations <i>Article D. 98-7 du CPCE</i>
- Les personnes exploitant un réseau de communications électroniques ouvert au public ; - Les fournisseurs de services de communications interpersonnelles fondés sur la numérotation, souvent dénommés OCE et MVNO¹²³ (ex. : <i>Orange, Bouygues Telecom, Free, SFR, Lebara, Lycamobile</i>) ; - Les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation (OTT)¹²⁴ (ex. : <i>Whatsapp, Signal, Messenger, Olvid, Telegram</i>) ; - Les fournisseurs d'accès à internet¹²⁵ (ex. : <i>Orange, Bouygues Telecom, Free, SFR</i>).	- Mise en place sur le territoire national (médiation¹²⁶) ; - Mise en œuvre sur le territoire national et ne pouvant pas l'être depuis l'étranger (réalisation de l'interception) ; - Utilisation d'une méthode de chiffrement validée par l'Etat pour les données transitant par l'étranger ; - Mobilisation d'agents qualifiés pour contrôler les fonctions d'interception et accéder aux données ; - Validation des dispositifs relatifs aux interceptions par l'Etat si les opérateurs souhaitent bénéficier de la juste rémunération.

Le champ d'application de ce régime juridique a progressivement été étendu. La directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen, transposée par l'ordonnance 2021-650 du 26 mai 2021¹²⁷, a intégré, au sein du CPCE, la nouvelle catégorie des « **services de communications interpersonnelles** », laquelle comprend les fournisseurs de services de messagerie instantanée, désormais soumis aux mêmes obligations de coopération que les opérateurs traditionnels de communications électroniques.

De leur côté, les articles L. 34-1 et R. 10-13 du CPCE définissent les catégories de données de connexion susceptibles d'être conservées et fixent, pour chacune d'elles, les finalités et les durées de conservation qui leur sont applicables¹²⁸.

¹²³ Article L. 32, 6° bis et 6° ter du CPCE. « OCE » pour opérateur de communications électroniques ; « MVNO » pour *Mobile virtual network operator*.

¹²⁴ 6° bis et 6° quater de l'article L. 32 du CPCE.

¹²⁵ Premier tiret du 6° de l'article L. 32 CPCE ; 1 du I. de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (dite LCEN).

¹²⁶ Les interceptions impliquent deux composantes : un système de médiation, d'une part, qui donne l'ordre d'intercepter et contient donc l'information sur la personne intéressée et le point d'interception, d'autre part, qui intercepte les communications des personnes intéressées et doit être situé dans le cœur de réseau.

¹²⁷ Ordonnance n° 2021-650 du 26 mai 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et relative aux mesures d'adaptation de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

¹²⁸ L'article R10-13 du CPCE distingue plusieurs catégories de données : « I.-Les informations relatives à l'identité civile de l'utilisateur, au sens du 1° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont : 1° Les nom et prénom, la date et le lieu de naissance pour une personne physique ou la raison sociale, ainsi que les nom, prénom, date et lieu de naissance de la personne agissant en son nom, lorsque le compte est ouvert au nom d'une personne morale ; 2° La ou les adresses postales associées ; 3° La ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant ; 4° Le ou les numéros de téléphone. II.-Les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte, mentionnées au 2° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont : 1° L'identifiant utilisé ; 2° Le ou les pseudonymes utilisés ; 3° Les données destinées à permettre à l'utilisateur de vérifier son mot de passe ou de le modifier, le cas échéant par l'intermédiaire d'un double système d'identification de l'utilisateur, dans leur dernière version mise à jour. III.-Les informations relatives au paiement mentionnées au 2° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, pour chaque opération de paiement, lorsque la souscription du contrat ou la création du compte est payante, sont : 1° Le type de paiement utilisé ; 2° La référence du paiement ; 3° Le montant ; 4° La date, l'heure et le lieu en cas de transaction physique. IV.-Les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, mentionnées au 3° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont : 1° L'adresse IP attribuée à la source de la connexion et le port associé ; 2° Le numéro d'identifiant de l'utilisateur ; 3° Le numéro d'identification du terminal ; 4° Le numéro de téléphone à l'origine de la

- **Des durées de conservation variables selon la nature des données et leurs finalités**

Les informations relatives à l'identité civile de l'utilisateur doivent être conservées « *pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale* », pendant cinq ans à compter de la fin de la validité du contrat ou, s'agissant des services prépayés, de la fin de validité du service. Les autres informations recueillies lors de la souscription d'un contrat, de la création d'un compte ou à l'occasion d'une opération de paiement sont conservées, pour les mêmes finalités, pendant un an.

Les données techniques permettant d'identifier la source de connexion ou les équipements terminaux¹²⁹ sont également conservés, pendant un an, afin de répondre – la finalité est cette fois-ci différente – aux « *besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale* ».

Enfin, les données de trafic et de localisation¹³⁰ obéissent à un régime distinct. En application de l'article L. 34-1, III., du CPCE leur conservation ne peut être imposée, par décret pris sur injonction du Premier ministre, qu'en présence d'une « *menace grave, actuelle ou prévisible* » contre la sauvegarde de la sécurité nationale, et ce pour un an. Ce dispositif doit faire l'objet d'un réexamen périodique afin de contrôler la persistance de la menace.

Les raisons de cette spécificité tiennent à la sensibilité des données concernées et aux garanties élaborées par le juge français et la Cour européenne de justice de l'Union européenne.

b) Les garanties exigées par le droit interne et le droit de l'Union européenne

Dans son arrêt *La Quadrature du Net* du 6 octobre 2020, la Cour de justice de l'Union européenne a en effet rappelé que l'article 15 de la directive « ePrivacy » 2002/58/CE du 12 juillet 2002¹³¹ « *ne s'oppose pas à une réglementation fondée sur des éléments objectifs, permettant de viser les personnes dont les données relatives au trafic et les données de localisation sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique ou encore un risque pour la sécurité nationale* »¹³².

communication. V.-Les **données de trafic et de localisation** mentionnées au III de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver sur injonction du Premier ministre, sont : 1° Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; 2° Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; 3° Les données techniques permettant d'identifier le ou les destinataires de la communication, mentionnées aux 1° à 4° du IV du présent article ; 4° Pour les opérations effectuées à l'aide de téléphones mobiles, les données permettant d'identifier la localisation de la communication. VI. - Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du CPP. »

¹²⁹ Les données techniques permettant d'identifier la source de la connexion ou les équipements terminaux utilisés recouvrent notamment l'adresse IP attribuée à l'utilisateur, au numéro de port associé, à l'identifiant de connexion de l'abonné, ainsi qu'au numéro d'identification du terminal utilisé.

¹³⁰ Les données de localisation permettent de situer géographiquement l'équipement terminal, notamment au moyen de l'identifiant de l'antenne-relais utilisée ou des changements lors des déplacements du terminal.

¹³¹ Directive « ePrivacy » 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.

¹³² CJUE, 6 octobre 2020, *La Quadrature du Net e.a ; c/ Premier ministre e.a.*, aff. Jointes C-511-18, C-512/18 et C-520-18.

Le juge européen admet ainsi un régime gradué selon la nature des données concernées.

Les données relatives à l'identité civile, de moindre sensibilité, peuvent à cet égard être conservées aux fins « *de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique* ». La conservation des adresses IP, de sensibilité plus haute dans la mesure où elles peuvent donner lieu, selon la Cour, à un « *traçage exhaustif du parcours de navigation* », doivent répondre à des finalités plus exigeantes : la prévention des menaces graves contre la sécurité publique ou encore la lutte contre la criminalité organisée.

Par sa **décision d'Assemblée *French Data Network* du 21 avril 2021**¹³³, le Conseil d'État a tiré les conséquences de cette jurisprudence en modulant, à son tour, les exigences propres à chaque catégories de données. Ainsi juge-t-il que les adresses IP doivent faire l'objet d'un régime spécifique en ce qu'« *elles ne révèlent aucune information sur les tierces personnes (...) et où elles peuvent constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée* » au moment de la commission d'une infraction. Elle relèvent dès lors de finalités fortes : la « *lutte contre la criminalité grave* », la « *prévention des menaces graves contre la sécurité publique* » et ce « *pour une période temporellement limitée au strict nécessaire* »¹³⁴. À l'instar du juge européen, la Haute Juridiction subordonne ainsi la conservation des données de trafic et de localisation à des garanties renforcées dans la mesure où elles permettent de reconstituer les déplacements, habitudes, relations et centres d'intérêt d'une personne.

Ces obligations de conservation organisent, conjointement avec l'exigence de coopération technique imposée aux opérateurs et aux fournisseurs de services rappelée plus haut, le cadre dans lequel les autorités administratives et judiciaires peuvent accéder aux données.

2) La dualité des régimes d'accès aux communications électroniques

Il n'est pas inutile de rappeler que le droit français organise l'accès aux communications selon une dualité de régimes répondant à la distinction entre police administrative et police judiciaire. Le régime administratif relève de la prévention des atteintes à l'ordre public et de la protection des intérêts fondamentaux de la Nation, sous l'autorité du Premier ministre ; le régime judiciaire est ordonné par l'autorité judiciaire et a pour finalité la constatation d'infractions graves précisées par le code de procédure pénale, la recherche de leurs auteurs et l'administration de la preuve.

Cette dualité a reçu sa première consécration législative dans la loi précitée du 10 juillet 1991, à la suite des arrêts de la Cour européenne des droits de l'homme, *Kruslin c. France* et *Huvig c. France* du 24 avril 1990, lesquels imposaient l'encadrement des interceptions de correspondances¹³⁵, et venaient compléter plusieurs arrêts de la Cour de cassation¹³⁶.

¹³³ CE, Ass., 21 avril 2021, *French Data Network* e.a.

¹³⁴ Dans son arrêt *La Quadrature du Net*, la CJUE rappelle que les adresses IP, faisant partie des données relatives au trafic, peuvent être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, permettant d'établir son profil détaillé.

¹³⁵ Il convient de rappeler que les interceptions administratives étaient pratiquées, avant la loi de 1991, sur des bases essentiellement réglementaires et administratives, tandis que les interceptions judiciaires étaient pratiquées, sous le contrôle du juge d'instruction, sur le fondement des anciens articles 81, 151 et 152 du CPP et de la jurisprudence de la Cour de cassation.

¹³⁶ Cour cass., ass. plén. du 24 novembre 1989, affaire *Baribeau*, ou encore Cour cass., crim., du 13 juin 1989.

a) Les régimes administratifs et judiciaires d'accès aux communications électroniques

Le régime administratif d'accès aux données issues des communications électroniques répond à l'objectif de défense et de promotion des intérêts fondamentaux de la Nation, tel que précisé à l'article L. 811-3 du CSI¹³⁷. Les techniques de renseignement permettent l'accès, selon des modalités strictement encadrées, au contenu des communications, aux données de connexion ainsi qu'aux données informatiques.

Chacune de ces données présente un intérêt opérationnel spécifique pour les services de renseignement. Les données de contenu permettent d'accéder aux échanges et sont susceptibles de révéler les intentions, les projets et les éléments de contexte des agissements visés. Les données de connexion permettent de reconstituer les réseaux relationnels, d'identifier les flux de communication, de localiser certains équipements ou de mettre en évidence des comportements atypiques. Les informations obtenues dans le cadre de la technique de recueil de données informatiques (RDI) permettent, en accédant à la totalité d'un système informatique, de contourner les dispositifs de sécurité, notamment le chiffrement.

- **Le cadre propre au renseignement**

Ce régime d'accès s'est constitué au rythme de l'évolution des besoins opérationnels des services de renseignement. Quatre étapes principales méritent d'être rappelées.

La loi du 10 juillet 1991 a soumis les interceptions de correspondances à l'autorisation préalable du Premier ministre, sous le contrôle d'une autorité indépendante, la Commission nationale de contrôle des interceptions de sécurité (CNCIS), devenue la Commission nationale de contrôle des techniques de renseignement (CNCTR).

La loi du 23 janvier 2006 relative à la lutte contre le terrorisme a marqué une première extension du dispositif en instituant un régime autonome d'accès administratif aux données de connexion, distinct des interceptions de sécurité. Le législateur retient alors que l'accès à ces données, moins intrusif que celui portant sur le contenu des communications, peut relever d'un cadre juridique différencié, tout en demeurant soumis à contrôle strict¹³⁸.

La loi de programmation militaire du 18 décembre 2013¹³⁹, dans un contexte d'accélération des usages numériques, a étendu ce dispositif à l'ensemble des services de renseignement habilités et introduit la possibilité d'un recueil en temps réel des données de connexion.

¹³⁷ Article L. 811-3, al. 1 du CSI : « Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation (...). »

¹³⁸ L'article 6, I., de la loi a créé un nouvel article 34-1-1 du CPCE autorisant les agents habilités à exiger des opérateurs, aux fins de la prévention des actes de terrorisme, la communication de certaines techniques conservées au titre de l'article L. 34-1. Le texte énumère limitativement les données accessibles : identification des numéros d'abonnement ou de connexion ; recensement des numéros d'une personne ; localisation des terminaux ; liste des numéros appelés et appelants ; date et durée des communications. En parallèle, le III. de l'article 6 modifie la loi du 10 juillet 1991 en créant un titre IV intitulé « Communication des données techniques relatives à des communications électroniques », instituant, à côté du régime des interceptions de sécurité, un régime autonome de communication administrative des données techniques. Cette architecture sera reprise par la loi de 2015.

¹³⁹ 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.

Enfin, l'importante loi du 24 juillet 2015 relative au renseignement¹⁴⁰ a procédé à une refonte d'ensemble du régime, codifié au livre VIII du CSI. Elle a placé dans un cadre commun d'autorisation et de contrôle les interceptions de correspondances et l'accès aux données de connexion, tout en encadrant de nouvelles techniques adaptées aux communications numériques (le recueil technique de données de connexion, la détection algorithmique de connexions susceptibles de révéler une menace terroriste, notamment).

- **Des finalités strictement définies par le législateur**

Le recours aux techniques de renseignement est subordonné aux sept finalités définies par l'article L. 811-3 du CSI : l'indépendance nationale, l'intégrité du territoire et la défense nationale (finalité 1) ; les intérêts majeurs de la politique étrangères et la prévention des ingérences étrangères (finalité 2) ; les intérêts économiques, industriels et scientifiques majeurs de la France (finalité 3) ; la prévention du terrorisme (finalité 4) ; la prévention des atteintes à la forme républicaine des institutions ou encore des violences collectives de nature à porter atteinte à la paix publique (finalité 5) ; la prévention de la criminalité et de la délinquance organisées (finalité 6) ; ainsi que la prévention de la prolifération des armes de destruction massive (finalité 7).

Ces techniques sont réservées aux services de renseignement désignés par les articles L. 811-1 et R. 811-2 du même code : les services de « premier cercle » ou services spécialisés de renseignement¹⁴¹, ainsi que les services disposant d'habilitations ciblées sur certaines finalités ou certaines techniques de renseignement¹⁴². Plusieurs de ces services ont été auditionnés par la mission.

- **Une mise en œuvre centralisée et soumise à un double contrôle**

La mise en œuvre des techniques de renseignement est autorisée par le Premier ministre, après avis de la CNCTR, conformément aux articles L. 821-1 et suivants du CSI. Les autorisations, nécessairement écrites et motivées, sont délivrées pour une durée limitée et leur renouvellement est subordonné à une nouvelle appréciation de leur nécessité. Leur exécution technique est, pour l'essentiel, assurée par le Groupement interministériel de contrôle (GIC), service à compétence nationale placé sous l'autorité du Premier ministre et adossé au SGDSN.

¹⁴⁰ Loi n° 2015-92 du 24 juillet 2015 relative au renseignement.

¹⁴¹ 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) ; la Direction nationale du renseignement et des enquêtes douanières (DNRED) ; ainsi que TRACFIN.

¹⁴² On rappellera que les services dits du « second cercle », contrairement aux six services spécialisés, n'est pas uniquement constituée de services de renseignement mais comprend des services de police judiciaire, de police aux frontières, de gendarmerie et de l'administration pénitentiaire, auxquels seules certaines techniques de renseignement sont ouvertes, et uniquement pour les finalités expressément prévues par le législateur.

Techniques de renseignement et messageries chiffrées « de bout en bout » au sein du CSI		
Catégorie	Technique de renseignement (TR)	Base juridique
Accès administratif aux données de connexion	Accès aux données de connexion en temps différé	Article L. 851-1
	Accès aux données de connexion en temps réel	Article L. 851-2
	Localisation en temps réel des équipements terminaux	Article L. 851-4
	Localisations des personnes ou des objets	Article L. 851-5
	Recueils de données de connexion par <i>IMSI-catcher</i>	Article L. 851-6
Interceptions de sécurité	Interceptions de sécurité via le GIC	I de l'article L. 852-1
	Interceptions des communications par <i>IMSI-catcher</i>	II de l'article L. 852-1
	Interceptions de sécurité sur les réseaux exclusivement hertziens	Article L. 852-2
	Interceptions de correspondances émises ou reçues par la voie satellitaire	Article L. 852-3
Sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques	Captations de paroles prononcées à titre privé et captations d'images dans un lieu privé	Article L. 853-1
	Recueils et captations de données informatiques	Article L. 853-2
	Introductions dans des lieux privés	Article L. 853-3

La CNCTR exerce un contrôle permanent *a priori* des techniques de renseignement et dispose, en application de l'article L. 833-1 du CSI, d'un accès direct aux demandes d'autorisation, aux renseignements collectés ainsi qu'aux dispositifs de traçabilité. Ses rapports annuels d'activité font état de 98 883 demandes examinées en 2024 et de 100 813 en 2025, pour 24 308 individus surveillés en 2024 et 25 332 en 2025 (+10,3% entre 2021 et 2025), soit 0,03 % de la population nationale.

Le contrôle juridictionnel est exercé par le Conseil d'État, dans les conditions prévues à l'article L. 841-1 du CSI¹⁴³. Toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard peut ainsi saisir la Haute Juridiction, après avoir préalablement saisi d'une réclamation la CNCTR. Cette dernière peut elle-même saisir la juridiction administrative lorsqu'elle estime insuffisantes les suites données à ses avis ou recommandations. Elle y est même tenue dans le cas où le Premier ministre ne suivrait pas l'avis défavorable qu'elle émet quant à l'utilisation d'une technique de renseignement¹⁴⁴. Le Conseil d'État peut également être saisi d'une question par un juge judiciaire ou administratif lorsque celui-ci s'interroge, dans le cadre d'une affaire en cours, sur la régularité d'une ou plusieurs techniques de recueil de renseignement¹⁴⁵.

Le nombre de réclamations présentées devant la CNCTR illustre la montée en puissance du contrôle *a posteriori* exercé sur les techniques de renseignement qui a dépassé, en 2025, le seuil symbolique de 100 par an, soit une augmentation 20,7% par rapport à 2024. Les recours devant le

¹⁴³ Le contentieux des techniques de renseignement, compétence de premier et dernier ressort, se rattache alors à l'excès de pouvoir (CE 4 février 2022, *Leferrec*, n° 456914, *Lebon T.* 853).

