

Sénat : Rapport d'activité 2025 de la Commission nationale de contrôle des techniques de renseignement

Category: 2020-2030,Actualités,Renseignement
12 octobre 2026



SÉNAT

Audition de M. Vincent Mazauric,
Président de la Commission nationale de contrôle des techniques de renseignement (CNCTR)

Mme Muriel Jourda, présidente de la commission des lois. – Monsieur le président Mazauric, nous vous entendons aujourd'hui, en commun avec la commission des affaires étrangères, de la défense et des forces armées, sur le rapport d'activité de la CNCTR pour 2025.

Cette audition revêt, cette année, une dimension particulière. Elle intervient au terme de dix années d'application de la loi du 24 juillet 2015 relative au renseignement, qui a donné un cadre légal complet pour autoriser, encadrer et contrôler les techniques de renseignement.

Comme l'a rappelé Philippe Bas dans le recueil publié pour les dix ans de la CNCTR, le débat parlementaire de 2015 nous avait conduits « au cœur de notre contrat social », puisqu'il s'agissait de concilier deux exigences d'importance égale : la sécurité de nos concitoyens et la préservation des libertés.

Dix ans après, cet équilibre demeure un acquis essentiel. Pour autant, il n'est pas figé. La loi de 2015 a été conçue dans un contexte de menace terroriste élevée et d'essor rapide des usages numériques.

Les conditions concrètes du renseignement ont évolué depuis lors. Le chiffrement des communications s'est fortement développé – jusqu'à devenir la norme –, tandis que les opérateurs et services utilisés se sont multipliés et internationalisés, ce qui modifie profondément les modalités d'accès aux données.

Les menaces qui pèsent sur notre pays se sont intensifiées, qu'il s'agisse des ingérences étrangères et des atteintes à la sécurité de la Nation – avec le retour de la guerre sur le continent européen – ou du narcotrafic qui constitue, pour reprendre les mots du rapport de la commission d'enquête du Sénat, « une menace existentielle pour les institutions et pour la démocratie ».

Les chiffres de l'année 2025 en donnent la mesure. Les demandes de techniques de renseignement présentées au Premier ministre ont franchi le seuil des 100 000. Surtout, la répartition des demandes par type de techniques montre une hausse très marquée des techniques plus intrusives, en particulier celle du recueil de données informatiques (RDI), dont les demandes ont progressé de 38,2 % en 2025, après une hausse déjà importante en 2024.

Cette technique peut notamment consister à « piéger » un téléphone, ce qui est susceptible de donner accès à l'ensemble des données de l'appareil. Le législateur a donc entendu en faire une technique subsidiaire, réservée aux cas où les renseignements recherchés ne peuvent être recueillis par un autre moyen légalement autorisé. Or votre rapport montre que, sous l'effet du chiffrement des communications et de l'usage croissant d'applications comme *WhatsApp* ou *Telegram*, cette technique devient parfois la seule réellement utile pour accéder au renseignement recherché. Dans ces conditions, comment la CNCTR apprécie-t-elle aujourd'hui cette exigence de subsidiarité ? Au regard de la progression de son usage, le cadre légal actuel encadrant cette technique vous paraît-il encore adapté, notamment s'agissant des durées d'exploitation et de conservation des données recueillies ?

Du point de vue du contrôle, comment éviter que la montée en puissance des techniques les plus complexes ne crée un décalage entre les capacités de collecte des services et les capacités effectives de contrôle de la Commission ?

Au-delà des techniques, l'évolution du contexte interroge aussi les finalités au nom desquelles les techniques de renseignement peuvent être autorisées. C'est l'objet de ma seconde question, qui porte sur le séparatisme et l'entrisme.

Ces deux phénomènes ont pris, en 2025, une place plus importante dans le débat public. Ils peuvent prendre des formes diverses, parfois dissimulées, et ne comportent pas nécessairement de dimension violente. Ils visent pour autant, par des voies diffuses, à affaiblir nos principes républicains et à contourner les règles communes. Je ne les crois pas, à certains égards, moins dangereux que le narcotrafic.

