ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Mercredi 9 juillet 2025
Séance de 14 heures

Compte rendu n° 13

SESSION EXTRAORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 14 heures 05.

Présidence de M. Philippe Latombe, président.

La commission spéciale a procédé à l'audition, ouverte à la presse, de M. Mahamadou Diarra, secrétaire général de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) ; M. Pascal Chauve, directeur du groupement interministériel de contrôle (GIC) ; et Mme Céline Berthon, directrice générale de la sécurité intérieure (DGSI).

M. le président Philippe Latombe. Dans le cadre de nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, nous allons traiter du chiffrement, sujet particulièrement important que nous n'avions pas encore abordé et sur lequel nous souhaitions avoir l'éclairage de la communauté du renseignement. Cette audition et la suivante seront entièrement consacrées à l'examen de l'article 16 *bis* du projet de loi, de ses implications concrètes et de son insertion dans le corpus législatif.

Disons-le d'emblée, si la question du chiffrement est importante, il n'était pas évident qu'elle trouve sa place dans le débat sur ce projet de loi au regard des dispositions de l'article 45 de la Constitution et du contrôle qu'en effectue le Conseil constitutionnel. Mais le Sénat ayant adopté un amendement d'Olivier Cadic, président de la commission spéciale, cet article 16 *bis* est désormais dans la navette parlementaire et il nous revient de l'examiner avec toute l'attention qu'il mérite.

La question du chiffrement avait fait l'objet de débats animés lors de l'examen de la loi du 13 juin 2025 visant à sortir la France du piège du narcotrafic. Dans sa formulation actuelle, l'article 16 *bis* dispose : « 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 des clés de déchiffrement maîtresses ou tout autre mécanisme permettant un accès non consenti aux données protégées. »

M. Mahamadou Diarra, secrétaire général de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT). Vous souhaitez disposer de l'éclairage de la communauté du renseignement sur cet article 16 *bis*. Dans le propos introductif dont j'ai été chargé, je vais vous présenter l'avis technique des services. Nous serons ensuite à votre disposition pour répondre à vos questions, sous réserve du respect du secret de la défense nationale. Nous pourrons entrer davantage dans les détails lors de la partie de l'audition qui se déroulera à huis clos, même si nous devons respecter les obligations qui s'imposent à nous.

Sur le fond, nous considérons que l'article 16 *bis* n'a pas sa place dans le projet de loi. Les services de renseignement sont confrontés au quotidien aux enjeux du chiffrement, évolution majeure de nos moyens de communication, qu'ils soient interpersonnels ou entre machines. Le chiffrement permet de sécuriser nos transactions bancaires, nos investigations sur internet, nos échanges de messages ou nos appels. C'est un élément essentiel de la politique française de cybersécurité, édicté dans la posture nationale sur le chiffrement. La

mission des services de renseignements est de protéger la propriété intellectuelle de nos industries et de sécuriser les communications des autorités de l'État. Pour le dire simplement, le chiffrement concourt en tant que moyen technique à la sécurité des systèmes d'information de la nation.

Dans leur travail quotidien, les services de renseignements constatent que certains moyens, notamment les messageries chiffrées, sont utilisés par des personnes mal intentionnées. Il ne s'agit pas ici de pointer du doigt les opérateurs de messageries chiffrées qui ne sont que des outils, mais de rappeler que certains usages ayant des impacts sur la sécurité nationale se développent à l'aide de ces outils. Nous ne sommes pas les seuls à faire ce constat. Il me semble que Johanna Brousse, cheffe de la section de lutte contre la cybercriminalité du parquet de Paris, et le général Christophe Husson, chef du commandement du ministère de l'intérieur dans le cyberespace, ont pu vous le rappeler pour ce qui concerne le judiciaire.

Dans tous les pays européens, cette évolution préoccupante fait l'objet d'un constat partagé. En avril 2024, les chefs de police européenne ont alerté *via* Europol sur les risques associés au fait de voir se développer des espaces de non-droit sur les plateformes numériques grâce au chiffrement et ils ont appelé les industriels du numérique à trouver le juste équilibre entre vie privée et sécurité publique. Un rapport de juin 2024, corédigé par Europol et Eurojust, dresse un état des lieux technico-opérationnel factuel de l'impact du chiffrement au-delà des seules communications chiffrées. Ultime exemple, le groupe d'experts de haut niveau HLEG a rendu un rapport mettant en relief trois nécessités : préservation des bénéfices du chiffrement pour nos sociétés ; transparence des entreprises du numérique en matière de données collectées ; coopération entre les États et les opérateurs pour mettre en œuvre des systèmes d'accès légal à leurs données, encadrés strictement par la loi et contrôlés.