¹⁴⁴ Article L. 821-1, al. 2, du CSI.

¹⁴⁵ Article L. 841-1, al. 5, du CSI.

Conseil d'État demeurent toutefois limités : 9 requêtes ont été communiquées à la CNCTR par la Haute Juridiction en 2025¹⁴⁶.

- **Les interceptions de sécurité**

L'accès au contenu des communications repose principalement sur les interceptions classiques de sécurité prévues à l'article L. 852-1 du CSI : « *Dans les conditions prévues au présent titre, peuvent être autorisées les interceptions de correspondances émises par la voie des communications électroniques et susceptibles de révéler des renseignements relatifs aux finalités mentionnées à l'article L. 811-3* ». Elles permettent l'accès au contenu des correspondances échangées par la voie des communications électroniques¹⁴⁷.

- **L'accès aux données de connexion**

Le livre VIII du CSI distingue les interceptions de sécurité des techniques d'accès aux données de connexion. L'article L. 851-1 autorise ainsi « *le recueil, auprès des opérateurs de communications électroniques (...), des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques (...)* ». Ces données peuvent notamment porter sur l'identification des abonnements et des équipements, les numéros appelés et appelants, les dates et durées de communication ainsi que sur les connexions réalisées et certaines données de localisation.

À ce dispositif général s'ajoutent plusieurs techniques spécialisées.

L'article L. 851-3 du CSI autorise, pour les seules finalités 1, 2 et 4 de la prévention du terrorisme, la mise en œuvre de traitements automatisés portant sur les données de connexion détenues par les opérateurs et les fournisseurs de services, afin de détecter des connexions susceptibles de révéler une menace terroriste. Le dispositif repose sur l'application à grande échelle de critères de détection préalablement autorisés, et non sur la surveillance d'une personne déterminée. Les données recueillies peuvent faire l'objet d'une levée d'anonymat dans les conditions prévues par la loi.

L'article L. 851-5 du CSI permet le recueil en temps réel des données de connexion d'une personne, d'un véhicule ou d'un objet préalablement identifié. Contrairement à l'article L. 851-1, qui porte principalement sur des données déjà traitées ou conservées par les opérateurs, cette technique permet le suivi des données au fur et à mesure de l'utilisation des réseaux.

Les articles L. 851-6 et L. 851-7 du CSI autorisent également l'utilisation de dispositifs techniques permettant de recueillir certaines données de connexion directement auprès des équipements terminaux présents dans une zone déterminée (« *IMSI-catchers* »¹⁴⁸).

¹⁴⁶ Les décisions rendues par la formation spécialisée du Conseil d'État sont publiques mais ne peuvent révéler des éléments couverts par le secret de la défense nationale. Les règles de communication des documents et de restriction du contradictoire sont en effet spécifiques : v. les articles L. 773-1 et s. ainsi que les articles R. 773-7 et s., de même que les décisions CE 19 octobre 2016, *Sottani*, n° 400688, *Lebon*, et CE 16 juin 2021, *M.A.*, n°430061, inédit, pt. 6.

¹⁴⁷ À côté des interceptions réalisées sur le territoire national, les articles L. 854-1 et suivants du CSI organisent un régime spécifique applicable à la surveillance des communications électroniques internationales. L'article L. 854-1 prévoit ainsi que peut être autorisée, aux seules fins de la défense et de la promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, la surveillance des communications émises ou reçues à l'étranger.

¹⁴⁸ Un « *IMSI-catcher* » (*International Mobile Subscriber Identity Catcher*) est un dispositif technique qui imite le fonctionnement d'une antenne-relais de téléphonie mobile afin d'inciter les terminaux situés à proximité à s'y connecter temporairement. Cette

- **Le recueil et la captation de données informatiques (RDI)**

L'article L. 853-2 du CSI a pour objet l'accès à des données informatiques présentes sur un système informatique ou accessibles depuis celui-ci. Cette technique – subsidiaire par principe et tenue au principe de nécessité et de proportionnalité – est subordonnée à l'impossibilité de recueillir les renseignements par d'autres moyens autorisés¹⁴⁹. Ainsi que le rappelle la CNCTR dans son rapport d'activité pour l'année 2025, « *la demande de RDI présentée par un service de renseignement portera sur un ou plusieurs appareils de la personne visée et l'autorisation délivrée permettra de capter toutes les données dans ces appareils* »¹⁵⁰, qu'il s'agisse d'une « tablette », d'un ordinateur ou d'un téléphone.

Il est à noter que la durée des autorisations relatives au RDI est moindre (deux mois), du fait de son caractère intrusif, que celle des autorisations relatives aux interceptions de sécurité (quatre mois). Il en ressort que **lorsque ces techniques sont concomitamment utilisées sur une même personne, une demande de renouvellement du RDI sera nécessaire pour accompagner la mesure d'interception classique**, sans que le législateur n'ait prévu de moduler cette durée d'autorisation en fonction de la technique de renseignement qu'elle vient le cas échéant compléter et de l'atteinte à la vie privée qu'elle est susceptible de provoquer. Nous y reviendrons dans la suite du présent rapport.

• **Le régime judiciaire : la dématérialisation accélérée de l'enquête pénale**

Dans ses travaux sur les investigations numériques en procédure pénale¹⁵¹, M. Bruno Roussel relève que la recherche de la preuve mobilise désormais, de manière croissante, des données produites, stockées ou transmises par des systèmes informatiques. **Les « traces numériques » laissées à l'occasion de l'utilisation des réseaux et des services numériques occupent ainsi une place centrale dans les investigations judiciaires**. Il en résulte une transformation profonde des investigations en environnement chiffré « de bout en bout », en particulier dans les nombreux cas de figure que nous avons exposé plus haut où les ramifications numériques s'avèrent complexes.

L'importance opérationnelle des données numériques se reflète dans l'activité de la PNIJ. Dans son rapport d'information du 20 novembre 2025, consacré aux frais de justice, le sénateur Antoine Lefèvre observait qu'« **en 2024, la PNIJ a servi plus de 3,5 millions de prestations, en hausse de 10,9 % sur un an** »¹⁵², illustrant le recours croissant des enquêteurs aux réquisitions de données, aux interceptions de correspondances et aux autres techniques d'enquête numérique¹⁵³.

connexion permet de recueillir certains identifiants techniques des équipements détectés, notamment l'IMSI de la carte SIM ou l'IMEI du terminal, ainsi que, dans les conditions prévues par la loi, certaines données techniques de connexion. Dans le droit du renseignement, les articles L. 851-6 et L. 851-7 du CSI autorisent l'utilisation de tels dispositifs afin d'identifier des équipements présents dans une zone déterminée, de localiser un terminal recherché ou de recueillir certaines données de connexion. Ils ne permettent pas, en eux-mêmes, d'accéder aux données stockées sur le téléphone ni au contenu des communications.

¹⁴⁹ L'article L. 853-2, I, du CSI précise en effet que le recueil de données informatique ne peut être autorisé, pour deux mois, renouvelable sur demande motivée du service dans les mêmes limites de durée, que « *lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé* ».

¹⁵⁰ Rapport d'activité 2025, CNCTR.

¹⁵¹ Bruno Roussel, *Les investigations numériques en procédure pénale*, Thèse de doctorat, Université de Bordeaux, 2020.

¹⁵² On rappellera toutefois, et ce n'est pas neutre, que les fournisseurs de messageries chiffrées, lorsqu'ils n'ont pas d'existence légale en France, ne sont pas raccordés à la PNIJ.

¹⁵³ Antoine Lefèvre, *Frais de justice*, Rapport d'information fait au nom de la Commission des finances, Sénat, 1^{er} octobre 2025.

Comme pour toute investigation, le contenu même des communications présente une valeur probatoire cardinale : les échanges textuels ou vocaux peuvent révéler la commission d'une infraction et l'intentionnalité de son auteur ; ils offrent des informations permettant d'éclairer les comportements observés, les modalités d'un passage à l'acte, l'identification d'éventuels complices ou la démonstration de manœuvres frauduleuses.

Dans leur rapport d'information intitulé « *Surveiller pour punir ? Pour une réforme de l'accès aux données de connexion dans l'enquête pénale* », les sénateurs Agnès Canayer et Philippe Bonnacarrère relèvent ainsi que **les données de connexion sont désormais « présentes dans 85 % des enquêtes pénales »**, tous types d'infractions confondus, et « *dans l'intégralité des procédures liées à la criminalité organisée* ». Ces données jouent par conséquent un rôle décisif dans la conduite des investigations et l'élucidation des crimes comme des délits¹⁵⁴.

Les services d'enquête judiciaire ont toutefois souligné, auprès de la mission, que **les données de connexion, si elles permettent de reconstituer les environnements relationnels et matériels dans lesquels s'inscrivent les comportements délinquants, présentent une valeur probatoire inférieure à celle du contenu des correspondances**. L'ANTENJ relève, à cet égard, que « *les métadonnées sont utiles pour établir un faisceau d'indices par recoupements* »¹⁵⁵. De son côté, la DGGN observe qu'il conviendrait que les services enquêteurs aient accès à « *davantage de métadonnées* »¹⁵⁶, tout en soulignant les difficultés liées à leur traitement volumétrique¹⁵⁷. Ces observations ne sont contradictoires qu'en apparence. Si la valeur probatoire des données de connexion demeure inférieure à celle des données de contenu, l'inaccessibilité de ces dernières en présence d'un chiffrement « de bout en bout » conduit les enquêteurs à déporter leurs investigations sur les métadonnées, qui constituent désormais la principale matière numérique disponible.

Dans cet environnement, le code de procédure pénale prévoit plusieurs techniques permettant aux services enquêteurs d'accéder aux communications électroniques et aux données qui leur sont associées. Elles relèvent, selon les cas, du droit commun de l'enquête ou de l'information judiciaire, ou sont réservées à la lutte contre certaines formes de criminalité grave.

- **Les interceptions de correspondances en flux ou stockées**

Les correspondances peuvent être recueillies en flux, pendant leur transmission, le code de procédure pénale prévoyant à cette fin deux régimes juridiques dont les conditions de mise en œuvre varient selon le stade de la procédure pénale et, dans certains cas, selon la nature des infractions poursuivies.

¹⁵⁴ Agnès Canayer et Philippe Bonnacarrère, *Surveiller pour punir ? Pour une réforme de l'accès aux données de connexion dans l'enquête pénale*, Rapport d'information fait au nom de la Commission des lois, Sénat, 15 novembre 2023.

¹⁵⁵ Audition du 18 février 2026.

¹⁵⁶ Audition du 24 février 2026.

¹⁵⁷ V. à cet égard la seconde partie du présent rapport.

Techniques d'enquête et messageries chiffrées « de bout en bout » au sein du CPP	
Catégorie	Base juridique
Interception des correspondances émises par la voie des communications électroniques (accès au flux à partir de l'autorisation).	Articles 100 à 100-8 et 706-95
Réquisitions aux fins de communication des données de connexion.	Articles 60-1-2, 77-1-1 et 99-3
Perquisition (données stockées dans un support numérique ou à distance en lien avec ce support).	Articles 56, 57-1, 76 et 97 et suivants
Mise au clair des données chiffrées.	Articles 230-1 à 230-5
Géolocalisation.	Articles 230-32 à 230-44
Technique spéciale d'enquête - Accès à distance aux <u>correspondances</u> stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique (stock avant l'autorisation).	Articles 706-95-1 à 706-95-3
Technique spéciale d'enquête - Captation des <u>données informatiques</u> .	Articles 706-102-1 à 706-102-5

Sans prétendre être exhaustif, au cours de l'information judiciaire, les interceptions sont régies par les articles 100 à 100-7 du code de procédure pénale. L'article 100 prévoit qu'« *en matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques.* »

Ce régime de droit commun relève de la compétence du juge d'instruction et n'est applicable qu'aux infractions punies d'au moins trois ans d'emprisonnement.

La décision d'interception est entourée de garanties substantielles. En application de l'article 100-1 du même code, elle doit être motivée « *par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires* » et comporter « *tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci* ».

L'autorisation initiale est limitée à une durée maximale de quatre mois, sans que la durée totale de l'interception puisse excéder un an pour le droit commun, deux ans pour les affaires relevant de la criminalité et de la délinquance organisées¹⁵⁸. L'article 100-4 impose, en outre, l'établissement d'un procès-verbal pour chaque opération d'interception et d'enregistrement, mentionnant « *la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée* ».

Par dérogation au régime de droit commun, certaines infractions, relevant notamment de la criminalité organisée ou du terrorisme¹⁵⁹, justifient le recours aux interceptions dès le stade de l'enquête de flagrance ou de l'enquête préliminaire. En application de l'article 706-95 du code de

¹⁵⁸ Article 100-2 du CPP.

¹⁵⁹ Sont ainsi visées les infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 du CPP.

procédure pénale¹⁶⁰, le juge des libertés et de la détention, saisi par requête du procureur de la République, peut autoriser « *l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques* », pour une durée maximum d'un mois renouvelable une fois. Le procureur de la République informe sans délai le juge des libertés et de la détention des actes accomplis en exécution de son autorisation.

À côté des interceptions de correspondances en flux, les articles 706-95-1 à 706-95-3 du code de procédure pénale organisent, sans limitation de durée, le régime d'accès aux correspondances stockées¹⁶¹ par la voie de communications électroniques et accessibles au moyen d'un identifiant informatique¹⁶². Relèvent de ce régime des courriels conservés dans une boîte de messagerie, des messages enregistrés dans un service de messagerie instantanée ou encore des conversations conservées dans un espace de stockage associé à compte utilisateur.

Lorsque les investigations sont conduites dans le cadre d'une information judiciaire, l'article 706-95-2 du code de procédure pénale confie cette compétence au juge d'instruction qui peut autoriser l'accès à distance, à l'insu de la personne visée, par ordonnance motivée et dans le cadre d'infractions relevant notamment de la criminalité et de la délinquance organisées, aux correspondances stockées, lesquelles peuvent être saisies, enregistrées ou copiées sur tout support. Pour les mêmes infractions, le juge des libertés et de la détention peut autoriser, au stade de l'enquête de flagrance ou de l'enquête préliminaire, à la requête du procureur de la République et par ordonnance motivée, l'accès à distance aux correspondances stockées.

La distinction entre le régime applicable aux correspondances en flux et celui des correspondances conservées est utile pour apprécier les effets du chiffrement sur les capacités d'investigation. Ces deux techniques peuvent, en effet, viser un même contenu, mais à des stades distincts du cycle d'échange numérique : lors de sa transmission ou après son enregistrement. Dès lors que le chiffrement a pour objet de protéger les échanges entre les deux extrémités de la communication, ses conséquences peuvent différer selon que l'autorité entend accéder à un contenu en cours d'acheminement ou déjà stocké.

- **Les réquisitions judiciaires génériques et leur adaptation aux données de connexion**

Peuvent par ailleurs être requises les données techniques détenues par les opérateurs de communications électroniques, les fournisseurs de services ou, plus largement, par toute personne, tout organisme ou toute administration susceptible de détenir des informations utiles à la manifestation de la vérité. Leur régime varie selon le stade de la procédure pénale.

¹⁶⁰ On rappellera que la loi dite « Perben II » du 9 mars 2004 a introduit l'article 706-95 CPP afin d'étendre les interceptions judiciaires, prérogative restée propre au juge d'instruction depuis la loi du 10 juillet 1991, aux enquêtes portant sur la criminalité organisée. Les travaux préparatoires montrent que le législateur entendait alors procéder avec prudence, imposant des conditions plus strictes qu'au stade de l'information judiciaire (contrôle préalable du juge des libertés et de la détention, durée plus brève, renouvellement limité). Ces restrictions sont également ajustées aux prescriptions de la CEDH dans ses arrêts *Kruslin c. France* et *Huvig c. France* du 24 avril 1990.

¹⁶¹ Ces correspondances sont dites « stockées » lorsqu'elles sont antérieures à la décision judiciaire autorisant leur accès.

¹⁶² On se souvient que la notion d'interception avait pu être interprétée comme couvrant l'ensemble des messages envoyés à une personne, y compris ceux archivés et donc stockés. Un arrêt rendu par la Cour de cassation le 8 juillet 2015 y avait mis fin. La Cour avait en effet soumis la saisie des correspondances antérieures à une décision d'interception au régime des perquisitions, laquelle impliquait l'information préalable et la présence de la personne concernée, à la différence des interceptions de correspondances en flux. L'article 2 de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement est venue corriger cette lacune.

L'article 60-1 du code de procédure pénale qui fixe le **régime de « réquisition générique »**, confère au procureur de la République ou à l'officier de police judiciaire ou, sous son contrôle, à l'agent de police judiciaire, le pouvoir de requérir de *« toute personne, tout établissement ou organisme privé ou public ou de toute administration publique (...) susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives »*, afin de lui remettre ces informations, *« sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel »*. L'abstention de réponse de la part du requis est constitutive d'un délit puni d'une peine d'amende¹⁶³.

L'accès judiciaire aux données de connexion appelle, à court terme, une mise en conformité législative

La jurisprudence de la Cour de justice de l'Union européenne a profondément renouvelé les conditions d'accès aux données de connexion. En distinguant les règles applicables à leur conservation de celles qui gouvernent leur communication aux autorités publiques, elle a précisé le degré d'ingérence attaché aux différentes catégories de données, les finalités susceptibles de justifier leur accès ainsi que les garanties procédurales qui doivent entourer leur utilisation.

Cette évolution a conduit le législateur français à adapter, dans un premier temps, le régime de conservation prévu par l'article L. 34-1 du CPCE. L'article 17 de la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement a ainsi redéfini les catégories de données susceptibles d'être conservées, les finalités justifiant leur conservation ainsi que les durées applicables.

Dans un second temps, l'article 12 de la loi du 2 mars 2022 visant à combattre le harcèlement scolaire a introduit dans le CPP un nouvel article 60-1-2 afin d'encadrer les réquisitions portant sur les données techniques permettant d'identifier la source d'une connexion ou les équipements terminaux utilisés, ainsi que les données de trafic et de localisation. L'article 60-1-2 réserve ainsi ces réquisitions, à peine de nullité, à quatre catégories de situations : lorsqu'elles sont nécessaires à la constatation d'un crime ou d'un délit puni d'au moins trois ans d'emprisonnement ; lorsqu'elles ont pour seul objet d'identifier l'auteur d'un délit commis au moyen d'un réseau de communications électroniques et puni d'une peine d'emprisonnement ; lorsqu'elles portent, à la demande de la victime, sur l'équipement terminal qu'elle utilise ; ou lorsqu'elles interviennent dans le cadre des procédures de recherche des causes de la mort, d'une disparition inquiétante ou la recherche d'une personne disparue.

Cette réforme n'a toutefois répondu qu'imparfaitement aux exigences résultant du droit de l'Union européenne.