Votre rapport rappelle toutefois que le séparatisme et l'entrisme ne constituent pas, en tant que tels, des finalités autorisant le recours aux techniques de renseignement au sens du code de la sécurité intérieure. En particulier, la finalité relative aux atteintes à la forme républicaine des institutions renvoie à des incriminations pénales précises, qui ne recouvrent pas ces stratégies.

Dans ce cadre, comment ces situations sont-elles aujourd'hui appréhendées ? Peuvent-elles, dans certains cas, être rattachées aux finalités déjà prévues par les dispositions du code de la sécurité intérieure ? Face à la nécessité de faire évoluer le droit existant, quelle voie vous semblerait la plus conforme à l'équilibre voulu par le législateur en 2015 ?

M. Cédric Perrin, président de la commission des affaires étrangères. – Monsieur le président Mazauric, l'an dernier, à pareille époque, vous étiez venu devant nos deux commissions présenter le rapport annuel de la CNCTR alors que vous veniez à peine d'être nommé. Je vous remercie donc d'avoir inscrit ce rituel à votre agenda et de nous présenter aujourd'hui votre rapport d'activité 2025.

Après en avoir réservé la primeur à la délégation parlementaire au renseignement (DPR) à l'occasion de sa publication jeudi dernier, il était important que vous puissiez venir présenter vos principaux constats et recommandations sur le contrôle des techniques de renseignement à l'ensemble des parlementaires en charge de la législation relative à la sécurité intérieure et à la sécurité extérieure.

J'avais déjà constaté, lorsque je présidais la DPR en 2023 et 2024, que les questions relatives au renseignement ne pouvaient rester cantonnées aux seuls parlementaires composant cette délégation, dès lors que sont discutées en séance publique des mesures législatives portant sur l'encadrement des techniques de renseignement. On l'a constaté lors des débats sur la proposition de loi visant à sortir la France du piège du narcotrafic.

Le vote du projet de loi actualisant la programmation militaire devrait à cet égard conforter et sécuriser le cadre juridique de l'usage de la technique dite des algorithmes grâce à l'accord obtenu en commission mixte paritaire sur la rédaction du Sénat, que j'ai défendue avec la présidente Muriel Jourda.

Je saisis cette occasion pour saluer sa décision, en qualité de présidente de la DPR, de publier une communication spécifique aux enjeux d'algorithmes et de messageries chiffrées. Ce travail pédagogique inédit met à bas quelques idées reçues : non, il n'y a pas de surveillance généralisée, mais au contraire un encadrement et un contrôle très strict de l'action des services, dont la CNCTR est un acteur essentiel. Cette communication appelle aussi clairement à progresser vers un dispositif permettant d'appliquer le régime des interceptions de sécurité au contenu des messageries cryptées. Il y a là un enjeu de sécurité nationale qui doit conduire à faire comprendre aux plateformes qu'elles doivent se conformer aux exigences de la protection des intérêts fondamentaux de la Nation lorsqu'une surveillance est justifiée, en

matière d'activité de terrorisme, d'ingérence étrangère ou de criminalité organisée.

J'avais jeté un pavé dans la mare lors de l'examen de la proposition de loi visant à sortir la France du piège du narcotrafic. Le dispositif que j'avais présenté n'a pas prospéré au-delà du Sénat, mais je répète qu'il y a urgence à trouver une solution. Votre rapport fait au moins deux constats.

Premièrement, plus de 25 000 personnes étaient surveillées en 2025, un chiffre en progression de 4,2 % par rapport à 2024.

Deuxièmement, l'obstacle des messageries chiffrées ne peut pas être compensé par la technique du recueil de données informatiques, qui est plus intrusive sur le plan des libertés individuelles, plus lourde et plus coûteuse.

Le débat ne peut pas en rester à une confrontation binaire entre ceux qui voudraient accéder à tous les messages cryptés – ce n'est absolument pas mon cas – et ceux qui voudraient interdire tout accès et qui défendent les intérêts commerciaux des plateformes.