Par son arrêt *Prokuratuur* du 2 mars 2021, la Cour a en effet jugé que l'accès des autorités publiques aux **données de trafic et de localisation**, dès lors qu'il permet de tirer des conclusions sur la vie privée des personnes concernées, devait, lorsqu'il est sollicité à des fins pénales, non seulement être réservé à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, mais être soumis au **contrôle préalable d'une juridiction ou d'une autorité administrative indépendante**.

Tirant les conséquences de cette jurisprudence, la chambre criminelle de la Cour de cassation a jugé, par quatre arrêts du 12 juillet 2022, que les articles 60-1, 60-2, 77-1-1 et 77-1-2 du CPP étaient incompatibles avec le droit de l'Union européenne. Ce dernier s'oppose, en effet, à ce que l'autorisation d'accès soit donnée par le ministère public lorsqu'il dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. La Cour ajoute qu'un fonctionnaire de police ne présente pas davantage les garanties d'indépendance et d'impartialité requises. Elle isole, toutefois, la situation du **juge d'instruction** en ce qu'il n'est pas partie à la procédure, n'exerce pas l'action publique et statue de façon indépendante.

Cette jurisprudence a conduit les juridictions du fond à exercer un **contrôle renforcé des réquisitions portant sur les données de connexion**. Ainsi, par un arrêt du 4 juillet 2024, la cour d'appel de Grenoble a annulé une réquisition portant sur des données de géolocalisation historiques¹⁶⁴ obtenues auprès d'un opérateur de téléphonie mobile sur le seul fondement que l'autorisation était délivrée par le procureur de la République, estimant que les exigences résultant du droit de l'Union n'étaient pas satisfaites.

¹⁶³ Article 60-1, al. 3 CPP.

¹⁶⁴ Les données de géolocalisation historique ou géolocalisation à temps différé renvoient à des données de localisation conservées par l'opérateur, permettant de reconstituer

La jurisprudence issue de l'arrêt *Prokuratuur* a suscité d'importants travaux. À cet égard, **le rapport d'information sur les données de connexion des sénateurs Agnès Canayer et Philippe Bonnacarrère** avaient relevé que la mise en conformité du droit français impose d'aménager le contrôle préalable de l'accès aux données de trafic et de localisation.

Le rapport sénatorial envisageait plusieurs orientations, parmi lesquelles la désignation du juge des libertés et de la détention comme autorité d'autorisation de droit commun pour ces données, le maintien d'un régime distinct pour les seules données d'identification, ainsi que l'instauration d'une procédure d'urgence assortie d'un contrôle juridictionnel *a posteriori*¹⁶⁵.

La mission observe que les risques de nullité pesant sur les réquisitions judiciaires invitent le législateur à mettre rapidement le droit positif en conformité avec les exigences fixées par la Cour de Justice de l'Union européenne, justifiant la recommandation n° 2 figurant ci-dessous.

L'article 60-2 du même code complète ce dispositif pour les **réquisitions aux fins de remise de données informatiques, exécutées par voie télématique ou informatique, ou « réquisitions rapides » de données**. Les organismes publics et les personnes morales de droit privé, administrant un système informatique ou un traitement de données à caractère personnel, sont en effet tenues de mettre à disposition « **les informations utiles à la manifestation de la vérité** » qu'ils détiennent, « à l'exception de celles protégées par un secret prévu par la loi¹⁶⁶ ».

Le même article prévoit que, sur réquisition du procureur de la République, préalablement autorisé par le juge des libertés et de la détention, les opérateurs de communications électroniques peuvent être tenus de prendre, sans délai, toutes mesures propres à assurer, pendant une durée maximale d'un an, **la préservation du contenu des informations consultées par les utilisateurs** de leurs services. Le refus de répondre est, là-aussi, puni d'une amende.

En enquête préliminaire, l'article 77-1-1 du code de procédure pénale organise un régime de réquisition analogue, sous l'autorité du procureur de la République. Enfin, au cours de l'information judiciaire, l'article 99-3 du même code permet au juge d'instruction, ou à l'officier de police judiciaire commis par lui, de requérir la remise rapide de tous documents intéressant l'information, y compris ceux issus d'un système informatique ou d'un traitement de données à caractère personnel.

- **L'exigence par le juge constitutionnel d'un contrôle préalable par une « juridiction indépendante »**

Le législateur a toutefois adapté le régime de réquisition de droit commun aux données de connexion, fruit d'une censure du Conseil constitutionnel. Saisi d'une question prioritaire de constitutionnalité (QPC), portant sur les articles 77-1-1 et 77-1-2 du code de procédure pénale, le juge constitutionnel était appelé à se prononcer sur la compatibilité de ces dispositions avec le droit de l'Union européenne, les principes de respect de la vie privée et de recours juridictionnel effectif.

La QPC interrogeait en particulier la possibilité pour le procureur, dans le cadre de l'enquête préliminaire, de **requérir sans contrôle préalable d'une juridiction indépendante** les informations

¹⁶⁵ Sénat, Commission des lois, Rapport d'information sur les données de connexion : préserver un équilibre entre sécurité et liberté, 2023.

¹⁶⁶ Secret médical, professionnel, des sources des journalistes, et c.

issues d'un système informatique ou d'un traitement de données personnelles, parmi lesquelles figurent les données de connexion.

Relevant que la réquisition de ces données était autorisée « *dans le cadre d'une enquête préliminaire qui peut porter sur tout type d'infraction et qui n'est justifiée par l'urgence ni limitée dans le temps* », le Conseil constitutionnel avait censuré les mots « *y compris celles issues d'un système informatique ou d'un traitement de données nominatives* », figurant à la première phrase du premier alinéa de l'article 77-1-1 du code de procédure pénale, ainsi que les mots « *aux réquisitions prévues par le premier alinéa de l'article 60-2* », figurant au premier alinéa de l'article 77-1-2 du même code¹⁶⁷.

La loi n° 2002-299 du 2 mars 2002 visant à combattre le harcèlement scolaire a cherché à tirer les conséquences de cette censure en créant l'article 60-1-2 du code de procédure pénale¹⁶⁸. Celui-ci soumet désormais, à peine de nullité, les réquisitions portant sur certaines données de connexion (données permettant d'identifier la source de connexion ou relatives aux équipements terminaux, données de trafic et données de localisation) à des conditions particulières tenant à la nature ou à la gravité de l'infraction. Leur réquisition n'est donc possible, lorsque les nécessités de la procédure l'exigent, que dans quatre hypothèses : un crime ou un délit puni d'au moins trois ans d'emprisonnement ; l'identification de l'auteur d'un délit puni d'au moins un an d'emprisonnement commis par l'utilisateur d'un réseau de communications électroniques ; les équipements terminaux de la victime d'un délit puni d'une peine d'emprisonnement, à la demande de celle-ci ; ainsi que la découverte d'une personne disparue ou dans le but de retracer le parcours criminel d'une personne dans le domaine de criminalité sérieuse ou non élucidée.

Cet encadrement se voulait une réponse au caractère particulièrement intrusif de ces données, le Conseil constitutionnel ayant relevé dans sa décision de 2021 précitée qu'elles sont susceptibles de fournir, sur les personnes concernées et, le cas échéant, sur des tiers, « *des informations nombreuses et précises, particulièrement attentatoires à leur vie privée* ».

Malgré les garanties apportées par le législateur, la mission observe que la mise en conformité de notre droit avec les exigences européennes demeure toutefois inachevée (v. encadré ci-dessus).

Recommandation n° 2 : Acheter l'adaptation du régime des réquisitions judiciaires de données de connexion aux exigences du droit de l'Union européenne, en présentant un projet de texte législatif s'inspirant notamment des orientations formulées par le rapport Canayer-Bonnecarrère.

¹⁶⁷ Cons. const., 3 décembre 2021, n° 2021-952 QPC, la censure étant alors reportée au 31 décembre 2022.

¹⁶⁸ Dans leur ouvrage de procédure pénale, MM. S. Guinchard et J. Buisson observent toutefois que le législateur est allé au-delà de la censure du Conseil constitutionnel. Alors que ce dernier avait écarté les dispositions prévoyant la réquisition de données de connexion dans le seul cadre de l'enquête préliminaire, au motif de l'absence d'urgence, le législateur a choisi d'étendre le nouveau régime à l'enquête de flagrance qui ne paraissait pas en cause dans la motivation de la décision. « *En sorte que* », concluent les auteurs, « *le législateur paraît avoir introduit davantage de complexité en cette matière (comme dans d'autres...) et méconnu l'urgence, réelle dans le cadre d'une enquête de flagrance, pour des infractions punies de peine d'emprisonnement inférieure à trois ans* ». S. Guinchard et J. Buisson, *Procédure pénale*, LGDJ, 17^e édition, 2024.

- La captation des données informatiques

Régie par les articles 706-102-1 à 706-102-5 du code de procédure pénale, la « *captation des données informatiques* » a été introduite par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2). À l'image du RDI en matière de renseignement, elle permet pour certaines formes de criminalité grave¹⁶⁹ d'accéder, à l'insu de la personne concernée, aux données contenues dans un système informatique¹⁷⁰.

Dans sa conception initiale, cette technique visait les données telles qu'elles s'affichent sur un écran ou sont introduites par saisie de caractères¹⁷¹. La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme l'a étendue aux données reçues ou émises par des périphériques audiovisuels (microphones, *webcams* et autres dispositifs permettant des communications « audio » ou « vidéo »).

La loi du 3 juin 2016 a franchi une nouvelle étape en permettant l'accès aux données stockées dans un système informatique et en l'étendant aux enquêtes de flagrance ou préliminaires. La réforme a ainsi permis d'inclure les données stockées sur des services de type « *cloud* ».

Enfin, la loi du 23 mars 2019 de programmation 2018-2022 et de réforme de la justice (LOPJ) a intégré la captation de données informatiques au régime de droit commun des techniques spéciales d'enquête¹⁷². À peine de nullité, la décision de mise en œuvre doit préciser « *l'infraction qui motive le recours à ces opérations ainsi que la durée de ces dernières* »¹⁷³.

Lorsque l'installation du dispositif technique l'exige, l'article 706-102-5 du code de procédure pénale autorise son introduction dans un véhicule ou un lieu privé. Le dispositif peut également être transmis par un réseau de communications électroniques¹⁷⁴.

¹⁶⁹ On se souvient que le Conseil constitutionnel, dans sa décision n° 2019-778 DC du 21 mars 2019, avait censuré l'extension des techniques spéciales d'enquête, dans le cadre d'une enquête de flagrance ou préliminaire, à « *tout crime* », le législateur ayant prévu à l'article 46 de la loi de programmation 2018-2022 et de réforme de la justice d'en étendre le périmètre au-delà des seules infractions relevant de la criminalité et de la délinquance organisées (cons. n° 165). Le Conseil avait en effet jugé que « *si une infraction d'une particulière gravité et complexité est susceptible de justifier le recours à de telles mesures, tel n'est pas nécessairement le cas d'infractions ne présentant pas ces caractères* ». En revanche, le Conseil semblait ne pas écarter l'extension des techniques spéciales d'enquête au-delà des infractions les plus graves à la condition d'un contrôle renforcé par le juge des libertés et de la détention (v. en ce sens le cons. n° 163).

¹⁷⁰ L'article 706-102-1 du CPP définit comme consistant 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 l'écran pour l'utilisateur dans 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* ».

¹⁷¹ Sont ainsi visées les données au moment où elles sont frappées au clavier (physique ou virtuel), avant leur traitement par le système informatique, qu'il s'agisse d'un texte dans une messagerie instantanée, d'un courriel en cours de rédaction, d'une recherche dans un navigateur, d'une URL, d'un identifiant ou d'un mot de passe, d'une commande saisie dans un terminal ou encore de tout texte saisi dans une application.

¹⁷² Articles 706-95-11 à 706-95-19 du CPP.

¹⁷³ Article 706-102-5 du CPP.

¹⁷⁴ L'article 706-102-5 du CPP exclut toutefois les systèmes de traitement automatisé de données situés dans les cabinets ou domiciles des avocats, les locaux des entreprises de presse, des services de presse en ligne, des agences de presse et des entreprises de communication audiovisuelle, les cabinets ou domiciles des professions protégées mentionnées à l'article 56-3, les locaux des juridictions et les domiciles des magistrats. Sont également exclus les systèmes situés dans le véhicule, le bureau ou le domicile d'un député, d'un sénateur, d'un avocat ou d'un magistrat, conformément au renvoi opéré à l'article 100-7 du CPP.

Le service technique national de captation judiciaire (STNCJ), rattaché au directeur technique de la DGSJ, assure la conception, la centralisation et la mise en œuvre des dispositifs techniques de captation¹⁷⁵.

La captation permet ainsi d'appréhender des données enregistrées sur un ordinateur, un téléphone mobile ou un serveur distant, des informations affichées à l'écran ou saisies au clavier avant leur transmission, ainsi que des données reçues ou émises par des périphériques audiovisuels. Elle offre ainsi la possibilité, comme le RDI en filière administrative, d'accéder aux informations avant leur chiffrement ou après leur déchiffrement, et a par exemple été **utilisée dans le cadre de l'affaire EncroChat**.

Au terme de ses travaux, la mission constate que les techniques d'enquête numérique judiciaire en général résultent d'une sédimentation normative, établie « *au gré des besoins, des censures ou des lacunes* », au point de se traduire par une « *instabilité du droit* », préjudiciable à sa cohérence d'ensemble¹⁷⁶. Cette construction par à-coups ne s'est pas démentie ces dernières années avec l'adoption de la loi dite de « lutte contre le narcotrafic »¹⁷⁷, en dépit des efforts du législateur pour créer un tronc commun des techniques spéciales d'enquête au sein du code de procédure pénale¹⁷⁸.

Les capacités d'investigation judiciaire liées aux nouvelles technologies sont ainsi multiformes, soit qu'elles résultent de dispositifs anciens mais adaptés à l'ère numérique¹⁷⁹, soit qu'elles ont été spécialement conçues au gré des évolutions techniques, et la plupart du temps utilisées au préalable dans le domaine du renseignement et de la police administrative¹⁸⁰, à l'image de l'accès à distance aux correspondances stockées par la voie de communications électroniques accessibles au moyen d'un identifiant¹⁸¹, de l'*IMSI-Catcher*¹⁸² ou de la captation des données informatiques.

Il en résulte **des dispositifs segmentés et non articulés entre eux**. À titre d'illustration, les réquisitions de données informatiques ont beau relever du régime des réquisitions judiciaires et l'interception des correspondances électroniques de celui des anciennes interceptions téléphoniques, l'unité n'est qu'apparente. Ainsi que le soulignent Mmes Florence Bellivier et Juliette Tricot, « *la construction du régime juridique des mesures NTIS est le fruit de réformes nombreuses dévoilant un intérêt particulier du législateur pour ces mesures mais une attention inégale aux effets*

¹⁷⁵ De création récente (2018) et détenant le monopole de la captation en matière judiciaire, le STNCJ s'appuie sur les capacités techniques et opérationnelles de la DGSJ développées pour le renseignement, de façon à mutualiser l'offre de logiciels espions au profit de la police judiciaire. Le coût de développement, de maintien et d'actualisation en continu des outils de RDI, de même que la nécessité de concentrer ces techniques entre les mains d'un nombre limité de personnes et de services, justifiaient leur centralisation autour des compétences et des investissements déployés dans le renseignement intérieur.

¹⁷⁶ V. ce sens l'analyse de M. Floran Vadillo, *Techniques d'enquête numérique judiciaire : les défis d'une survie dans la modernité*, in Les métiers du droit au défi du numérique, Annales des Mines – Enjeux numériques, 2018/3.

¹⁷⁷ Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic.

¹⁷⁸ Au Chapitre II du Titre XXV du Livre IV du CPP.

¹⁷⁹ Citons, pêle-mêle, la réquisition de documents (art. 60-1, 77-1-1 et 99-3 du CPP), la réquisition rapide de données informatiques stockées (art. 60-2 du CPP), la perquisition et la saisie de données informatiques stockées (art. 57-1 du CPP) ou encore les interceptions de correspondances émises par la voie électronique (art. 100 à 100-8 du CPP) et ce qu'il est convenu d'appeler l'infiltration numérique (art. 706-35-1 du CPP).

¹⁸⁰ V. en ce sens F. Bellivier et J. Tricot, *Pratiques et principes de l'enquête pénale à l'épreuve des nouvelles technologies d'investigation et de surveillance*, Rapport n° 20.48, IERDJ, février 2025. Les auteurs y observent d'ailleurs que les dispositifs d'investigation rattachés aux nouvelles technologies ont ceci de commun qu'ils ont tous été utilisés en pratique avant d'être validés *ex post* par le législateur.

¹⁸¹ Articles 706-95 à 706-95-3 du CPP.

¹⁸² Article 706-95-20 du CPP.

systémiques de ces interventions répétées par lesquelles il paraît plutôt courir après les pratiques et les techniques (...) »¹⁸³.

Les conséquences ne sont pas nulles. Pour les enquêteurs qui sont soumis à un droit d'une particulière complexité ; pour le droit au respect de la vie privée, sur lequel l'impact des ajustements législatifs n'a pas toujours été mesuré. À titre d'exemple, les perquisitions numériques qui permettent l'accès aux données de connexion et de contenu sont ainsi entourées de garanties moindres que celles prévues pour les réquisitions visant les seules données de connexion.

Aussi, la mission estime nécessaire que soit engagée une réflexion d'ensemble sur la mise en cohérence des techniques d'enquête numérique judiciaire, afin d'en améliorer la lisibilité, l'articulation et la sécurité juridique. Cette réflexion devrait tendre à rapprocher, lorsque leur objet et leur degré d'ingérence le justifient, les régimes applicables, sans figer dans la loi des techniques susceptibles d'être rapidement dépassées par l'évolution des technologies. Autant d'objectifs qui avaient d'ailleurs présidé à l'élaboration de la loi du 24 juillet 2015 sur le renseignement.

Recommandation n° 3 : Engager une refonte d'ensemble du cadre juridique des techniques d'enquête numérique judiciaire, afin d'en renforcer la sécurité juridique pour les enquêteurs et de mieux proportionner les garanties applicables aux atteintes à la vie privée.

À cet égard, si l'article 2 de la loi programmation du ministère de la justice 2023-2027 n'a habilité le Gouvernement à réécrire par ordonnance le code de procédure pénale qu'afin d'« *en clarifier la rédaction et le plan* » à droit constant, l'examen prochain du projet de loi de ratification de l'ordonnance n° 2025-1091 du 19 novembre 2025 portant réécriture du code de procédure pénale (partie législative), déposé au Sénat le 6 mai 2026, pourrait donner le coup d'envoi, en parallèle, de cette réflexion. À cette fin, un **comité associant praticiens, spécialistes et représentants des deux assemblées pourrait être rapidement constitué sous l'égide du garde des sceaux, ministre de la Justice**, avec pour objectif de rendre ses conclusions au terme de cette année.

Un cadre juridique constitutionnel et conventionnel garantissant un accès strictement encadré

À l'échelle conventionnelle, l'article 8 de la CEDH garantit à toute personne le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Dans des termes proches, l'article 7 de la Charte des droits fondamentaux de l'Union européenne protège le respect de la vie privée et des communications.

Cette protection est mise en œuvre par la directive « ePrivacy », déjà citée, dont l'article 5 consacre le principe de confidentialité des communications électroniques et des données de trafic. Les États membres sont ainsi tenus de garantir que nul ne puisse écouter, intercepter, stocker ou surveiller les communications sans le consentement des utilisateurs ou en dehors des cas expressément prévus par le droit de l'Union.

À l'échelle nationale, le secret des correspondances bénéficie d'une protection constitutionnelle¹⁸⁴ et trouve sa traduction notamment le CP, dont l'article 226-15 établit le régime de sanctions encourues en cas de violation ainsi qu'à l'article L.

¹⁸³ *Ibid.*, p. 69.

¹⁸⁴ V. par exemple Cons. Const., 2 mars 2004, n° 2004-492 DC, cons. 4.

32-3 du CPCE. S'y ajoutent des dispositions sur la protection des données personnelles telle que la loi dite « informatique et liberté » de 1978¹⁸⁵ et, au plan européen, le RGPD¹⁸⁶.

L'article 15 « e-privacy » autorise les États membres à adopter des mesures législatives limitant le principe de confidentialité des communications lorsqu'elles constituent une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

En droit français, le Conseil constitutionnel rappelle de façon constante que toute atteinte doit être « *proportionnée à la gravité et à la complexité des infractions commises* » et, dans le domaine judiciaire, « *conduite dans le respect des prérogatives de l'autorité judiciaire à qui il incombe en particulier de garantir que leur mise en œuvre soit nécessaire à la manifestation de la vérité* »¹⁸⁷.

Compte tenu de la sensibilité des données issues des messageries chiffrées, plusieurs niveaux de protection interviennent :

- protections technique : obligations strictes pour les opérateurs en termes de responsabilité pour la sécurité des données détenues, assorties de régimes de sanctions administratives, par la CNIL, et pénales ; les services de l'État sont soumis à des dispositions protectrices des usagers telles que la garantie que les dispositifs de renseignement et de techniques spéciales d'enquête ne constituent pas une faille de cybersécurité¹⁸⁸ ;
- protection contre les accès abusifs : en-dehors des cas rigoureusement énumérés par la loi et mis en œuvre sous autorisation et contrôle judiciaire ou administratif, tout accès illégitime aux données des services de communication est sévèrement sanctionné par le code pénal¹⁸⁹ ;
- protection contre les techniques intrusives : conditions d'emploi et de contrôle spécifiques.

b) Un principe d'effectivité aux effets limités appelant des aménagements

Plusieurs dispositions s'essaient à garantir l'effectivité des prérogatives des services d'enquête en renseignement comme dans le domaine judiciaire.

Les articles 60-1, 60-2 et 77-1-1 du code de procédure pénale précités prévoient ainsi **des peines d'amendes, limitées à 3750 euros, dès lorsqu'il n'est pas déféré aux réquisitions judiciaires.**

Le code pénal (CP) y ajoute un régime de sanction spécifique au déchiffrement. L'article 435-15-2 sanctionne le refus, « *pour quiconque* » en ayant connaissance, de remettre ou de mettre en œuvre « *la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit* ». La peine est fixée à trois ans d'emprisonnement et 270 000 euros d'amende ; elle est portée à cinq ans d'emprisonnement et 450 000 euros d'amende dans le cas où l'information « *aurait permis d'éviter la commission d'un délit ou d'un crime, ou d'en limiter les effets* »¹⁹⁰.

¹⁸⁵ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

¹⁸⁶ Règlement UE 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

¹⁸⁷ 2014-693 DC, 25 mars 2014, cons. 9 à 12.

¹⁸⁸ Ces dispositions sont notamment mises en place par les articles 226-3, R. 226-1 et R. 226-12 du code pénal.

¹⁸⁹ Article 226-15 du CP.

¹⁹⁰ La Cour de cassation a pu juger, à cet égard, que le refus par un suspect de communiquer le code de déverrouillage de son téléphone portable était constitutif d'un délit dès lors que la réquisition a été formellement délivrée et que la remise de ce code emporte mise en œuvre de la convention de déchiffrement (Cass. crim., 13 octobre 2020, n° 20-80.150). La Cour a toutefois circonscrit cette jurisprudence en considérant qu'« *une convention de déchiffrement s'entend de tout moyen logiciel ou de toute autre information permettant la mise au clair d'une donnée transformée par un moyen de cryptologie, que ce soit à l'occasion de son stockage ou de sa transmission. Il en résulte que le code de déverrouillage d'un téléphone mobile peut constituer une clé de déchiffrement si ce téléphone est équipé d'un moyen de cryptologie* » (Cass. crim. plén., 7 novembre 2022, n° 21-83.146). Sur la base de cette définition fonctionnelle, les juges du fond sont alors conduits à rechercher si le téléphone en cause est équipé d'un tel moyen et si son code de déverrouillage permet de mettre au clair tout ou partie des données cryptées qu'il contient.

En matière de renseignement, l'article L. 871-1 du code de la sécurité intérieure ne vise pas les seuls opérateurs de communications électroniques mais « *les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité* ». Ces derniers ont l'obligation de remettre, dans un délai de soixante-douze heures, les conventions permettant le déchiffrement des données. Les agents habilités peuvent également leur enjoindre de mettre elles-mêmes en œuvre ces conventions, sauf si elles démontrent être dans l'impossibilité de satisfaire à cette demande. Le non-respect de ces obligations est réprimé, au terme de l'article L. 881-2 du même code, de deux ans d'emprisonnement et de 150 000 euros d'amendes.

Ces dispositifs présentent une effectivité limitée face à la généralisation du chiffrement « de bout en bout ». Leur mise en œuvre suppose que les plateformes soit effectivement en possession d'une convention permettant le déchiffrement ou dispose de la capacité de la mettre en œuvre : cette condition fait précisément défaut en présence de services E2EE.

Au surplus, même lorsqu'une convention de déchiffrement existe et peut-être remise, l'efficacité de la sanction est parfois mise en défaut. Il a été signalé à la mission que certaines personnes mises en cause préfèrent s'exposer aux poursuites pénales de l'article 434-15-2 du code pénal plutôt que de communiquer le code de déverrouillage de leur terminal et permettre l'accès à des données susceptibles de révéler des infractions plus lourdement sanctionnées.

L'impossibilité technique résultant du chiffrement est susceptible d'expliquer, au moins en partie, **l'absence de contentieux identifié à l'encontre des principaux fournisseurs de messageries chiffrées « de bout en bout »** pour refus de remise ou mise en œuvre des conventions de déchiffrement. Les recherches conduites par la mission n'ont d'ailleurs permis d'identifier aucune procédure visant *Signal*, *WhatsApp* ou tout autre fournisseur comparable.

Les services de l'État ont eux-mêmes souligné, devant la mission, que la mise en œuvre de ces procédures suppose d'établir préalablement que l'opérateur détienne effectivement les moyens permettant l'accès en clair aux données recherchées. Plusieurs d'entre eux ont, pour cette raison, mis en doute l'utilité de poursuites fondées sur le refus de remettre une convention de déchiffrement à l'encontre de fournisseurs dont le service repose sur une architecture E2EE.

La mission estime que **cette stratégie de « non-poursuite » a priori doit être corrigée** : les refus opposés aux réquisitions devraient pouvoir faire l'objet d'un examen systématique et donner lieu à des poursuites dès lors que des éléments permettent d'établir que leur destinataire détenait la convention de déchiffrement requise ou disposait des moyens techniques pour la mettre œuvre. **L'invocation d'une architecture de chiffrement « de bout en bout » ne saurait en effet dispenser l'opérateur de justifier l'étendue de son impossibilité technique.**

Plusieurs modifications pourraient être apportées au droit positif pour **favoriser un changement d'approche**.

Il est tout d'abord proposé de durcir le régime des sanctions applicables aux réquisitions judiciaires, en fixant un délai de réponse obligatoire et en relevant substantiellement le montant de l'amende, lorsque la réquisition porte sur des données numériques et s'adresse à un opérateur de communications électroniques ou à un fournisseur de services.

Recommandation n° 4 : Rehausser le niveau de la sanction financière applicable au défaut de réponse aux réquisitions judiciaires portant sur des données lorsqu'elles sont adressées à un opérateur de communications électroniques ou à un fournisseur de services.

D'autre part, la rédaction actuelle de l'article L. 871-1 du code de la sécurité intérieure pourrait être plus adaptée qu'elle ne l'est aujourd'hui à la réalité des architectures de chiffrement « de bout en bout ».

En l'état, l'article L. 871-1, alinéa 1^{er}, du code de la sécurité intérieure, repose sur une fiction juridique largement inopérante : il impose aux opérateurs de remettre les conventions permettant le déchiffrement des données, comme si leur disponibilité était acquise ou, à tout le moins, possible, et sans envisager l'hypothèse dans laquelle aucune convention ne serait détenue par l'opérateur. Une « exception d'impossibilité » est certes prévue, mais dans le seul cas où la réquisition porte sur la mise en œuvre, par l'opérateur lui-même, de ces conventions. Celui-ci peut alors s'y soustraire s'il « *démontre qu'[il n'est] pas en mesure de satisfaire à ces réquisitions* ». L'article L. 881-2 du même code sanctionne, quant à lui, sans autre précision, « *le fait de ne pas déférer (...) aux demandes formulées* » dans les conditions du premier alinéa de l'article L. 871-1 du code de la sécurité intérieure.

Une autre approche consisterait à soumettre les opérateurs à une obligation de communiquer les éléments permettant d'apprécier l'impossibilité technique faisant obstacle à la remise ou la mise en œuvre des conventions de déchiffrement.

L'article L. 871-1 pourrait ainsi prévoir que les personnes physiques ou morales qu'il vise sont tenues soit de remettre ou de mettre en œuvre les conventions permettant le déchiffrement¹⁹¹ – c'est le droit applicable – soit, lorsqu'elles soutiennent ne pas disposer de telles conventions ou de tels moyens, de communiquer aux agents autorisés les éléments permettant d'établir cette impossibilité. Partant, l'article L. 881-2 du code de la sécurité intérieure pourrait sanctionner, lorsque les personnes physiques ou morales visées affirment ne pas détenir les conventions de déchiffrement, le fait de ne pas communiquer les éléments permettant d'en attester ou de communiquer des éléments insuffisants, voire erronés. Le même raisonnement pourrait être transposé aux dispositions de l'article 434-15-2 du code pénal.

Cette obligation de communication ou de transmission se distinguerait de la clause d'exonération figurant à la seconde phrase de l'alinéa 1^{er} de l'article L. 871-1. En effet, en l'état de sa rédaction, la démonstration par les opérateurs « *qu'ils ne sont pas en mesure de satisfaire* » à une demande de mise en œuvre se borne à prévoir les conditions dans lesquelles les opérateurs peuvent être dispensés de la réquisition. La nouvelle obligation aurait un objet similaire mais une portée différente. Elle imposerait aux opérateurs un comportement positif et contrôlable : l'obligation de communication pourrait être sanctionnée indépendamment de l'appréciation portée

¹⁹¹ On rappellera ici que toutes les architectures de chiffrement ne privent pas les opérateurs et fournisseurs de la maîtrise des éléments permettant le déchiffrement. La généralisation en cours du chiffrement « de bout en bout » ne saurait donc justifier l'abandon d'une obligation qui demeure opérante pour les autres architectures. Cette observation est d'ailleurs cohérente avec la définition fonctionnelle que donne la Cour de cassation des conventions de déchiffrement, lesquelles portent sur la mise au clair de données effectivement transformées par un moyen cryptographique quel qu'il soit. V. à cet égard l'arrêt précité : Cour cass., ass. plén., 7 novembre 2022, n° 21-83.146.

sur l'existence d'une capacité de déchiffrement. Elle aurait, en outre, une portée plus large en s'appliquant aux réquisitions de remise comme de mise en œuvre des conventions.

L'application de cette obligation modifierait la logique probatoire actuelle : pour poursuivre les opérateurs, les services n'auraient plus à établir préalablement que ceux-ci étaient en mesure de satisfaire à la réquisition. Le manquement susceptible de fonder les poursuites résiderait, d'une part, dans le défaut de communication des éléments permettant d'apprécier le refus de l'opérateur de remettre ou mettre en œuvre la convention de déchiffrement ou, d'autre part, dans la transmission d'éléments insuffisants ou erronés pour en apprécier la réalité.

Ainsi conçue, l'adaptation de l'article L. 871-1 du code de la sécurité intérieure emporterait deux conséquences sinon favorables, du moins utiles : **elle inciterait à des poursuites systématiques** dès lors que les opérateurs omettraient de transmettre les informations exigées par la loi ; par ailleurs, les poursuites engagées sur ce fondement permettraient, au-delà de leur fonction répressive, d'**améliorer le suivi des réquisitions adressées aux opérateurs**, tout en permettant de faire émerger un contentieux susceptible de préciser la portée d'obligations dont l'application aux architectures de chiffrement « de bout en bout » demeure aujourd'hui largement indéterminée.

Au cas par cas, la conjugaison de sanctions pénales et administratives (cf. les prérogatives de l'ARCEP) devrait être envisagée.

Recommandation n° 5 : Créer, à la charge des opérateurs et des fournisseurs, une obligation de communiquer les éléments justifiant l'impossibilité de remettre ou mettre en œuvre une convention de déchiffrement, et sanctionner le manquement à cette obligation.

De façon plus générale, la question de l'efficacité du régime actuel de sanction met en évidence le décalage entre les prérogatives d'accès reconnues aux autorités et les conditions techniques de leur exercice. **La généralisation du chiffrement a ainsi pour conséquence de dissocier la règle de droit de son effectivité.** Il en résulte le déplacement d'une partie des techniques de renseignement et d'enquête numérique vers les données qui ne sont pas couvertes par le chiffrement « de bout en bout ».

B) La perte d'accès au contenu réoriente les voies d'accès à l'information pour les enquêteurs

L'extension du chiffrement « de bout en bout » rompt avec l'économie des interceptions classiques. Il en résulte **une dégradation du rendement des interceptions classiques**, incitant les services soit à « viser ailleurs » (les données de connexion), soit à contourner le chiffrement « de bout en bout » (le piégeage des terminaux). Ce que le président de la CNCTR, M. Vincent Mazauric, résume par cette formule : « *le tarissement des bonnes vieilles interceptions de sécurité* »¹⁹².

¹⁹² Audition par la Commission des lois de l'Assemblée nationale, conjointe avec la Commission de la défense et des forces armées, de M. Vincent Mazauric, président de la CNCTR, le 24 septembre 2025.

1) Le droit cède le pas devant la disponibilité technique des données

Dans un environnement chiffré « de bout en bout », **les opérateurs et les fournisseurs de services sont, en quelque sorte, les vrais maîtres de l'enquête**. Car deux catégories de données coexistent : celles auxquelles ils n'ont pas accès, dès lors qu'ils décident de déployer des services chiffrés ; et celles qui sont susceptibles, certes, d'être produites « hors chiffrement », mais dont ils contrôlent la production, et donc l'existence, au regard de leurs politiques de confidentialité.

a) Les données en clair dépendent de leur détention par les fournisseurs

Une controverse persiste sur la nature des données réellement détenues par les plateformes.

D'un côté, les fournisseurs de messageries opposent les propriétés du chiffrement « de bout en bout » qui les prive, par construction, de l'accès au contenu intelligible des communications, sauf à changer de standard et donc de paradigme. De l'autre, une partie des services de l'État, parfois parmi les plus sensibles, émettent plus que des doutes sur cette affirmation. Un service du premier cercle observe toutefois qu'« *il n'existe pas de pays dans le monde qui aurait posé un principe d'accès total au chiffrement et l'aurait obtenu* »¹⁹³.

Ces divergences entretiennent un étrange « dialogue de sourd » entre certains services de l'État, les fournisseurs de messageries chiffrées et, plus largement, les acteurs du débat public. Au demeurant, elles nourrissent le soupçon envers les autorités de viser l'introduction de mécanismes supplémentaires dans l'architecture des services qualifiés, selon les cas, de « *backdoors* » ou de « *master keys* »¹⁹⁴. *Signal* a d'ailleurs pu instrumentaliser cette controverse auprès de ses utilisateurs, au point d'en faire un quasi-argument commercial : « *Signal ne sait toujours rien à votre sujet, mais les autorités continuent néanmoins de nous demander si c'est bien le cas* »¹⁹⁵.

Une hypothèque mérite par conséquent d'être levée : les fournisseurs de services de messageries rencontrés par la mission affirment être, en théorie, en mesure d'atteindre des informations chiffrées¹⁹⁶. **Mais procéder à de telles modifications reviendrait, en l'état des techniques disponibles, à sortir du modèle du chiffrement « de bout en bout » et à renoncer, par conséquent, au standard le plus élevé de protection des échanges numériques.**

Mme Yasmine Douadi, analyste en cybersécurité, relève à cet égard que tout mécanisme visant à « *forcer les messageries chiffrées à créer un flux parallèle vers les autorités (...)* » constituerait, quelles qu'en soient les modalités techniques, « *une porte dérobée* », c'est-à-dire « *une vulnérabilité systémique exploitable par n'importe qui* »¹⁹⁷.

Dans ce contexte, **la mission rappelle que les autorités administratives et judiciaires rencontrées ont toutes revendiqué la « réplication du modèle historique des interceptions**

¹⁹³ Audition du 24 février 2026.

¹⁹⁴ La première désigne un accès dissimulé au système ; la seconde, un dispositif assumé permettant à un tiers autorisé d'obtenir le contenu intelligible au moyen d'une clé supplémentaire.

¹⁹⁵ Signal, *Government Requests, MLAT order from Luxembourg for Signal user data*, 2 novembre 2021.

¹⁹⁶ Audition du 18 février 2026.

¹⁹⁷ « Affaiblir le chiffrement des données affaiblit la sécurité de tous », *Le Monde*, 27 octobre 2025.

légal »¹⁹⁸ aux échanges numériques chiffrés : mêmes finalités, mêmes garanties, mêmes contrôles. Ni accès permanent, ni contrôle de masse que les règles constitutionnelles et conventionnelles qui s'imposent fort heureusement à nous écartent au demeurant par principe.

Devant les controverses et parfois les doutes qui traversent la sphère de l'État et nos concitoyens, la mission se borne en tout cas à un constat : **factuellement, les autorités administratives et judiciaires n'accèdent pas aux clés permettant de mettre au clair les correspondances protégées par un chiffrement « de bout en bout »**, raison pour laquelle la mission propose de renforcer les obligations pesant sur les opérateurs et les fournisseurs (v. les propositions n° 4 et 5 *supra* et n° 7 et 9 *infra*).