C'est pourquoi, monsieur le président Mazauric, nous serions très intéressés par vos constats et vos propositions dans ce domaine pour répondre, comme vous l'écrivez dans votre rapport, à ce « défi pour le renseignement dans un État démocratique ».

Enfin, vous évoquez l'absence d'encadrement des échanges internationaux entre services français et étrangers. Quelles sont vos recommandations dans ce domaine ?

M. Vincent Mazauric, président de la Commission nationale de contrôle des techniques de renseignement. –

Je suis particulièrement sensible au temps que vous consacrez une nouvelle fois aux travaux de notre commission. La CNCTR attache en effet une grande importance à ses relations avec le Parlement.

Nous ne sommes pas une autorité administrative indépendante tout à fait comme les autres. Nos interlocuteurs sont des services publics qui appliquent des politiques publiques et mettent en œuvre la loi. À ce titre, nous concourons, à vos côtés, au contrôle de la bonne application de celle-ci. Le lien avec la délégation parlementaire au renseignement revêt, de ce point de vue, une importance particulière.

Sans revenir en détail sur les principaux chiffres de l'année 2025, il est intéressant de relever que, comme en 2023, la finalité relative à la prévention de la criminalité et de la délinquance organisées arrive en tête lorsque l'on raisonne en nombre de personnes surveillées. Elle représente 30 % des 25 000 personnes suivies au cours de l'année.

Au-delà de notre travail quotidien d'examen des plus de 100 000 demandes sur lesquelles nous rendons un avis avant décision du Premier ministre, nous avons effectué, en 2025, 120 contrôles sur pièces et sur place dans l'ensemble des services. Ce travail est accompli par une équipe modeste composée de 22 personnes, dont 14 sont affectées aux missions de contrôle, et d'un collège de neuf membres, composé de quatre parlementaires et de cinq magistrats et personnalités qualifiées.

Le constat d'ensemble que je peux vous présenter aujourd'hui est sans doute plus positif que celui qui ressortait de notre rapport pour 2024. Nous pouvons confirmer le légalisme des services de renseignement, leur attention et leur écoute, même si l'on peut naturellement relever des nuances, notamment en fonction de la taille des services. Je renvoie, à cet égard, à la seconde des deux études figurant dans notre rapport, qui s'efforce de décrire de manière vivante et franche le déroulement des contrôles, en donnant la parole aux différents acteurs.

L'année 2025 a été marquée par deux progrès techniques importants. Le premier tient à la décision de la direction générale de la sécurité extérieure de permettre à nos équipes d'utiliser l'outil servant à requêter les grandes masses de données exploitées dans le cadre de la surveillance internationale. Sans cet outil, notre capacité de contrôle aurait été très limitée ; grâce à lui, elle atteint désormais un niveau que nous pouvons juger satisfaisant.

Un autre service important a également commencé à organiser avec nous des échanges à distance sur les données obtenues par le RDI. C'est un prélude au dispositif qui, nous l'espérons, sera pleinement opérationnel l'an prochain, à la suite de l'arbitrage rendu par le Président de la République en 2023, permettant d'accéder à distance à cette source importante et sensible de renseignements tout en maintenant le dialogue contradictoire avec le service.

Cette tonalité plus positive ne diminue en rien notre vigilance. La surveillance internationale doit faire l'objet d'un contrôle particulièrement attentif, car la loi lui assigne une limite claire : elle ne doit ni ne peut concerner le territoire national. L'outil est différent de ceux propres à la surveillance domestique, et son usage doit l'être tout autant.

Nous restons également très attentifs à la bonne répartition des investigations entre police administrative et police judiciaire, de telle sorte qu'un service ne demeure pas trop longtemps dans le premier cadre lorsqu'il devrait déjà relever du second.

Deux autres points de vigilance demeurent classiques, mais leur importance n'a pas diminué. Le premier concerne les demandes présentées par les services au titre de la prévention des violences collectives susceptibles de porter gravement atteinte à la paix publique. Nous touchons ici à la frontière de libertés fondamentales telles que les libertés de pensée, d'expression, d'association et de manifestation. Nous constatons une légère décline des demandes présentées à ce titre, qui représentent désormais un peu moins de 10 % des requêtes, contre un peu plus de 10 % l'an dernier ; c'est un signe de mesure.