Force est donc de constater que les prérogatives légales ne garantissent plus l'accès à un contenu intelligible : **celui-ci dépend moins de l'étendue des prérogatives reconnues à la puissance publique que de leur disponibilité technique**. Cette rupture entre l'habilitation juridique et la possibilité technique de rendre intelligible le contenu illustre ce que la communauté des experts désigne sous l'expression de « *going dark* ».

b) Le « *going dark* » ou l'approche fondée sur les données encore disponibles

Le « *going dark* » ne signifie pas que toute information relative aux échanges échapperait aux fournisseurs et donc aux autorités. **Le chiffrement « de bout en bout » ne plonge pas les services enquêteurs dans une « obscurité » totale**. Il dépeint une sorte de *ténébrisme* inversé, où le cœur des communications s'assombrit (le contenu), tandis que ses contours (les métadonnées) demeurent partiellement éclairés.

Ainsi, en valeur absolue, en matière de renseignement, les demandes d'interceptions fondées sur l'article L. 852-1 du code de la sécurité intérieure demeurent soutenues, passant de 12 891 en 2020 à 14 284 en 2025 (+10,8). Mais, en valeur relative, leur part dans l'ensemble des autorisations sollicitées de la CNCTR recule de 16,19% en 2020 à 14,17% en 2025.

Dans son rapport d'activité pour 2024, la CNCTR relève à cet égard que, si les interceptions de sécurité sont indispensables pour appréhender l'environnement d'une personne surveillée et orienter les investigations, « *l'utilité opérationnelle de cette technique est (...) moindre qu'auparavant, compte tenu du chiffrement des données de contenu* ».

En conséquence, la Commission souligne que « *les pratiques des services de renseignement (...) changent (...) en fonction des évolutions technologiques qui remettent (...) en cause l'intérêt de certaines techniques en raison d'une efficacité peu satisfaisante* »¹⁹⁹. Dans son rapport d'activité pour 2025, l'autorité administrative indépendante va plus loin et qualifie le chiffrement de « *défi pour le renseignement* », soulignant que « *l'emploi de plus en plus répandu des messageries chiffrées a réduit de façon majeure l'intérêt des interceptions de sécurité* ». Il en est évidemment de même en matière judiciaire.

¹⁹⁸ Audition de la DGSI du 24 février 2026.

¹⁹⁹ Rapport d'activité pour 2024.

Dès lors, **les enquêtes migrent vers les données encore produites, conservées et intelligibles**, ainsi que vers les techniques permettant de recueillir les informations directement sur les systèmes informatiques (RDI). En d'autres termes, de la même façon que notre regard se porte spontanément vers les parties éclairées d'une scène, les capacités d'enquête se tournent vers les données accessibles.

- *L'importance prise par le recueil des données de connexion*

En matière de renseignement, cette réorientation ressort de **la place désormais incontournable occupée par les techniques fondées sur les données de connexion**.

Les demandes d'identification d'abonnés ou de recensement de numéros fondées sur l'article L. 851-1 du code de la sécurité intérieure sont ainsi passées de 30 758 en 2020 à 32 866 en 2025. Les autres accès en temps différé, comprenant notamment les « factures détaillées », ont progressé de 18 006 à 22 872 sur la même période.

La diminution des accès aux données de connexion en temps réel autorisés sur le fondement de l'article L. 851-2 du code de la sécurité intérieure, passés de 1 644 demandes en 2020 à 677 en 2025, ne remet pas en cause ce constat. La CNCTR relève au contraire que les accès en temps différé, moins intrusifs, permettent d'apprécier l'opportunité de poursuivre la surveillance, tandis que les accès en temps réel répondent à des besoins plus ciblés.

Les géolocalisations en temps réel, prévues par l'article L. 851-4 du code de la sécurité intérieure, demeurent pour leur part utilisées à un niveau élevé (8 394 demandes en 2020 ; 10 215 en 2024, soit + 18%).

Réunies, ces catégories représentaient 55 738 demandes d'autorisation en 2025 : en nombre de demandes, elles constituent **la technique de surveillance de première intention**.

- *La montée en puissance du recueil de données informatiques*

La seconde traduction de cette réorientation ressort, toujours en matière de renseignement, du recours au recueil des données informatiques de l'article L. 853-2 du code de la sécurité intérieure dont le nombre de demandes d'autorisation est passé de 2 418 en 2020 à 7 900 en 2025, soit une augmentation de 226,7% et un volume multiplié par près de 3,3 sur la période. En valeur relative, la place du RDI demeure toutefois limitée à 7,84% de l'ensemble des demandes d'autorisation en 2025, contre 3,04% cependant en 2020. Outre les effets du chiffrement, la CNCTR rattache cette forte augmentation à la meilleure maîtrise de cette technique par les services et à l'étendue des données recueillies sur les systèmes informatiques ciblés.

Ainsi, l'accès à l'information repose désormais sur la combinaison de techniques conçues jusqu'ici comme un complément des interceptions classiques et dont les régimes juridiques ont été pensés et calibrés en considération de cette complémentarité. Partant, cette « nouvelle économie des investigations » forcée ne peut que s'avérer imparfaite en contexte de numérisation de masse des échanges.

2) La « nouvelle économie des investigations » demeure imparfaite

La migration des investigations vers des données et techniques périphériques fait apparaître trois difficultés. D'une part, elle dépend, nous l'avons vu, des choix opérés par les fournisseurs qui demeurent, en l'état de la technologie, libres de décider des catégories de données générées par leurs services²⁰⁰. D'autre part, la volumétrie et l'hétérogénéité des données collectées imposent des capacités avancées de traitement et de stockage qui restent hors de portée pour certains services. Enfin, la montée en puissance des techniques de recueil de données informatiques, par définition intrusive, soulève plusieurs interrogations sur ses conditions d'emploi.

Une observation mérite d'être faite pour expliciter le point de vue de la mission : si une solution techniquement neutre devait, à terme, rétablir l'accès aux données de contenu, les équilibres traditionnels de l'investigation retrouveraient certes leur cohérence passée. Toutefois, dans l'intervalle, et pour peu que de telles évolutions se réalisent, une « nouvelle économie des investigations » se recompose sous nos yeux qui pourrait durablement s'installer et nécessite que des réponses soient apportées par la puissance publique à très court terme. Deux voies pourraient être empruntées pour y contribuer : la première consiste à **imposer aux opérateurs et aux OTT des obligations supplémentaires de transparence** ; la seconde, à **renforcer les capacités des services d'investigation**.

a) Les opérateurs et les OTT doivent répondre à des exigences de transparence

Si les données de connexion constituent une précieuse source de substitution aux données de contenu, leur disponibilité à moyen et long terme est loin d'être acquise : elle dépend, pour partie, des choix de confidentialité et d'architecture technique des fournisseurs. Cette dépendance soulève la question centrale de **la gouvernance de la donnée** et justifie des exigences accrues.

- **Contenir les stratégies de « data minimisation » qui pèsent sur la disponibilité des métadonnées**

Plusieurs OTT revendiquent d'ores et déjà **une politique offensive de minimisation des données de connexion**.

Signal précise, par exemple, que son objectif n'est pas seulement de protéger le contenu des échanges mais de limiter, autant que possible, la collecte de métadonnées. Son ambition est « *d'avoir accès à aussi peu de données que possible* ». L'entreprise indique n'avoir d'ores et déjà pas accès aux messages, appels, informations de profil et de groupes, aux contacts, aux *stories*, aux journaux d'appels ni à de nombreuses autres catégories de contenu et de métadonnées, et se prévaut de n'avoir « *jamais détenu* » certaines des données demandées par les autorités judiciaires.²⁰¹ *Signal* vise ainsi le développement de « *techniques destinées à réduire encore la quantité d'informations accessibles au service* »²⁰².

²⁰⁰ La création des données doit ainsi être distinguée de leur conservation.

²⁰¹ *Signal, Government Requests, Grand jury subpoena for Signal user data in the United States District Court for the District of Columbia*, 6 mars 2026.

²⁰² *Signal, Technology preview : Sealed sender for Signal*, 29 octobre 2018.

WhatsApp semble adopter une approche en partie différente. Sa politique de confidentialité fait apparaître la collecte de données de compte, d'usage, de terminal et de réseau, ainsi que des informations nécessaires à l'acheminement des communications, notamment les numéros de téléphone et certains horodatages relatifs aux messages et aux appels. La durée de conservation varie selon la nature des données, leur finalité et les obligations légales applicables. Pour les principales données de compte, de connexion, de réseau et d'usage, *WhatsApp* se borne à indiquer qu'elles sont conservées « *aussi longtemps qu'elles demeurent nécessaires au fonctionnement, à la sécurité et à l'intégrité du service, ainsi qu'au respect des obligations légales* », sans préciser la durée effective de conservation²⁰³.

Olvid revendique une démarche plus radicale. Les choix techniques retenus, notamment l'absence de numéro de téléphone ou d'adresse électronique pour créer un compte, excluent, « *par construction, la détention de certaines métadonnées* »²⁰⁴. Sa politique de confidentialité indique que sa technologie « *ne requiert aucune donnée personnelle pour fonctionner, ni numéro de téléphone, ni adresse électronique, ni nom, ni prénom* »²⁰⁵.

Cette stratégie de réduction des métadonnées se poursuit au gré de l'extension du chiffrement. La fonctionnalité « *Sealed Sender* », déployée par *Signal* depuis le 29 octobre 2018, en est une bonne illustration. Conçue pour limiter les informations accessibles au serveur, elle chiffre notamment l'enveloppe contenant l'identité de l'expéditeur, tout en laissant encore visibles les adresses IP, les horodatages et les volumes des échanges. Dans le même esprit, le protocole *Messaging Layer Security* (MLS), normalisé par l'IETF américaine en 2023, vise certes le chiffrement « de bout en bout » des conversations et donc des seuls contenus de groupe, mais son architecture de référence fait également de la protection des métadonnées un « objectif de conception ».

À cet égard, les travaux du High-Level Group sur l'accès aux données (HLEG) mettent en évidence plusieurs évolutions convergentes : la généralisation des politiques de restriction des données générées, la réduction des catégories de données conservées, la limitation de la durée de conservation et la faible visibilité des autorités sur les données détenues par les fournisseurs²⁰⁶.

La mission constate ainsi que le principal risque, à court terme, n'est plus tant l'impossibilité technique d'accéder aux contenus chiffrés que la contraction progressive des données périphériques elles-mêmes, sous l'effet des stratégies de « *data minimisation* » déployées par les opérateurs et fournisseurs de services.

Les auditions conduites par la mission semblent pourtant démontrer que la mobilisation des administrations est essentiellement orientée vers la recherche de solutions permettant d'accéder aux contenus – c'est en effet indispensable –, mais sans que la disponibilité même des métadonnées ne soit affirmée comme un objectif prioritaire de même niveau.

En renseignement comme en judiciaire, pourtant, nous l'avons vu, les investigations portant sur les données de connexion sont désormais les premières en volume, démontrant leur caractère

²⁰³ *WhatsApp Privacy Policy (European Region)*, section *How We Retain Information*, version applicable depuis le 26 mars 2026.

²⁰⁴ Audition du 18 février 2026.

²⁰⁵ *Olvid, Privacy Policy*, consultée le 22 avril 2026.

²⁰⁶ HLEG, *Concluding report of the High-Level Group on access to data for effective law enforcement*, 15 novembre 2024.

stratégique pour les enquêteurs. Partant, **la raréfaction des métadonnées finirait de compromettre les capacités d'investigation déjà fortement entamées par le chiffrement « de bout en bout »**.

À l'issue de ses travaux, la mission considère par conséquent que la préservation de la disponibilité des données de connexion et des autres données techniques doit constituer **un objectif de même niveau** que la recherche de solutions d'accès aux contenus chiffrés.

Recommandation n° 6 : Faire de la préservation de la disponibilité des métadonnées un objectif stratégique à part entière face aux politiques de « data minimisation » déployées par les opérateurs et les fournisseurs.

Les réflexions conduites à l'échelle européenne identifient dès à présent plusieurs leviers d'action qui toutes appellent une action coordonnée à l'échelle du marché unique : la conservation obligatoire de certaines données (adresses IP, numéro de port), la standardisation des données générées et conservées ; la normalisation des demandes d'accès légales, voire – arme fatale – la question du conditionnement de l'accès au marché unique. Certaines de ces recommandations ont été portées par le HLEG sur l'accès aux données²⁰⁷, déjà cité, et reprises par la Commission européenne dans sa feuille de route du 24 juin 2025²⁰⁸.

La mission ne peut que souscrire à ces orientations et inviter la France à poursuivre le rôle actif qu'elle prend dans ces discussions.

L'échelle d'action européenne ne doit toutefois pas exclure que des mesures en faveur d'une plus grande transparence soient prises sur le plan national, sur au moins deux points : d'un côté, les données effectivement détenues par les opérateurs et les fournisseurs ; de l'autre, la capacité de ces derniers à renseigner les réquisitions administratives et judiciaires.

- ***Organiser l'obligation de transparence sur les métadonnées effectivement détenues***

Les services de renseignement et d'enquête disposent aujourd'hui d'une connaissance essentiellement empirique des données de connexion effectivement détenues par les opérateurs et les fournisseurs de services. Cette situation n'est d'ailleurs pas propre à la France : elle résulte de la diversité des architectures techniques, des politiques de minimisation et des pratiques hétérogènes de conservation déjà évoquées.

Il en ressort une incertitude sur les catégories de données qui peuvent être requises. Il apparaît par conséquent indispensable d'organiser une plus grande transparence des données effectivement détenues par les plateformes, à tout le moins sous la forme d'une obligation d'information, notamment pour renforcer la prévisibilité des réquisitions.

²⁰⁷ V. en particulier les recommandations n° 15, 16, 17, 22, 27 et 32 du HLEG.

²⁰⁸ Commission européenne, *Feuille de route pour un accès licite et effectif aux données à des fins répressives*, COM(2025) 349 final, 24 juin 2025.

Recommandation n° 7 : Imposer aux opérateurs de communications et aux fournisseurs de services accessibles en France une obligation d'information sur les données qu'ils génèrent, traitent et conservent.

On rappellera à cet égard que les politiques de confidentialité répondant aux exigences du RGPD n'ont ni pour objet ni pour effet de recenser les données effectivement générées et détenues par les fournisseurs, mais d'informer les personnes concernées sur les traitements de données à caractère personnel mis en œuvre. La présente recommandation ne paraît par conséquent pas en contradiction avec le droit européen.

Certains des fournisseurs pourraient, bien sûr, revendiquer de ne pas se soumettre au droit français – argument classique des tenants du « *forum shopping* » normatif – mais **une obligation d'information assortie de sanctions financières proportionnées pourrait être entendue**, ce d'autant plus que certaines plateformes ont dès à présent adopté des pratiques plus vertueuses que d'autres, et pourraient s'engouffrer dans cette démarche à des fins réputationnelles.

- **Faire la lumière sur les réponses aux réquisitions administratives et judiciaires**

Dans le même temps, la lumière reste à faire sur les réponses apportées aux réquisitions de données. **Les « rapports de transparence » publiés par certaines des grandes entreprises numériques sont aujourd'hui l'une des rares sources publiques** permettant d'apprécier l'exécution des réquisitions adressées par les autorités françaises.

Meta indique avoir reçu, pour la France et le premier semestre 2025, 16 055 demandes émanant d'autorités publiques (« *government requests for data* »), dont 6 883 fondées sur une procédure légale (« *legal process request* ») et 9 172 sur une demande de divulgation en urgence (« *emergency disclosure requests* »). Ces demandes visaient, selon l'entreprise, 18 438 utilisateurs ou comptes (« *users/accounts requested* »). 84,08% d'entre elles auraient donné lieu à la transmission d'« *au moins certaines données* » (« *requests where some data was produced* »)²⁰⁹.

Apple déclare, sur la même période, avoir reçu 2 458 demandes (« *government requests* »), réparties entre 1 116 demandes relatives à des appareils (« *device requests* »), 241 portant sur des identifiants au moyen d'un paiement ou d'une transaction (« *financial identifier requests* »), 1047 sur des comptes (« *account requests* »), et 3 sur des « jetons de notification »²¹⁰ (« *push token requests* »). 51 demandes en urgence (« *emergency requests* ») auraient également été requises. Au total, 1382 demandes auraient donné lieu à la communication de données (« *requests where data provided* »), soit 56,2% des réquisitions²¹¹.

Google fait état, pour la même période, de 8 897 demandes de communication de données (« *requests for disclosure of user information* »), visant 17 716 comptes (« *accounts specified* »), dont 81% auraient abouti à la transmission d'« *au moins certains des cas* » (« *requests where some*

²⁰⁹ Meta, *Transparency Center – Government Requests for User Data – France*, consulté le 5 août 2026.

²¹⁰ Un jeton d'identification est un identifiant technique, attribué par un système d'exploitation, pour permettre au fournisseur de services d'adresser une notification à un appareil déterminé.

²¹¹ Apple, *Transparency Report – Government Requests – France*, consulté le 5 août 2026.

information was disclosed »). Ces demandes portaient notamment sur 149 demandes en urgence (« *emergency disclosure requests* »)²¹².

Ces résultats doivent être interprétés avec prudence.

Les fournisseurs ne publient en effet ni les mêmes catégories de demandes, ni les mêmes indicateurs, rendant difficile toute comparaison. Ces informations ne permettent d'identifier ni les catégories de données transmises, ni les réponses partielles ou les refus explicites (absence de collecte, difficultés procédurales, obstacles techniques, divergences d'interprétation du droit applicable, ...). En outre, **les procédures internes mises en place pour le traitement prioritaire des situations d'urgence peuvent constituer un obstacle aux réquisitions.**

Plusieurs fournisseurs disposent en effet de circuits spécifiques, destinés à traiter en priorité les demandes faisant état d'un « danger imminent pour la vie » ou pour « l'intégrité physique d'une personne ». Mais, outre que ces catégories diffèrent d'un fournisseur à l'autre, et ne se rattachent pas à une définition pénale précise, elles supposent que l'autorité judiciaire précise les circonstances justifiant l'urgence à un stade de la procédure où il n'est pas toujours possible de la caractériser. Dès lors, la demande est au mieux traitée par la voie ordinaire, hors urgence ou, au pire, rejetée. **Les fournisseurs opèrent ainsi un véritable contrôle de l'opportunité sur le fond des demandes qui leur sont adressées**, en fonction de critères qui leur sont propres.

Dans le même temps, et dans un autre registre, le périmètre de la PNIJ ne couvre pas les *OTT* qui opèrent par contournement du réseau. N'ayant pour la plupart pas d'existence légale en France, ils ne sont pas raccordés à la plateforme²¹³. Il en résulte qu'à la différence des opérateurs de communications électroniques (OCE)²¹⁴, **les demandes adressées aux fournisseurs de services ne transitent pas par le canal automatisé de la PNIJ et font l'objet de réquisitions *ad hoc***, rendant difficile la construction de statistiques consolidées sur l'état des réquisitions.

Ces caractéristiques propres aux fournisseurs de services ont récemment été pris en compte. Dans sa **circulaire du 13 avril 2026 relative à l'accès aux données détenues par les fournisseurs de services ou de messageries électroniques**, la DACG demande aux parquets de saisir systématiquement les fournisseurs *OTT* lorsque les nécessités de l'enquête le justifient, de veiller à la qualité des réquisitions adressées et de recenser les « *refus ou des carences systématiques des fournisseurs de services fréquemment utilisés par les réseaux criminels* ». La DACG demande également aux juridictions de « faire remonter » à la chancellerie les difficultés rencontrées avec les opérateurs requis afin d'établir un état des lieux national²¹⁵.

Le dispositif lancé par la DACG se limite toutefois à organiser une centralisation de l'information en quelque sorte « manuelle », réduite pour l'essentiel aux difficultés rencontrées, sans véritablement constituer un dispositif national de suivi consolidé et automatique des réquisitions judiciaires adressées aux fournisseurs de services.

²¹² Google, *Transparency Report – Requests for Disclosure of user information – France*, consulté le 5 août 2026.

²¹³ On rappellera que, de la même façon, les fournisseurs d'accès à Internet et les opérateurs satellitaires ne sont pas non plus raccordés à la PNIJ.

²¹⁴ Encore faut-il rappeler, comme l'indiquaient dans leur rapport de 2023 les sénateurs A. Canayer et Ph. Bonnacarrère, qu'une vingtaine d'opérateurs sont raccordés à la PNIJ sur les 1800 environ présents sur le territoire national.

²¹⁵ DACG, circulaire NOR JUSD2605231C, n° 2026-5/CAB-20/02/2026, relative à l'accès aux données détenues par les fournisseurs de services ou de messageries électroniques, 13 avril 2026.

La problématique n'est, là-encore, pas spécifique à la France. À l'occasion des travaux préparatoires du HLEG sur l'accès aux données, les experts soulignaient « *les difficultés rencontrées pour produire des statistiques permettant de quantifier l'importance de l'accès légal aux données pour la conduite des enquêtes et des poursuites pénales, indépendamment du type d'infraction concernée ou de la catégorie de données requise* »²¹⁶. Bien que **des standards ont été définis par l'ETSI pour le format des réquisitions**²¹⁷, force est de constater qu'ils ne sont pas mis en œuvre de manière constante et uniforme dans l'Union européenne.

Quoi qu'il en soit, ce déficit de connaissance dénote **un paradoxe : alors que les pouvoirs publics cherchent à renforcer l'accès aux données, la France ne dispose pas d'un mécanisme performant permettant d'apprécier le degré d'exécution des réquisitions.**

Ces constats conduisent la mission à formuler deux recommandations complémentaires.

Recommandation n° 8 : Instaurer un dispositif national, permanent et interministériel de suivi de l'exécution des réquisitions administratives et judiciaires. Ce dispositif devrait prioritairement porter sur l'identification des données sollicitées, la qualité, les délais et la motivation des réponses formulées par les plateformes.

Recommandation n° 9 : Soumettre les opérateurs et les fournisseurs à une obligation de publication d'indicateurs harmonisés sur l'exécution des réquisitions qui leur sont adressées.

Cette nouvelle obligation déclarative devrait pouvoir faire l'objet d'un contrôle effectif, le cas échéant assorti de sanctions proportionnées et dissuasives en cas d'absence de publication, de déclaration délibérément inexacte ou de dissimulation d'informations. Elle serait de nature à « visibiliser » les pratiques des plateformes, à favoriser la standardisation de leurs procédures internes et à créer un mécanisme de responsabilisation utile au pilotage des politiques publiques.

Un autre point mérite d'être soulevé : **le croisement des différents entretiens conduits par la mission ne permet pas d'affirmer avec certitude que les services et agents de l'État ayant recours aux réquisitions ont toujours la pleine connaissance des capacités offertes par le cadre existant.** Ainsi, il a semblé à la mission que les réquisitions se concentraient principalement, sinon exclusivement, sur les opérateurs de messagerie. Or, des acteurs plus périphériques, tels les **hébergeurs de données**, sont soumis aux obligations légales françaises et peuvent détenir des données de contenu en clair issues des messageries chiffrées²¹⁸.

²¹⁶ *Operational Challenges Faced by Law Enforcement Related to Access to Data. Input to the Second Plenary Meeting of the High-Level Group on Access to Data for Effective Law Enforcement*, Commission européenne, Direction générale des migrations et des affaires intérieures, 21 novembre 2023.

²¹⁷ ETSI, *Lawful Interception – Interface for warrant information*, mai 2026 (après de précédentes versions en 2024 et 2025). L'ETSI y définit « une interface électronique entre deux systèmes destinée à l'échange des informations nécessaires à la mise en œuvre et à la gestion d'une interception légale. Cette interface est destinée à l'échange des informations nécessaire à la mise en œuvre et à la gestion d'une interception légale. Cette interface est destinée (...) à être utilisée entre, d'une part, un fournisseur de services de communications et, d'autre part, une autorité chargée de l'application de la loi habilitée à demander la mise en œuvre d'une interception légale ».

²¹⁸ Il en est ainsi s'agissant des données de « *back-up* » : la sauvegarde de messages déchiffrés par un expéditeur ou un destinataire peut, dans certains cas, se faire en clair auprès des hébergeurs de données. Selon les applications, le chiffrement en vue du stockage est appliqué par défaut ou n'est pas appliqué, il revient alors à l'utilisateur de le paramétrer. En outre, selon les messageries, certaines

Ces cas sont probablement d'ampleur limitée mais il serait utile que les services réquisitionnaires analysent leurs pratiques et vérifient si l'ensemble des leviers de réquisition sont exploités. Au besoin, la mission estime qu'ils devraient pouvoir adapter leurs doctrines internes pour améliorer la circulation de l'information relative au cadre légal de réquisition et la formation des agents réquisitionnaires. Le ministère de la justice a lancé plusieurs initiatives en ce sens – formation des enquêteurs, acculturation des magistrats, guide de la preuve numérique – qui pourraient être utilement prolongées.

Recommandation n° 10 : Établir une doctrine de réquisition tenant compte du rôle de chaque acteur numérique dans la chaîne de gestion de la donnée de contenu des messageries chiffrées.

b) Les capacités des services doivent être renforcées

La seconde série de mesures consiste à consolider les capacités des services pour faire face à la réorganisation des enquêtes vers les données disponibles. De ce point de vue, la mission ne peut bien sûr qu'appeler à la poursuite de la consolidation budgétaire fixée par les différentes lois de programmation²¹⁹. En contexte budgétaire (et politique) tendu, la mission est toutefois conduite à privilégier des mesures d'optimisation.

- **Le volume des données collectées appelle une stratégie de retraitement renforcée**

Ce que nous avons appelé la « nouvelle économie des investigations » emporte un défaut majeur : elle a tendance à dégrader le ciblage des investigations. Privés d'accès au contenu, les enquêteurs sont conduits à élargir le périmètre de leurs recherches. Cette perte de précision se traduit par **l'augmentation considérable du volume de données à collecter pour prévenir les infractions et cartographier les organisations criminelles**.

À l'échelle européenne, les travaux conduits dans le cadre du programme SIRIUS, sous l'égide d'Europol et Eurojust, illustrent cette évolution générale. En 2023, huit fournisseurs de services ont reçu à eux seuls 266 855 demandes de communications de données émanant des autorités administratives et judiciaires, soit une progression de 22% en un an, dont 38 809 demandes pour la France (125 758 en Allemagne). Les demandes d'urgence ont, dans le même temps, augmenté de 17% pour atteindre 21 746 (ce qui, au demeurant, pèse sur les capacités des fournisseurs de services²²⁰), portant principalement sur les données de compte, les journaux de connexion et les adresses IP.

Les autorités administratives et répressives sont ainsi confrontées au traitement de plusieurs téraoctets, voire pétaoctets, de données numériques²²¹.

fonctionnalités permettraient de confier à l'hébergeur de données une clé de déchiffrement. Ces services visent à faciliter l'accès par un utilisateur à ses archives.

²¹⁹ La LOPMI et la LOPJ, adoptées l'une et l'autre en 2023.

²²⁰ Europol et Eurojust, *SIRIUS EU Electronic Evidence Situation Report 2024*, novembre 2024.

²²¹ Europol et Eurojust, *Common Challenges in Cybercrime*, 2024.

Certes, comme le soulignent plusieurs auteurs, « *avec la multiplication des traces numériques croît l'empire de la preuve, avec la multiplication des traces numériques accessibles à tout un chacun croît l'empire de l'enquête* »²²². Mais **la disponibilité « juridique » et technique des données – elle est en soi, nous l'avons exposé, une difficulté – ne suffit plus à garantir leur exploitation effective**. Leur volume, la diversité des supports et des formats imposent des capacités avancées de stockage et de rapprochement. L'ensemble des services entendus par la mission a confirmé que ces exigences mobilisent des moyens techniques et humains considérables qui demeurent parfois insuffisants au regard des volumes à traiter.

D'importants efforts ont cependant été engagés ces dernières années.

La loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (LOPMI) identifiait l'enjeu de transformation numérique comme un levier de renforcement des capacités opérationnelles des forces de sécurité intérieure, notamment dans le domaine de l'enquête, y compris les outils de retranscription et de traitement des données numériques collectées au cours de l'enquête. Le rapport annexé à la loi identifiait les cibles d'investissements que sont les capacités d'analyse, de traitement des données et de R&D. Dans le domaine des techniques d'enquête numérique judiciaire, l'ANTENJ joue un rôle pivot pour le développement des capacités de retraitement des données, qu'il s'agisse de la mise en oeuvre de la PNIJ ou de la conception d'outils innovants, à l'image de « modules » déployés pour le retraitement des données de localisation.

La mission constate toutefois que l'effort de renforcement des capacités techniques de retraitement des données numériques est aujourd'hui réparti entre plusieurs administrations, y compris au sein de la sphère judiciaire. S'il est souhaitable que les services développent une doctrine technique et tactique adaptée à leurs besoins opérationnels, le défi représenté par la montée en puissance volumétrique du recueil des métadonnées plaide pour **une stratégie unifiée de renforcement des outils de traitement des données de connexion en particulier et des données numériques en général**. Une attention particulière devant à cet égard être portée sur les capacités augmentées qu'offre le recours à l'intelligence artificielle.

Aussi, la mission recommande-t-elle de constituer une **agence nationale des techniques de retraitement des données** recueillies en filière administrative comme en matière judiciaire. Chargée de piloter la stratégie d'innovation et de conception des capacités de retraitement, de mutualiser et coordonner les initiatives, d'exercer en amont le contrôle de leur emploi, l'agence aurait vocation à s'appuyer sur les expertises acquises dans chacune des filières et à concentrer les ressources publiques qui y sont consacrées.

Recommandation n° 11 : Créer une agence nationale chargée de piloter et coordonner la stratégie d'innovation et de développement des capacités de retraitement des données numériques collectées dans le cadre des investigations administratives et judiciaires.

²²² O. Leclerc, É. Verges et G. Vial, « Preuves scientifiques et technologiques », Cahiers Droit, Sciences & Technologies, 15, 2022.

- **Les réflexions à conduire sur les techniques de recueil et de captation des données informatiques**

La forte augmentation du recours à la technique dite du « RDI », dans ses versants administratifs et judiciaires, invite à une réflexion d'ensemble des règles qui lui sont appliquées aux termes du code de la sécurité intérieure et du code de procédure pénale.

Un dénominateur commun se détache dans les deux filières : en renseignement (art. 853-2 du code de la sécurité intérieure) comme en judiciaire (art. 706-102-1 du code de procédure pénale), **le législateur a construit un régime juridique unique dans ses règles mais pluriel dans ses effets.**

Le recueil et la captation de données informatiques recouvrent en effet des techniques composites dont la mise en œuvre conduit à des atteintes d'intensité variables à la vie privée : la copie ponctuelle d'un fichier présent sur un disque dur ne présente pas le même degré d'intrusion que l'accès aux données au moment où elles s'affichent sur l'écran d'un terminal ou lorsqu'elles sont introduites par saisie de caractères.

L'observation est particulièrement vraie en matière de renseignement.

- **La recherche d'une modulation plus fine du RDI en renseignement**

Cette absence de « gradation juridique », que relève la CNCTR dans son dernier rapport d'activité²²³, se double d'une absence de sélectivité des dispositifs techniques quant aux données recueillies (critique du « chalutage »). Il appartient alors au service chargé de l'exploitation de cette technique, sous le contrôle de la CNCTR, d'opérer *a posteriori* le tri des données collectées afin de ne conserver que celles présentant un rapport avec la finalité poursuivie au titre de l'article L. 811-3 du code de la sécurité intérieure.

Dans le même temps, lorsque plusieurs techniques sont mises en œuvre à l'égard d'une même personne, la durée d'autorisation du RDI (deux mois) impose des renouvellements successifs pour accompagner, le cas échéant, une interception de sécurité (autorisée quant à elle pour quatre mois). Ce décalage engendre des contraintes opérationnelles pour les services et affecte, au demeurant, la mission de contrôle de la CNCTR²²⁴.

Dès lors, la mission estime que trois pistes de réflexion pourraient être envisagées : celle, sensible, de la modification de la durée des autorisations²²⁵ ; celle, complexe, de la modulation de cette durée selon le degré de l'atteinte à la vie privée résultant du dispositif technique employé ; celle, technologique, de l'amélioration de la sélectivité des dispositifs afin de circonscrire les données recueillies.

²²³ « (...) Le recueil de données informatiques ne connaît aucune gradation juridique. (...) À la différence d'une interception de sécurité, qui se prête à une sélection des conversations ou des échanges d'intérêt pour le service, un recueil de données informatiques est susceptible de collecter une quantité de données beaucoup plus grande dans un champ beaucoup plus large. Il revient alors au service chargé de l'exploitation de cette technique, sous le contrôle de la commission, de ne conserver que celles qui ont un rapport réel et plausible avec la finalité poursuivie. Ceci représente une charge pour le service de renseignement et constitue un point de vigilance pour la commission », CNCTR, *Rapport d'activité 2025*, p. 48.

²²⁴ *Ibid*, p. 59.

²²⁵ La question est posée de façon sensiblement différente en judiciaire où, finalité répressive oblige, les durées d'autorisation des captations judiciaires sont à la fois plus finement définies et plus étendues qu'en renseignement dont les finalités demeurent préventives. L'article 706-95-16 du CPP prévoit en effet une durée d'un mois, renouvelable une fois, au cours de l'enquête et de quatre mois, renouvelables jusqu'à deux ans, au cours de l'information judiciaire.

Ces trois pistes de réflexion sont liées entre elles. Une plus grande sélectivité des dispositifs techniques permettrait de mieux cibler les données recueillies sur les systèmes informatiques et, partant, de mieux maîtriser l'atteinte à la vie privée. La durée d'autorisation pourrait ainsi être modulée en fonction du degré d'intrusion effectivement attaché au dispositif employé et aux données susceptibles d'être recueillies.

Faute de pouvoir, à court terme, disposer de dispositifs techniques plus sélectifs, **l'objectif opérationnel effectivement poursuivi par le service à l'origine de la demande pourrait constituer un critère de modulation de la durée d'autorisation.**

Les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure étant relativement larges, la demande de RDI pourrait davantage préciser les données recherchées et leur lien avec l'objectif opérationnel poursuivi. Les conditions dans lesquelles les demandes de RDI doivent être formulées pourraient être enrichies en conséquence²²⁶.

Cette délimitation plus fine permettrait de mieux apprécier le degré d'intrusion attendu de la mesure et, par suite, d'adapter la durée des autorisations aux besoins opérationnels. Comme aujourd'hui, il appartiendrait au service chargé de l'exploitation, sous le contrôle de la CNCTR, d'écarter les données sans rapport réel ou plausible, non seulement avec l'une des finalités mentionnées à l'article 811-3 du code de la sécurité intérieure, mais avec l'objectif opérationnel et les catégories de données recherchées préalablement définis dans la demande d'autorisation.

Captation et recueil de données		
Service	Captation judiciaire des données	Recueil administratif des données
Finalité	Judiciaire	Renseignement
Base légale	Articles 706-102-1 à 706-102-5 du code de procédure pénale	Article L. 853-2 du code de la sécurité intérieure
Champ d'application	Articles 706-73 et 706-73-1 du code de procédure pénale	Article 811-3 du code de la sécurité intérieure
Condition	Si les nécessités de l'enquête l'exigent	Subsidiarité Proportionnalité
Autorisation	Juge des libertés et de la détention	Premier ministre, sur avis de la CNCTR
Mise en œuvre	STNCJ (DGSI)	Services spécialisés de renseignement
Contrôle	Juge des libertés et de la détention	CNCTR

²²⁶ Article L. 821-1 du CSI précise en effet les conditions dans lesquelles les demandes d'autorisation sont formulées et motivées.

- **L'organisation d'une stratégie unifiée de développement des dispositifs techniques**

En complément, la mission constate que **l'augmentation du recours au recueil et à la captation de données informatiques nécessite un effort soutenu en recherche et développement, en matière administrative comme judiciaire.**

L'objectif d'une plus grande sélectivité des dispositifs techniques devrait à cet égard constituer une priorité : de nature à desserrer le caractère « monolithique » des régimes juridiques actuels, elle permettrait de mieux proportionner les collectes opérées sur les systèmes informatiques.

De ce point de vue, la concentration auprès de la DGSJ des moyens nécessaires à la mise en œuvre, y compris judiciaire, des techniques de piégeage répondait à une logique qui conserve toute sa pertinence : réunir des compétences techniques rares, constituer un pôle d'expertise de haut niveau et éviter que les administrations ne se concurrencent.

Ce choix présente toutefois des limites : il concentre auprès d'un seul service des capacités de conception destinées à répondre aux besoins de l'ensemble des services d'enquête.

La mission estime nécessaire de faire évoluer cette organisation pour l'adapter à la montée en puissance des techniques de recueil et de captation des données informatiques. La conception et le développement des dispositifs techniques pourraient ainsi être confiés à une structure transversale, commune aux ministères de l'intérieur et de la justice, chargée de répondre aux besoins exprimés par les différents services. Ceux-ci seraient appelés à concentrer leurs moyens sur la mise en œuvre et l'exploitation opérationnelle des dispositifs.

La mission conclue de ces réflexions deux séries de recommandations.

La première tient à la nécessité de redimensionner les capacités techniques du RDI. Coûteuses, parfois incertaines et soumises à des procédures légitimement exigeantes, les techniques de piégeage ne sont certes pas industrialisables. **L'État devrait néanmoins tendre vers une organisation dans laquelle le recours au RDI serait effectivement déterminé par les exigences de subsidiarité, de nécessité et de proportionnalité et non contraint, en pratique, par des limites capacitaires aujourd'hui réelles.**

La mission recommande par conséquent la création d'**une direction technique nationale dédiée à la conception et au développement des dispositifs de recueil des données informatiques**, placée sous la double tutelle des ministères de l'intérieur et de la justice. Il s'agirait alors de mener à son terme la logique de mutualisation qui a présidé à l'organisation actuelle et d'accroître, en particulier, la masse critique des capacités en recherche et développement, en maintenance et en certification des dispositifs de piégeage, en y associant, le cas échéant, des laboratoires de recherche publics et privés, dans des conditions évidemment strictes de confidentialité.