Le second point concerne la protection que la loi accorde aux personnes exerçant une profession protégée : parlementaires, magistrats, avocats et journalistes.

Plusieurs sujets intéressant directement le législateur ont été évoqués. Après dix années d'application, la loi de 2015 fonctionne encore bien et demeure adaptée aux pratiques technologiques actuelles. Certaines difficultés que l'on pouvait anticiper se sont néanmoins matérialisées, tandis que de nouveaux débats sont apparus.

Le premier concerne le chiffrement. Le président Perrin a rappelé le mouvement pendulaire observé en 2025 sur ce sujet. Le chiffrement n'a pas vocation, par principe, à faire obstacle aux investigations légitimes destinées à protéger les intérêts fondamentaux de la Nation. Il serait absurde, et contraire à l'esprit de la loi, que le seul recours au chiffrement protège des

personnes de toute investigation. Mais, comme le rappelle depuis longtemps la Cour européenne des droits de l'homme, le chiffrement protège aussi tout un chacun, personnes publiques comme privées. Il ne faut donc l'ébranler qu'avec certitude et précaution.

Les deux solutions schématiquement opposées qui ont été débattues en 2025 avaient un point commun : aucune n'avait encore pu s'appuyer sur une expertise technique suffisante pour nourrir une réflexion juridique solide, puis une délibération politique. Si l'on peut parler, à ce stade, d'un match nul, la partie n'est certainement pas terminée.

La CNCTR n'a pas les compétences d'expertise technique particulières sur ce sujet, elle n'est que le contrôleur du comportement des services en rapport avec l'application de la loi. Je pense donc plus particulièrement à la mission confiée par le Premier ministre au président de la commission des lois de l'Assemblée nationale, M. Boudié, qui doit rendre prochainement ses conclusions sur la voie technique éventuellement possible et, le cas échéant, sur la délibération parlementaire qui pourrait s'ensuivre.

Si l'on met en balance la question du chiffrement et celle, soulevée par la présidente Jourda, du recueil de données informatiques, mieux vaut un bon déchiffrement, convenablement encadré et protecteur de tous ceux qui n'ont rien à craindre et qui sont en droit de voir leur vie privée respectée. Un déchiffrement maîtrisé vaut mieux qu'un recours sans cesse croissant au RDI.

La croissance de cette technique est en effet notable : 38 % en 2025, après 27 % en 2024. Elle ne fonctionne pas systématiquement et diffère à ce titre de l'écoute téléphonique classique. Mais lorsqu'elle fonctionne, elle peut aspirer des quantités très importantes de données. La Commission appelle donc à une réflexion collective sur le meilleur usage, et le plus prudent, de cette technique. C'est un travail que nous menons au quotidien avec les services.

Cette technique, qui figure parmi les plus intrusives, doit respecter non seulement les principes de nécessité et de proportionnalité, mais aussi le principe de subsidiarité. Un service ne peut souhaiter y recourir que s'il est en mesure d'établir qu'aucune autre technique ne lui apportera le renseignement nécessaire.

On peut craindre que le principe de subsidiarité appliqué à cette technique soit devenu assez théorique tant est haut l'obstacle du chiffrement. Mais on peut aussi considérer qu'il est respecté, car l'on constate fréquemment – hélas ! – que le chiffrement n'a pas permis d'accéder aux données recherchées.

La durée légale de conservation des données recueillies par cette technique est de 120 jours. D'autres durées sont beaucoup plus longues : les données de connexion peuvent, notamment en matière de surveillance internationale, être conservées jusqu'à six ans. La durée de conservation, qui se situe tout en aval de la chaîne de mise en oeuvre du RDI, ne me paraît pas être la question la plus urgente à traiter, à condition que les services puissent nous exposer clairement les conditions techniques d'exploitation des données recueillies.

Tous les services ne disposent pas des mêmes compétences. Les services dits du premier cercle prêtent souvent main-forte à ceux du second, pour la collecte comme pour l'exploitation. Le groupement interministériel de contrôle contribue également à une meilleure exploitation des données au profit des services du second cercle.

Nous souhaiterions voir progresser un meilleur discernement dans les données collectées, afin d'apprécier plus rapidement leur lien avec les besoins de l'enquête. Ce serait aussi un soulagement quantitatif pour les services chargés de les traiter. Tout ce qui est capté n'est pas indispensable ni nécessairement relié à l'enquête. Il est possible, par exemple, de collecter un très grand nombre de photographies sur plusieurs années, alors que l'intérêt de l'investigation porte d'abord sur les messages échangés par une personne.

La question de la durée de conservation doit donc être replacée dans un ensemble plus large : celui d'une meilleure maîtrise, par les services, du traitement de cette technique. J'espère également que le projet que j'ai évoqué, qui permettra un accès à distance pour le contrôleur que nous sommes, y aidera.

Vous avez aussi, madame Jourda, mentionné la question, extrêmement délicate, du séparatisme et de l'entrisme. En 2025, les services, sur instruction du Gouvernement, s'en sont saisis. Un constat partagé s'est établi entre le ministère de l'intérieur et la commission chargée du contrôle : dans son cadre juridique actuel, la finalité relative à la protection de la forme républicaine des institutions ne permet pas d'enquêter sur ces phénomènes dans toutes les circonstances.

Des progrès sont possibles, y compris par voie réglementaire ; il ne faut pas les négliger. La direction nationale du renseignement territorial, désignée par le Gouvernement comme service pivot des investigations en la matière – son savoir-faire et son implantation le justifient – ne peut pas mobiliser toute la gamme des finalités prévues par la loi. Elle ne peut notamment pas invoquer celles qui concernent la protection contre l'ingérence étrangère, à la différence des services du premier cercle, comme la direction générale de la sécurité intérieure. Or certains phénomènes de séparatisme ou d'entrisme peuvent être liés à de telles influences ou ingérences étrangères.

Le débat peut aussi se situer au niveau législatif. Votre commission des lois, en examinant une proposition de loi sur ce sujet, a fait preuve d'une sage prudence. La CNCTR n'est pas le législateur et n'a pas à avoir d'avis propre ; elle est chargée d'aider les services à comprendre un cadre juridique et à le faire respecter.

Je me permettrai simplement de rappeler un élément de ce cadre : la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales admet que les politiques publiques de renseignement puissent porter atteinte à la vie privée, à condition que cette atteinte soit nécessaire dans une société démocratique. C'est à cette aune qu'il appartiendra au législateur de se prononcer.

Le président Perrin a cité un autre sujet, que je suis presque désolé d'évoquer de nouveau tant il a l'âge de la commission et de la loi : l'absence regrettable de tout encadrement juridique des échanges d'informations, au demeurant légitimes, entre les services de renseignement français et leurs partenaires étrangers.

Ces échanges existent, et les directeurs de service ont raison d'en souligner la nécessité. Mais le fait qu'aucun encadrement n'existe n'est pas normal. Ce n'est en outre ni conforme à la jurisprudence de la Cour européenne des droits de l'homme ni comparable au cadre juridique de nos partenaires les plus proches.

Notre rapport contient une proposition d'encadrement mesurée. Il ne s'agit pas d'empêcher les échanges, mais de rappeler des principes simples de réciprocité et de parité, comme il en existe dans d'autres domaines de coopération internationale, en particulier pénale ou fiscale. Il s'agit de ne pouvoir recevoir d'un partenaire étranger que ce que notre propre loi permettrait de collecter. Ces principes n'entraveraient pas l'action des services ; ils accompagneraient la conduite d'une politique publique.

Nous comptons, en 2026 et en 2027, renforcer encore notre lien de confiance avec les services. La confiance, selon la sagesse populaire, n'exclut pas le contrôle. Notre travail est d'apporter une garantie, mais notre mission, telle que nous la concevons, consiste aussi à porter cette garantie devant vous et à obtenir des services qu'ils y concourent.