Recommandation n° 12 : Créer une direction technique nationale, rattachée aux ministères de l'intérieur et de la justice, pour la conception, le développement et la certification des dispositifs techniques de recueil et de captation de données informatiques.

La seconde série de recommandation, en parallèle des préconisations de la mission en matière de techniques d'enquête numérique judiciaire (recommandation n° 3), tient à la nécessité d'apporter une réponse procédurale à la progression du recours au RDI en matière de renseignement en engageant la réflexion sur l'adaptation de son régime juridique, dont quelques pistes viennent d'être esquissées. Les garanties applicables pourraient ainsi être graduées en fonction de l'intensité de l'atteinte portée à la vie privée. Un socle commun de garanties serait appelé à cohabiter avec des exigences différenciées, permettant de mieux calibrer les contraintes juridiques qui doivent l'encadrer aux caractéristiques de chacune des modalités du RDI.

Recommandation n° 13 : Instaurer, en matière de renseignement, un régime juridique gradué du RDI reposant sur un socle commun de garanties, complété d'exigences adaptées au degré d'intrusion des différentes modalités de captation.

Document l'Informé

III) Conclusion : Face aux tensions sur le chiffrement, repenser la relation aux plateformes

Si, depuis la loi de 2004 pour la confiance dans l'économie numérique, le cadre juridique des communications électroniques a fait l'objet d'adaptations successives, les difficultés propres au chiffrement « de bout en bout » n'ont donné lieu que récemment à des tentatives de réformes. De ce point de vue, les débats ont été marqués, au cours des 12 derniers mois, par **une logique d'affrontement dont la mission constate qu'elle s'est avérée particulièrement improductive.**

A) Les clivages autour du chiffrement doivent être dépassés

1) Un débat hélas binaire : pour le chiffrement, tapez « 16 bis » ; contre, tapez « 8 ter »

Soutenu par le Gouvernement, l'épisode dit de « l'article 8 ter », un temps inséré dans la proposition de loi « de lutte contre le narcotrafic », procédait à une réécriture de l'article L. 871-1 du code de la sécurité intérieure. Le débat autour de cette disposition est d'ailleurs à l'origine de la présente mission, proposée par son rapporteur dès le printemps 2025, et formellement constituée au mois de janvier de cette année.

En lieu et place de l'obligation, pour les prestataires de cryptologie, de remettre dans un délai de soixante-douze heures les conventions de déchiffrement, l'article 8 ter entendait leur imposer la transmission des données déchiffrées issues des informations, documents, données ou renseignements dont la collecte aurait fait l'objet, au préalable, d'une autorisation de mise en œuvre des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4, L. 851-6, L. 852-1, L. 852-3 et L. 853-2 du code de la sécurité intérieure.

Au terme de cet article, introduit par voie d'amendement, les entités visées n'auraient pu exciper d'aucun motif contractuel ni technique pour faire obstacle à cette obligation, tranchant avec les dispositions actuelles du code de la sécurité intérieure dont nous avons vu qu'elles prévoient la possibilité, pour les opérateurs ou fournisseurs de services, de s'opposer à la transmission des conventions de déchiffrement, dès lors qu'ils démontrent ne pas être en mesure de satisfaire aux réquisitions²²⁷.

La mission observe que l'article 8 ter était conçu, par ses auteurs, comme une riposte à l'affirmation selon laquelle les opérateurs et fournisseurs de services ne détiennent pas les clés de chiffrement, rejoignant les soupçons que nous avons décrits plus haut dans le rapport.

Afin d'en assurer l'effectivité, le dispositif renforçait le régime des sanctions applicables, les manquements étant passibles d'une amende pouvant atteindre 1,5 million d'euros et, pour les personnes morales, 2% du chiffre d'affaires mondial annuel²²⁸.

²²⁷ Art. L. 871-1, al. 1^{er}, 2^{de} phrase, déjà évoqué.

²²⁸ Hors taxes.

L'article 8 ter visait également à ce que les vulnérabilités le cas échéant engendrées par l'ouverture d'un canal de transmission en clair des informations chiffrées, soient comblées par les opérateurs et fournisseurs eux-mêmes. Le ministre de l'Intérieur de l'époque pouvait alors affirmer, à l'occasion des débats parlementaires, au Sénat comme à l'Assemblée nationale, que l'article 8 ter entendait substituer à l'actuelle « *obligation de moyen* » une simple « *obligation de résultat* », sans préjuger des solutions techniques retenues.

Pour y parvenir, l'amendement sénatorial apportait plusieurs modifications au CPCE, complétant les prescriptions de l'article L. 33-1²²⁹ par celles relatives à « *la protection des intérêts fondamentaux de la Nation* ». Il insérait, enfin, une nouvelle section 10 au sein du même code pour soumettre les plateformes aux « *prescriptions exigées par l'ordre public, la défense nationale, la sécurité publique ou la protection des intérêts fondamentaux de la Nation* » pour l'exécution des techniques d'enquête numérique judiciaire comme des techniques de recueil de renseignement²³⁰.

Ces dispositions ont ravivé, au-delà de la seule représentation nationale, le débat sur l'ouverture de « *backdoors* ».

Ces craintes n'étaient d'ailleurs pas nouvelles. Il convient de rappeler que la perspective d'introduire des « *backdoors* » a été un temps assumée par l'État. Ainsi, dans une réponse du 18 février 2020 à la question écrite n° 10778 de M. Julien Borowczyk, le Gouvernement reconnaissait étudier l'approche par « *porte dérobée* », et soulignait que « *cette évolution dépend[ait] cependant des négociations entre l'État et les concepteurs de ces solutions de communication. Ces négociations ne sont pas rendues publiques. De même, cette approche nécessite des évolutions du cadre juridique existant qui doivent faire face aux divisions de l'opinion publique, opposant les exigences de sûreté nationale à la défense des libertés publiques* »²³¹.

À l'occasion des débats sur l'adoption de l'article 8 ter, le Gouvernement avait toutefois infléchi cette analyse, en soutenant que le dispositif ne relevait pas d'une « *backdoor* » et qu'il revenait aux plateformes de construire la solution technique la plus adaptée.

En réaction aux débats suscités par l'article 8 ter, le projet de loi relatif à la résilience des infrastructures et au renforcement de la cybersécurité, qui constitue le véhicule de transposition de trois textes européens²³², a vu être introduit, toujours au Sénat, et contre l'avis de la commission parlementaire spécialement constituée comme du Gouvernement, un article 16 bis dont la

²²⁹ On rappellera ici que le I de l'article L. 33-1 CPCE fixe plusieurs limites au principe de liberté de l'établissement et de l'exploitation des réseaux ouverts au public, ainsi que de la fourniture de services de communications électroniques, lequel s'exerce en particulier sous réserve « des prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre ».

²³⁰ Le III du nouvel article L. 34-18 renvoyait à un décret en Conseil d'État la définition des garanties de juste rémunération prévues au e du I de l'article L. 33-1 du CPCE. Le IV permettait toutefois, à titre exceptionnel, au ministre chargé des communications électroniques d'autoriser les opérateurs ou prestataires à déroger aux obligations prévues au II lorsque les coûts permettant d'y satisfaire sont disproportionnés au regard du nombre de demandes.

²³¹ Assemblée nationale, réponse du 18 février 2020 à la question écrite n° 10778 de M. Julien Borowczyk, JORF du 18 février 2020, p. 1259.

²³² La directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques dite « directive REC » ; la directive (UE) 2022/2555 du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite directive « NIS 2 » ; et la directive (UE) 2022/2556 visant à adapter plusieurs directives sectorielles au règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, dit « règlement DORA ».

rédaction, modifiée par l'Assemblée nationale, dispose qu'« *il ne peut être imposé aux fournisseurs de services de chiffrement, y compris aux prestataires de services de confiance qualifiés, l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques tels que les clés de chiffrement maîtresses, ou tout autre mécanisme ou processus permettant un accès non consenti aux données protégées* ».

L'exposé sommaire des auteurs de l'amendement ayant conduit à l'adoption de l'article 16 bis exprimait, sans ambiguïté, l'objectif poursuivi : « *certaines initiatives législatives et réglementaires, tant au niveau national qu'international, ont cherché à imposer aux fournisseurs de services de chiffrement des obligations visant à insérer des dispositifs techniques permettant un accès aux données protégées par des tiers, notamment par les autorités publiques. Ces dispositifs, communément appelés portes dérobées (backdoors), clés de déchiffrement maîtresses ou autres mécanismes d'affaiblissement volontaire de la sécurité, présentent des risques considérables pour la sécurité informatique et la protection des droits fondamentaux* ». Les auteurs de l'amendement invitaient ainsi « *à inscrire dans la loi un principe clair de sécurité numérique* »²³³.

La commission spéciale de l'Assemblée nationale a d'ailleurs confirmé, tout en l'étendant, cette intention, complétant la notion de « *mécanisme* » retenue par le Sénat par celle, plus large, de « *processus* », dans le but d'interdire tout contournement des systèmes de sécurité et de confidentialité par des dispositifs non intégrés techniquement aux systèmes de chiffrement, à l'image de la conservation ou de la transmission de copies de clés privées permettant le déchiffrement des communications.

L'article 16 bis est ainsi devenu, au fil des débats parlementaires, le pendant exactement inversé de l'article 8 ter : là où ce dernier entendait garantir un accès au contenu intelligible des communications malgré le chiffrement, l'article 16 bis érige en principe général l'interdiction d'imposer aux fournisseurs tout mécanisme susceptible d'en altérer l'intégrité.

2) L'article 16 bis du projet de loi « résilience » : de très nombreuses réserves juridiques

Au-delà de son objectif affiché, la rédaction de l'article 16 bis invite à s'interroger, ainsi que l'a fait la Délégation parlementaire au renseignement, sur le risque de « [fragilisation du] *cadre juridique des techniques de renseignement et d'enquête* »²³⁴ et, par conséquent, celui d'entraver leur mise en œuvre. **La mission tient à cet égard à souligner les nombreuses zones d'ombre juridiques qui entourent la rédaction de cette disposition.**

- Deux motifs d'inquiétude

Le premier motif d'inquiétude tient au fait que l'article 16 bis, s'il était définitivement adopté par le Parlement, impliquerait **l'adoption unilatérale par la France d'un principe général susceptible de faire obstacle à toute évolution future des modalités d'accès légal aux données.** Alors que les réflexions sont engagées entre les États membres de l'Union européenne pour élaborer une réponse commune aux difficultés créées par le chiffrement « de bout en bout », dans

²³³ L'amendement n°1 rect. quinquies présenté par M. Olivier Cadic et plusieurs de ses collègues a été adopté lors du scrutin public du 12 mars 2025 par 181 voix pour et 134 voix contre dont 129 sénateurs (sur 131) du groupe *Les Républicains* et 5 sénateurs (sur 59) du groupe de l'*Union Centriste*.

²³⁴ Communication de la DPR, mai 2026.

le respect de nos libertés publiques, une telle initiative serait de nature à isoler notre pays face à des opérateurs dont l'activité, arrimée au marché unique numérique, dépasse le cadre national.

2. Le second motif d'inquiétude tient au déséquilibre que le principe général posé par l'article 16 bis pourrait introduire dans les relations entre l'État et les acteurs numériques : ceux-ci ne manqueraient d'exciper de sa portée générale, et de sa contrariété avec les textes en vigueur instituant leurs obligations en matière d'interceptions légales, pour tenter de s'y soustraire.

Ces deux motifs d'inquiétude demeureraient théoriques s'ils ne s'appuyaient sur l'analyse des termes mêmes de l'article 16 bis.

- Trois zones d'incertitude aux termes de la rédaction actuelle du 16 bis

La première incertitude tient à l'étendue des procédés susceptibles d'être couverts par l'interdiction prévue à l'article 16 bis. Si le législateur entend interdire, par cette disposition, « *l'intégration de dispositifs techniques visant à affaiblir la sécurité des systèmes d'information et des communications électroniques tels que les clés de chiffrement maîtresses* », il prohibe également, dans une seconde branche de sa rédaction, tout « *mécanisme ou processus permettant des accès non consentis aux données protégées* ».

Cette seconde formulation dépasse sensiblement la seule question des « portes dérobées » ou des « clés maîtresses » mises en avant par les auteurs de l'article 16 bis. Par principe, les techniques de renseignement et d'enquête numérique ne sauraient reposer sur le consentement des personnes concernées. Qu'il s'agisse de l'interception d'une communication, de la réquisition de données informatiques, de l'installation d'un dispositif technique sur un terminal ou, plus largement, de toute autre modalité d'accès légal aux informations protégées par le secret des correspondances, ces techniques ont en commun d'être imposées à leur destinataire.

Dès lors, si la première branche de l'article 16 bis est circonscrite aux dispositifs susceptibles d'affaiblir le chiffrement, la seconde ne définit ni la nature des « *mécanismes ou processus* » concernés ni les techniques auxquelles elle s'appliquerait. **Sa généralité est par conséquent de nature à affecter le principe même des techniques de renseignement et d'enquête numérique.**

La deuxième objection tient à la notion de « données protégées ». Là-encore, si l'intention du législateur était de viser les seules données dont le contenu est protégé par le chiffrement, la rédaction retenue aux termes de l'article 16 bis vise mal sa cible.

La protection d'une donnée peut, en effet, intervenir à deux niveaux, éventuellement cumulatifs : sur la donnée elle-même, lorsqu'un procédé cryptographique en transforme le contenu en une forme inintelligible en l'absence de la clé requise ; ou sur les conditions de son accès, lorsqu'un mécanisme d'indentification, d'authentification ou de contrôle d'accès (identifiant, mot de passe, code PIN, dispositif biométrique, ...) réserve sa consultation ou son utilisation aux personnes habilitées. Une donnée conservée en clair peut ainsi être placée derrière un contrôle d'accès, tandis qu'une donnée chiffrée peut être accessible sans que son contenu puisse être exploité en clair. Les deux niveaux de protection sont fréquemment combinés, le secret présenté par l'utilisateur permettant alors de déverrouiller et de « dériver » la clé cryptographique.

Dès lors, en l'absence d'une définition plus précise, la notion de « *données protégées* » est susceptible de désigner, non seulement les données rendues inintelligibles par la technique du chiffrement, mais également celles, chiffrées ou non, dont l'accès est subordonné à un simple mécanisme d'authentification ou de contrôle d'accès. **L'article 16 bis pourrait ainsi recevoir une interprétation excédant les seules technologies de chiffrement et englober tout dispositif destiné à protéger l'accès aux données.**

Pris ensemble, les deux critères retenus – l'accès non consenti et les données protégées – ne permettent pas d'identifier les procédés techniques couverts par l'interdiction qui résulterait de la disposition législative en cours d'examen.

Enfin, une troisième incertitude juridique tient à l'identification des opérateurs auxquels l'interdiction posée par l'article 16 bis serait applicable.

Si la notion de « *prestataire de services de confiance qualifié* » renvoie à une catégorie définie par le règlement (UE) 910/2014 du 23 juillet 2014 (« eIDAS »), celle de « *fournisseur de services de chiffrement* » est parée, en l'état de notre droit, d'un halo d'indétermination ... Elle ne correspond, en effet, à aucune catégorie juridique stabilisée. L'expression est certes employée, de manière assez constante, dans la littérature technique et peut à cet égard désigner les entreprises fournissant à des tiers une fonctionnalité de chiffrement, soit comme service autonome, soit comme composante d'un service de communication sécurisé, en particulier les messageries chiffrées. Mais, faute de définition plus précise, **il n'est pas possible de déterminer si l'article 16 bis serait limité aux opérateurs dont le chiffrement constitue l'objet même du service ou s'il s'étendrait à ceux qui, tout en proposant des services d'une autre nature, mettent en œuvre des mécanismes de chiffrement destinés à protéger les données qu'ils hébergent, stockent ou transmettent.**

Une telle interprétation pourrait ainsi conduire à y inclure certains réseaux sociaux, plateformes collaboratives ou, plus étrangement encore, des services de visioconférence intégrant un chiffrement « de bout en bout » ...

Au total, quelle que soit l'interprétation retenue de l'article 16 bis – extensive pour ses détracteurs, restrictive pour ses défenseurs – la mission observe que les ambiguïtés inhérentes à sa rédaction sont susceptibles de produire des effets juridiques non maîtrisés par ses auteurs et, ainsi, de favoriser l'émergence d'un contentieux abondant²³⁵, inévitablement source d'insécurité juridique pour nos services d'investigation administratifs et judiciaires.

Dès lors, la mission ne peut que recommander d'écarter définitivement cette disposition qui, au demeurant, ne trouve aucune application comparable dans aucun des États-membres de l'Union européenne, ni au-delà d'ailleurs.

²³⁵ Au-delà de ces difficultés juridiques, d'autant plus préoccupantes qu'elles recouvrent un domaine d'une particulière sensibilité, l'article 16 bis constitue désormais le principal point de blocage de l'adoption du projet de loi et, par voie de conséquence, de l'achèvement par la France de la transposition de la directive (UE) 2022/2555 du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (NIS 2). Il convient en effet de rappeler que cette directive devait être transposée au plus tard le 17 octobre 2024 et que la Commission européenne a engagé, sur le fondement de l'article 258 du traité sur le fonctionnement de l'Union européenne (TFUE), une procédure en manquement contre la France. Après une lettre de mise en demeure adressée le 28 novembre 2024, la Commission a émis, le 7 mai 2025, un avis motivé, dernière étape avant une éventuelle saisine de la CJUE.

Recommandation n° 14 : Renoncer aux dispositions de l'article 16 bis du projet de loi dit de « résilience », compte tenu des sérieuses zones d'ombre qu'emporte sa rédaction.

B) Une double approche à construire avec les plateformes, coopérative et contraignante

Au terme de ses travaux, la mission estime qu'il est indispensable de réengager un dialogue structuré entre l'État et les acteurs numériques.

La mission n'ignore pas que, pour un certain nombre de services de l'État, le dialogue ne pourrait s'établir dans de bonnes conditions qu'en renforçant la position des autorités publiques *via* un durcissement préalable du cadre juridique imposé aux fournisseurs de services, lequel passerait par l'obligation, de type « 8 ter », de transmettre les données chiffrées en clair.

Cette stratégie, lorsqu'elle a été conduite, n'a pas toujours été couronnée de succès ... À l'image de la démarche du *Home Office* britannique engagée contre *Apple* et finalement abandonnée, les initiatives nationales semblent vouées à l'échec.

Un tel choix reste bien sûr possible et relève de l'appréciation du pouvoir politique. Il implique néanmoins que les conséquences susceptibles d'en résulter sur les réquisitions en cours, sur les plans économique et diplomatique également, soient intégrées dans l'arbitrage public.

La mission privilégie une stratégie différente.