Le contrôle que nous exerçons n'aurait pas de sens si les services ne s'imposaient pas à eux-mêmes leur propre discipline. Nous y veillons et resterons, en 2026 comme en 2027, équitables et mobilisés.

Mme Michelle Gréaume. – La loi du 24 juillet 2015 relative au renseignement doit-elle être révisée afin de mieux encadrer l'usage de l'intelligence artificielle dans le traitement des données collectées ?

M. Vincent Mazauric. – Je ne veux pas manquer de prudence, mais il me semble qu'une telle révision ne s'impose pas aujourd'hui, car l'usage de l'intelligence artificielle n'est pas considérablement répandu, du moins tel que nous pouvons l'apprécier avec la distance du contrôleur, qui ne voit pas tout, tout le temps.

L'intervention de la loi deviendrait nécessaire si nous constatons une perte de contrôle. Nous rappelons d'ailleurs dans notre rapport d'activité de 2024, en nous appuyant sur une étude du Conseil d'État, combien le principe du maintien d'un contrôle humain de la décision doit être préservé en toutes circonstances.

Si la décision de mettre en oeuvre une technique de renseignement devait dépendre de l'intelligence artificielle, il faudrait légiférer sans délai. Tel n'est pas le cas aujourd'hui. L'intelligence artificielle est utilisée comme une modalité de traitement de la donnée. Dans la mesure de nos moyens, nous demeurons attentifs à l'évolution de ces usages.

Mme Sophie Briante Guillemont. – Pourriez-vous revenir sur la question des fichiers dits de souveraineté ?

M. Vincent Mazauric. – Le rapport évoque de nouveau ce sujet. Je ne suis pas certain de pouvoir décrire sans erreur ce qu'est un fichier de souveraineté, tant l'expression est employée par les services pour désigner un compartiment de données qu'ils estiment extérieur au cadre légal de 2015 et, par conséquent, soustrait aux investigations de la Commission.

Juridiquement, certains fichiers relèvent du contrôle de la Commission nationale de l'informatique et des libertés (Cnil) et non de celui de la CNCTR, et c'est très bien ainsi. Ce que la Commission constate et signale d'année en année, avec peut-être davantage d'insistance dans son rapport 2025, c'est qu'une forme de nominalisme conduit parfois un service à qualifier ainsi un ensemble de données. Or le contrôleur qu'est la CNCTR ne peut pas franchir une porte qui affiche cette étiquette.

La CNCTR ne souhaite pas, ne peut pas et ne doit pas exercer des contrôles qui ne relèvent pas d'elle. Nous souhaitons seulement être assurés que ces fichiers dits de souveraineté ne contiennent pas de données collectées en application du livre VIII du code de la sécurité intérieure, que nous devons continuer à observer afin de vérifier, comme partout ailleurs, que les délais de conservation ont été respectés et que, si des données ont été « capitalisées » – pour employer le vocabulaire des services –, c'est parce qu'elles étaient, selon les termes de la loi, « indispensables à l'enquête ».

Pour le dire de manière imagée, nous ne souhaitons pas forcer cette porte, mais nous ne pouvons pas davantage nous contenter de l'étiquette qui y est apposée. Ce sujet, déjà soulevé à plusieurs reprises, justifierait un examen juridique serein, conduit tranquillement avec les différents acteurs. De quoi parle-t-on exactement ? Que faut-il vérifier ? Qu'est-ce qui doit demeurer en dehors du contrôle de la CNCTR ?

M. Olivier Cadic. – En tant qu'auteur de l'article 16 *bis* du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité – je précise que cet article vise à interdire les portes dérobées dans les messageries chiffrées –, je suis heureux de pouvoir enfin parler publiquement de ce sujet qui touche directement aux libertés publiques. Jusqu'à présent, j'ai rencontré la DGSI, le ministre de l'intérieur et plusieurs personnalités au plus haut niveau de l'État, mais le débat n'a pas vraiment pu être conduit de manière ouverte.

Non, monsieur le président Perrin, mon intention n'est pas de défendre des intérêts commerciaux privés, juste les libertés publiques.

Installer une porte dérobée dans les messageries cryptées, les États-Unis l'ont déjà fait, et l'expérience s'est retournée contre eux. Mais il y aura toujours des apprentis sorciers persuadés d'être plus malins que les autres.

L'objectif du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité était de renforcer la protection cyber de notre pays. Si j'ai voulu ajouter un article 16 *bis* à ce texte, c'est parce que je ne pouvais accepter l'article 8 *ter* de la loi visant à sortir la France du piège du narcotrafic.

Le Sénat a adopté l'article 16 *bis*. En commission, l'Assemblée nationale a conforté, et même développé cette disposition, mais le Gouvernement bloque désormais l'inscription de ce projet de loi à l'ordre du jour de l'Assemblée nationale, et donc son adoption définitive par le Parlement. À aucun moment le Gouvernement n'a proposé une rédaction alternative de cet article. Il s'est contenté de bloquer l'ensemble du projet de loi, avec les conséquences dramatiques que nous constatons aujourd'hui : des vols de données à grande échelle sans aucune sanction. Qui protège aujourd'hui le pays ? Le ministre de l'intérieur m'a lui-même indiqué que, techniquement, on ne savait pas faire.

Ma première question est donc simple : comment entendez-vous procéder techniquement ?

Ma seconde question porte sur la souveraineté. Il existe une messagerie chiffrée française, Olvid. Si l'on devait comparer les niveaux de sécurité, sur une échelle de 0 à 10, WhatsApp serait à 2, Signal à 3 et Olvid à 8. Simplement, Olvid est payante. Nous préférons donc utiliser des messageries gratuites américaines plutôt qu'une messagerie française offrant un très haut niveau de sécurité. C'est la réalité de nos pratiques, y compris au Parlement.

Face au blocage actuel, j'ai organisé au Sénat une réunion avec les plus grands spécialistes mondiaux du chiffrement, y compris français. Ils m'ont indiqué ne pas avoir eu d'échanges avec la CNCTR au sujet des techniques de chiffrement. Je ne détaillerai pas ici tous les modes de contournement qui seraient mis en place si l'on suivait la voie que vous évoquez. Mais avez-vous échangé avec les entreprises qui travaillent sur le chiffrement afin d'analyser les impacts techniques ? Lorsque je les ai rencontrées, elles m'ont indiqué que cela n'avait pas été fait.

Comment imaginez-vous les mettre en place ? La question n'est évidemment pas de protéger le narcotrafic, le terrorisme ou la pédocriminalité. Mais il existe d'autres techniques pour obtenir les informations recherchées, maîtrisées par de nombreux acteurs et États. Les avez-vous toutes évaluées ?

M. Vincent Mazauric. – Cette occasion est en effet propice à un débat, même si je ne suis que le président du collège d'une autorité de contrôle. Je ne suis ni le Gouvernement ni le coordonnateur national du renseignement et de la lutte contre le terrorisme. Je n'ai donc pas de réponse directe à la question, de bon sens, de savoir si des échanges ont eu lieu avec les sociétés spécialisées dans le chiffrement et quelles conclusions en ont été tirées. Ce n'est pas le rôle de la CNCTR.

En revanche, dans notre rôle juridique de gardien du comportement des services au regard de la loi, nous constatons que la subsidiarité n'est plus tout à fait ce qu'elle était en matière de recueil de données informatiques.

Le chiffrement ne peut pas, en lui-même, suffire à mettre certaines personnes à l'abri d'investigations indispensables à la protection des intérêts fondamentaux de la Nation. Or, le droit actuel est, de ce point de vue, assez faible. Le code de la sécurité intérieure permet de demander à un prestataire de messagerie chiffrée l'accès au contenu en clair de certaines conversations, mais il lui offre aussitôt la possibilité de se prévaloir d'une impossibilité technique. Si vous interrogez le groupement interministériel de contrôle, il pourra peut-être vous indiquer que le résultat n'est pas toujours nul ; certaines réponses peuvent parfois être obtenues. Mais le texte actuel n'est sans doute pas pleinement adapté.