Elle recommande, en premier lieu, dans sa proposition n° 6, de faire de la préservation de la disponibilité des métadonnées, aujourd'hui fortement compromise par les politiques de « *data minimisation* », un objectif stratégique à part entière, de même niveau que la recherche de solutions juridiques et techniquement neutres, d'accès aux contenus aux fins de prévention et de répression.

Elle recommande, en second lieu, dans ses propositions n° 7, 8, 9 et 10, de soumettre les opérateurs et les fournisseurs de services à de nouvelles obligations de transparence sur le traitement des réquisitions et les données qu'ils détiennent effectivement, tout en renforçant la capacité des services à assurer le suivi des réquisitions administratives et judiciaires.

Elle recommande, en troisième lieu, dans ses propositions n° 2, 3, 4, 5, 11, 12 et 13, d'adapter le cadre juridique des techniques de renseignement et d'enquête numérique judiciaire ainsi que d'accroître les capacités techniques de traitement des services pour faire face au véritable « mur de la donnée » qui se dresse devant eux pour contourner les effets du chiffrement.

Elle recommande, enfin, après avoir écarté l'initiative dite de « l'article 16 bis » (proposition n° 14), de réengager la relation avec les plateformes numériques, non sans avoir au préalable introduit de nouvelles mesures de fermeté (propositions n° 4 et 5).

C'est l'objet des développements qui suivent.

1) Une meilleure coopération avec les acteurs numériques doit être engagée

Le dialogue entre l'État et les acteurs du numérique devrait pouvoir porter sur deux volets complémentaires.

- *Renouer avec l'esprit de 2015 et le « groupe de contact permanent »*

Le premier volet vise à atteindre une série d'améliorations de nature « procédurale » ou « fonctionnelle » qui ne résultent pas directement du chiffrement.

Plusieurs services de l'État ont mentionné les avancées obtenues dans la coopération avec les plateformes *via* le « **groupe de contact permanent** » mis en place à la suite des attentats du 13 novembre 2015 à Paris et à Saint-Denis. À titre d'exemple, les autorités publiques et les acteurs numériques s'étaient accordés pour développer des plateformes standardisées de réquisition, remplaçant les procédures adoptées de manière empirique par les agents habilités, lesquels procédaient souvent par simples courriers électroniques de réquisition, sans format uniformisé, présentant parfois des lacunes fragilisant la procédure elle-même.

La mission estime qu'il est urgent de recréer le cadre d'un dialogue structuré entre l'État et les messageries. Il devrait pouvoir prendre la forme de rencontres plénières et de sessions dédiées à chaque entreprise pour tenir compte de ses spécificités et du secret des affaires. Ce dialogue devrait bien sûr être également conduit à une échelle plus large, par exemple dans le cadre d'une initiative européenne. La Commission européenne s'y montre favorable dans sa feuille de route de juin 2015 sur l'accès licite et effectif aux données.

Recommandation n° 15 : Engager un dialogue structuré et permanent entre l'État et les acteurs du numérique afin d'améliorer les conditions de leur coopération opérationnelle.

- *Développer et confronter des solutions techniquement neutres d'accès aux données*

Le second volet porte sur le cœur des difficultés : construire des solutions techniques d'accès aux contenus, selon des finalités strictement délimitées et sans affaiblir le chiffrement.

Sur ce point, les scientifiques et les industriels rencontrés par la mission ont témoigné de plusieurs pistes de travail, bien qu'elles suscitent parfois des interrogations en termes de faisabilité, voire d'opportunité. Il est utile d'en restituer – avec prudence – les principaux mécanismes.

- Une première série d'hypothèses vise un accès différé aux données.

Le registre des clés

Ce scénario viserait à réunir des « clés privées » de déchiffrement dans des coffres-forts numériques, accessibles aux seules personnes agréées. Le niveau de chiffrement – c'est-à-dire la complexité des clés – ne feraient pas l'objet d'un affaiblissement. Le risque proviendrait en revanche de cyberattaques sur les registres de clés, à des fins de détournement. En outre, les opposants à cette technique mettent en avant la complexité inhérente à la tenue de registres, ainsi que la

difficulté d'établir un cadre d'emploi unanimement admis. Dès les années 1990, l'hypothèse de registres de clés avait été évoquée puis abandonnée, pour ces mêmes raisons. Pour ses défenseurs, au contraire, cette option permettrait de créer des registres limités aux réquisitions légalement encadrées des services d'investigation. Le risque de détournement serait réduit par un « découpage des clés » et la remise des segments à plusieurs entités distinctes. Les segments de clés pourraient faire l'objet de mises à jour régulières ou dès lors qu'un risque de détournement aurait été identifié.

Les données de « back-up »

La sauvegarde de messages déchiffrés par un expéditeur ou un destinataire peut, dans certains cas, se faire en clair auprès d'hébergeurs de données. Selon les applications, le chiffrement en vue de la sauvegarde est appliqué par défaut ou n'est pas appliqué : il revient à l'utilisateur de le paramétrer. En outre, selon les messageries, certaines fonctionnalités permettraient de confier à l'hébergeur de données une clé de déchiffrement, afin notamment de faciliter l'accès de l'utilisateur à ses archives (en cas de perte d'un appareil, par exemple).

- Une seconde série d'hypothèses vise l'accès en temps réel aux données.

L'utilisateur fantôme

Cette technique consiste à introduire, à l'insu des utilisateurs légitimes, une tierce partie invisible dans un canal de communication électronique. La tierce partie a ainsi accès à l'intégralité des échanges entre les utilisateurs légitimes, sans nécessairement intervenir dans les correspondances. Ce scénario ne présenterait pas d'affaiblissement technologique du chiffrement, le protocole de chiffrement continuant de fonctionner normalement. En revanche, le mécanisme pourrait être exploité et contourné par des cyberattaquants. Ceux-ci pourraient usurper les droits des tiers introduits dans les canaux de communication ou obtenir les autorisations initiales accordées par le gestionnaire du service en se faisant passer pour un tiers légalement autorisé à intégrer le flux de communication. Pour ses détracteurs, cette solution serait quoi qu'il en soit contraire à la philosophie même du E2EE qui suppose l'exclusion d'une tierce partie à l'échange.

L'exploitation des registres de clés publiques

Dans les messageries actuelles, les registres sont généralement gérés par l'entreprise proposant la solution de communication. Ces registres distribuent automatiquement les clés permettant de chiffrer les communications entre utilisateurs. Ce système peut être exploité ou compromis pour permettre à un tiers de remplacer la clé publique d'un utilisateur par la sienne. Les messages sont alors chiffrés avec une fausse clé, ce qui permet au tiers de les lire avant de les retransmettre au véritable destinataire, sans que les deux correspondants légitimes s'en aperçoivent. Le chiffrement reste techniquement intact.

Le « safety number »

Le « safety number » garantit que, sur une application de messagerie, les expéditeurs et destinataires qui échangent sont bien les interlocuteurs légitimes. Des processus de vérification de ces numéros et de leur attachement à un utilisateur légitime sont prévus par les messageries afin de se prémunir contre toute usurpation d'identité. Selon certains experts, les services de

messaging, en tant qu'initiateurs de « *safety numbers* », pourraient faciliter l'insertion d'interlocuteurs tiers en lieu et place de correspondants légitimes, et ce à l'occasion des opérations de vérification de ces numéros de sécurité. Cette hypothèse présente de nombreuses limites techniques et opérationnelles, mais elle est identifiée comme un processus maîtrisé, au moins partiellement, par les fournisseurs de services.

Les « *client side coming* »

L'« analyse côté client » est une technique algorithmique consistant à analyser les données contenues dans une correspondance (texte, images, vidéos, fichiers) au regard d'une base de données de contenus interdits. L'analyse intervient avant l'envoi du message au destinataire. Cette solution n'ouvre pas d'accès aux contenus chiffrés pour des tiers mais isole les seuls contenus identifiés comme illicites. Divers risques associés à cette technique sont relevés : liés à la cybersécurité (augmentation de la surface d'attaque des messageries) ou à la fiabilité du traitement algorithmique (risques de faux positifs).

Il n'est évidemment pas dans les capacités de la mission, ni dans son rôle, de produire des recommandations opérationnelles sur ces hypothèses de travail. Elles montrent, en revanche, qu'un bouquet de solutions techniques peut servir de base de dialogue entre les autorités publiques et les acteurs numériques.

Sur ce sujet, deux remarques.

D'une part, seule une analyse informée, robuste et soumise au contradictoire de ces hypothèses de travail sera de nature à en mesurer l'opportunité au regard des objectifs à concilier : le renforcement de l'accès aux données pour les besoins des forces de sécurité et de justice, la protection des libertés fondamentales et la sécurité des systèmes d'information.

D'autre part, il ne suffira évidemment pas de frapper à la porte des opérateurs des plateformes pour les convaincre de tester la robustesse des solutions techniques envisagées, aussi pertinentes soient-elles. L'intérêt immédiat de ces opérateurs mondialisés est bien sûr de prolonger un modèle économique solide, générant d'immenses profits, avec à leur disposition une multitude d'ordres juridiques désynchronisés. Sans doute faudra-t-il en passer par une phase beaucoup plus avancée qu'aujourd'hui sur le plan des pistes de réflexions technologiques pour déclencher le dialogue, allant peut-être jusqu'au **prototypage des solutions techniques**²³⁶. C'est en tout cas la conviction acquise par la mission.

Ces observations invitent par conséquent à recommander au Gouvernement d'approfondir les hypothèses techniques de contournement du chiffrement technologiquement neutres.

Pour ce faire, **une *task force* interministérielle**, composée des services techniques et des directions juridiques pertinents, issus de la sphère « sécurité-justice » et « numérique »²³⁷, devrait

²³⁶ À titre de comparaison, le Pôle d'expertise de la régulation numérique (PEReN) et la CNIL ont élaboré en 2022 une solution expérimentale de vérification d'âge en ligne qui, bien sûr, ne recouvre pas un défi technologique comparable. Mais cette proposition visait à démontrer que des solutions pouvaient être performantes, robustes, peu contraignantes et respectueuses de la vie privée des utilisateurs.

²³⁷ Par exemple la Direction interministérielle du numérique (DINUM), placée sous l'autorité du Premier ministre, et le ministère du numérique.

être formée à très court terme, par exemple sous la double direction de la CNRLT et du SGDSN. Avec un objectif prioritaire : **piloter une démarche offensive et partagée de consolidation des hypothèses techniquement neutres d'accès aux données.**

Cette dynamique devrait s'ouvrir aux laboratoires publics de recherche et aux acteurs industriels. Dans ces deux écosystèmes, la France a vu se développer des compétences de premier plan en cryptographie, cybersécurité et rétro-ingénierie. Des programmes de recherche et développement pourraient être lancés : en matière de cryptographie, la mission observe que l'essentiel de l'effort de R&D a en effet été porté, ces dernières années, vers le renforcement du chiffrement. De nouveaux axes de recherche pourraient ainsi être déployés vers des solutions d'accès aux données de communication, dans des conditions maximales de sécurité numérique.

Quand bien même cette démarche conduirait à l'identification de solutions opérationnelles et acceptables, la mission observe que des obstacles ne manqueraient pas de se dresser.

Certains fournisseurs de messageries, fondées par construction sur la pleine confidentialité des communications, refuseraient d'entrer dans une démarche coopérative ou même exploratoire. Des usagers pourraient également migrer vers d'autres services. Ces effets de report vaudraient aussi en matière de criminalité. Ils seraient probablement accentués par la mise à disposition en « *open source* » de protocoles qui permettent le développement libre de messageries chiffrées « de bout en bout ». De fait, des groupes criminels eux-mêmes ont pu développer leurs propres solutions de messagerie chiffrée « de bout en bout »²³⁸.

D'autres techniques de contournement pourraient s'affirmer, par exemple les services de communication utilisant des réseaux décentralisés ou « *mesh networks* », qui minimisent par nature la collecte de données de connexion. La migration de messageries chiffrées vers ce type de réseaux ferait alors perdre l'accès aux données de communication et de connexion. Quant au développement du chiffrement « anamorphique », encore au stade du prototypage, il permettrait à des services de messagerie de donner des illusions de coopération, tout en offrant aux utilisateurs des capacités d'échange intégralement confidentielles.

Ces limites, aussi fortes soient-elles, ne doivent pas conduire à renoncer à une approche partenariale avec les plateformes, ce qui n'exclue d'ailleurs par une forme de confrontation, nous venons de le voir, en ce qui concerne les solutions techniques envisageables, et ce pour deux raisons. D'une part, de futures avancées techniques pourraient aboutir, à terme, à des solutions satisfaisantes pour conjuguer un accès ciblé aux données de communication et une sécurité maximale des systèmes d'information. D'autre part, la démarche globale de responsabilisation des plateformes numériques, qui s'affirme certes lentement et pas à pas en matière de régulation des contenus, doit inclure les messageries chiffrées.

Recommandation n° 16 : Constituer une *task force* interministérielle, pilotée par la CNRLT et le SGDSN, pour renforcer le partage de connaissance, identifier, concevoir et évaluer les solutions techniques envisageables pour accéder, sans affaiblir le chiffrement, aux contenus nécessaires à la lutte contre la délinquance et la criminalité organisées ainsi que le terrorisme.

²³⁸ Fin 2024, par exemple, dans le cadre de la lutte contre le trafic de stupéfiant, la France et les Pays-Bas ont démantelé un réseau utilisant une solution de communication chiffrée développée en interne par un groupe criminalisé officiant à partir du protocole *open source* Matrix.

2) Un déchiffrement forcé n'emporterait aucun avantage pour les politiques de sécurité

L'obligation de mise au clair des données chiffrées était, nous l'avons rappelé, l'ambition de du Gouvernement dans le cadre des débats sur la proposition de loi dite de « lutte contre le narcotrafic ». Il n'est pas besoin de rappeler que les principaux groupes politiques de l'Assemblée nationale, qui ne trouvent pas toujours matière à se rejoindre, s'étaient assez largement accordés pour le rejeter²³⁹. Au-delà, toutefois, de ces circonstances, et en conclusion des développements précédents, **la mission considère qu'une réforme de cette nature ne permettrait pas de résoudre la difficulté d'accès aux contenus chiffrés.**

En premier lieu, tout porte à penser que l'ancien article 8 ter, s'il avait été définitivement adopté par le Parlement, aurait principalement conduit les plateformes soit à annoncer leur retrait immédiat ou différé du marché national, comme ce fut le cas en son temps au Royaume-Uni, soit, plus sûrement encore, à refuser d'exécuter les réquisitions prises sur ce fondement. Avec, au demeurant, ce paramètre incontournable, que l'on s'en réjouisse ou qu'on le déplore : **à l'ère de la massification des échanges numériques, nous ne savons pas, en l'état de la technologie, faire fonctionner à grande échelle des systèmes sûrs sans chiffrement « de bout en bout ».**

En second lieu, la mission retient que la philosophie sur laquelle reposait l'ancien article 8 ter procédait d'un raisonnement pour le moins fragile : une obligation juridique de résultat était supposée faire naître une solution technique. « *Dura lex, sed lex* », certes ; mais, tout autant, « *nemo ad impossibilia tenetur* ». En d'autres termes, la loi peut imposer une obligation ; elle ne peut, par sa seule force, créer les conditions de son exécution.

Il faut donc ici renverser le raisonnement : ce n'est pas de l'obligation juridique que peut naître la solution technique ; c'est de l'identification préalable d'une solution technique, permettant un accès ciblé aux contenus protégés, sans compromettre l'intégrité du chiffrement, et donc en protégeant notre sécurité numérique comme nos libertés publiques, que pourrait procéder, le cas échéant, une nouvelle obligation légale.

La mission constate que cette condition n'est pas aujourd'hui réunie. Elle n'en conclut pas qu'il faille renoncer à la rechercher. Au contraire, elle préconise d'intensifier les travaux déjà engagés par les services de l'État pour identifier les différentes hypothèses de travail, dont certaines ont été décrites dans le présent rapport. Plus encore, la mission préconise de porter ces travaux à une échelle plus structurée et offensive, d'en modéliser et éprouver la faisabilité, ainsi que les garanties, puis d'en organiser le développement et la confrontation, y compris avec les plateformes.

Recommandation n° 17 : Écarter toute disposition comparable à l'ancien article 8 ter tant que n'a pas été établie la faisabilité d'une solution technique permettant un accès strictement ciblé aux contenus protégés, sans compromettre le chiffrement, la confidentialité des échanges ni la sécurité des systèmes numériques.

²³⁹ Après sa suppression en Commission des lois de l'Assemblée nationale, l'article 8 ter avait fait l'objet de plusieurs amendements de rétablissement, dans une rédaction toutefois modifiée. Ils ont été rejetés en séance publique du 20 mars 2025 par 119 voix contre, 24 voix pour et 6 abstentions.

Liste des entités entendues ou contributrices

Campus Cyber I Commission nationale de contrôle des techniques de renseignement I Commission nationale de l'informatique et des libertés (CNIL) I Coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) I Direction interministérielle du numérique (DINUM) I Dr Alain Couvreur, enseignant-chercheur (Institut polytechnique de Paris) I Dr Cristina Onete, enseignante-chercheuse (université de Limoges) I Dr Philippe Gaborit, enseignant-chercheur (université de Limoges) I Dr Olivier Blazy, enseignant-chercheur (Institut polytechnique de Paris) I European Digital Rights (EDRi) I Google I Ildata I La Quadrature du Net I M. Ivan Kwiatkowski, expert en sécurité informatique I M. Matthieu Bouthors, président de Hackerzvoice (HZV) I Meta Platforms – WhatsApp I Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique – Direction générale des Douanes et des Droits indirects (DGDDI) – Direction nationale du renseignement et des enquêtes douanières (DNRED) I Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique – Direction générale des Entreprises – Service de l'économie numérique I Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique – Direction générales des Entreprises – Commissariat aux communications électroniques de défense (CCED) I Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique – TRACFIN I Ministère de l'Intérieur – Direction générale de la Gendarmerie nationale (DGGN) I Ministère de l'Intérieur – Direction générale de la Police nationale (DGPn) I Ministère de l'Intérieur – Direction générale de la Sécurité intérieure (DGSI) I Ministère de l'Intérieur – Secrétariat général – Direction des libertés publiques et des affaires juridiques (DLPAJ) I Ministère de la Justice – Agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ) I Ministère de la Justice – Direction des affaires criminelles et des grâces (DACG) I Ministère de la Justice – parquet national anticriminalité organisée I Ministère de la Justice – parquet national anti-terroriste I Ministère de la Justice – procureure de la République près le tribunal judiciaire de Paris I Ministère des Armées et des Anciens combattants – Direction du Renseignement et de la sécurité de la défense (DRSD) I Ministère des Armées et des Anciens combattants – Direction du Renseignement militaire (DRM) I Ministère des Armées et des Anciens combattants – Direction générale de la Sécurité extérieure (DGSE) I Numeum I Olvid I Orange I Pôle d'expertise et de régulation numérique (PEReN) I Portyq I Proton AG I Secrétariat général de la défense et de la sécurité nationale (SGDSN) I Secrétariat général des affaires européennes (SGAE) I Synacktiv I Thales Group