La Commission observe les pratiques des services, l'usage qu'ils font des techniques et leur manière d'appliquer la loi. Elle constate, modestement mais clairement, que ni l'article 8 *ter* de la loi visant à sortir la France du piège du narcotrafic ni l'article 16 *bis* du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité n'apportent aujourd'hui de solution satisfaisante, dans la mesure où ils sont diamétralement opposés. Mais il n'appartient pas à la CNCTR de proposer une solution.

Juridiquement, une voie peut être trouvée, puisque le principe n'a pas été écarté par la Cour européenne des droits de l'homme. Il serait donc probablement excessif d'interdire complètement l'accès au contenu en clair des communications chiffrées, mais il faut l'entourer de garanties solides. Or ces garanties ne peuvent résulter que d'une expertise technique sérieuse. C'est, je l'espère, ce que pourra réaliser la mission confiée au président Boudié.

M. Cédric Perrin, président de la commission des affaires étrangères. – Je souhaite répondre à Olivier Cadic, afin d'éviter toute mauvaise interprétation de mes propos. Je ne visais personne en particulier.

Cette année, sous la présidence de Muriel Jourda, la délégation parlementaire au

renseignement a choisi de recueillir davantage d'informations techniques et juridiques auprès des différents opérateurs. En effet, lors du dépôt de l'amendement portant sur l'article 8 *ter* de la proposition de loi visant à sortir la France du piège du narcotrafic, nous avons constaté une grande incompréhension sur le sujet. Il n'a jamais été question de créer des portes dérobées ; l'objectif était de rechercher la possibilité d'intégrer, dans certaines applications, un outil permettant un contrôle *a priori*, avant chiffrement.

Nous savons que cette question est extrêmement complexe et que ses conséquences peuvent être dangereuses. C'est précisément pourquoi la présidente de la DPR a souhaité que nous consacrons l'année 2026 à ce travail, afin de mieux apprécier les moyens qui pourraient être mobilisés et les résultats que l'on peut raisonnablement en attendre.

Je rejoins ce qui a été dit : le rôle de la CNCTR n'est pas de mettre en oeuvre les techniques de renseignement, mais de les contrôler. Je comprends donc parfaitement que le président Mazauric ne puisse pas répondre à toutes les questions. Certaines techniques existent, mais elles supposent, me semble-t-il, une captation physique, ce qui rend leur emploi particulièrement complexe.

Nous devons trouver un équilibre entre la protection des libertés publiques et la nécessité de disposer de techniques adaptées à l'évolution constante des technologies. Les plateformes progressent sans cesse et permettent aujourd'hui à des criminels de s'abriter derrière le chiffrement. La société doit pouvoir se protéger contre ces moyens de contournement devenus considérables.

Il n'y a pas de raison d'être plus vertueux avec les messageries privées que nous ne le sommes avec les SMS ou les courriels, qui font l'objet de contrôles parfaitement maîtrisés sans que cela soulève de difficulté particulière. Il faut donc trouver un équilibre.

Je reconnais que l'amendement que nous avons déposé sur l'article 8 *ter* de la proposition de loi visant à sortir la France du piège du narcotrafic présentait un trou dans la raquette. Je ne l'ai jamais nié. Mais il était aussi important de déposer cet amendement pour lancer le débat et tenter de trouver des solutions.

Je reste persuadé que nous ne pouvons pas continuer à laisser des criminels – qu'ils relèvent de la criminalité organisée, du narcotrafic ou d'autres formes de délinquance – s'abriter derrière le chiffrement. Encore une fois, aucun sénateur n'est visé, pas plus Olivier Cadic qu'un autre.

Les auditions que nous avons conduites dans le cadre de la DPR avec les opérateurs de messageries nous ont aussi montré que le chiffrement total constitue pour eux un argument commercial majeur. Il sert à promouvoir leurs produits. Une forte pression est donc exercée par le lobby du numérique ; nous l'avons vu s'agiter lors du dépôt de l'amendement à l'article 8 *ter*, et j'en ai été le témoin direct.

Mme Muriel Jourda, présidente de la commission des lois. – Nous vous remercions, monsieur Mazauric.

[Site du Sénat](#)

Mercredi 01 juillet 2026