La complexité du sujet – bénéfice du chiffrement et enjeux associés – implique de développer une approche nuancée, fondée sur un principe de proportionnalité. Rappelons le cadre d'action des services de la communauté du renseignement qui regroupe 20 000 agents au sein de dix services relevant de quatre ministères – intérieur, armées, justice, économie et finances. Consacrée par la loi du 24 juillet 2015, la politique publique de renseignement est fondée sur la défense et la promotion de sept intérêts fondamentaux de la nation, définis à l'article L. 811-3 du code de la sécurité intérieure, notamment la prévention du terrorisme et la prévention de la criminalité et de la délinquance organisées – ce sont les 4° et 6° dudit article.

Bénéficiant d'outils d'enquête importants dont nous sommes conscients, les techniques de recueil du renseignement (TRR), les services de renseignement font l'objet de mécanismes de contrôle stricts définis par le législateur, afin de s'assurer que ces outils sont utilisés dans le cadre défini par la loi et de manière proportionnée. La loi a ainsi institué la Commission nationale de contrôle des techniques de renseignement (CNCTR), composée de magistrats de l'ordre judiciaire et de l'ordre administratif ainsi que de parlementaires. Elle est systématiquement saisie pour avis par le premier ministre de chaque demande de techniques de renseignement et elle effectue un contrôle *a posteriori* sur pièces et sur place. Elle élabore chaque année un rapport public dont la dernière édition a été diffusée le 25 juin dernier. La délégation parlementaire au renseignement (DPR) est composée de quatre députés et quatre sénateurs habilités qui exercent la mission de contrôle parlementaire de la politique publique du renseignement. Son dernier rapport public date du 30 avril dernier.

Les services de renseignement doivent adapter leurs moyens d'action aux évolutions technologiques, comme il a fallu le faire par le passé avec l'apparition de la poste, du télégraphe ou des réseaux téléphoniques. Le principe de proportionnalité est au cœur du dispositif légal en vigueur à travers l'article L. 801-1 du code de la sécurité intérieure : « Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité. »

Selon notre analyse, cet équilibre fondamental serait ébranlé par l'article 16 *bis* du projet de loi qui pourrait avoir des effets de bord au-delà de la seule consécration du chiffrement. Nous en concluons qu'il convient de laisser sa place au travail technique approfondi et exhaustif, qui prend du temps au regard de la technicité du sujet, afin d'englober les problématiques très différentes et de restituer au gouvernement et au législateur un ensemble factuel leur permettant d'évaluer en toute connaissance de cause l'opportunité d'une évolution du dispositif légal. C'est ce qui occupe actuellement l'administration et singulièrement la communauté du renseignement. Étant donné la nature des droits en cause, aucune évolution ne se fera sans revenir devant le Parlement, ce qui garantit votre rôle majeur, votre office, dans toute éventuelle décision en la matière.

En résumé, les dispositions de l'article 16 *bis* nous interdiraient de réfléchir aux différentes options sur un sujet aussi central. *A contrario*, laisser à l'administration le temps de travailler permet de documenter plusieurs options. L'une d'elles consiste à apporter des réponses aux enjeux de sécurité posés par le chiffrement si et seulement si un équilibre et des garanties sont trouvées en termes de secret des correspondances et de sécurité des systèmes d'information. Autre option : ne pas donner accès aux communications chiffrées, mais prendre ces décisions en conscience sur la base d'un travail étoffé sur les plans juridique, technique et opérationnel, qui est en cours.

Laisser à l'administration le temps d'approfondir ses travaux permet d'éviter de prendre des initiatives à l'emporte-pièce, sous le coup de l'émotion, dans un sens ou un autre, ce qui est probablement le plus important. Il me semble que Nicolas Roche, secrétaire général de la défense nationale et de la sécurité nationale (SGDSN), a adopté cette même position lorsque vous l'avez auditionné, il y a quelques semaines.

M. Éric Bothorel, rapporteur général. Avant toute chose, je voulais remercier les hommes et les femmes des services qui concourent à la sécurité de nos concitoyens.

Vous avez donné votre opinion sur l'article 16 *bis*, mais nous ne manquerons pas de revenir sur le sujet car la porte est ouverte à des évaluations techniques permettant de concilier liberté et sécurité.

Comment adapter la sécurité informatique de la société aux vulnérabilités des appareils personnels ? De telles mesures pourraient-elles être introduites dans la loi ?

Comme la direction générale de la sécurité intérieure (DGSI) le souligne de temps à autre, le facteur humain est le principal vecteur de compromission des systèmes d'information, notamment au travers de la mauvaise utilisation d'une messagerie professionnelle. Comment remédier à ces cas de figure ?

En quoi consiste la réalisation d'investigations en sources ouvertes du premier niveau sur internet et les réseaux sociaux et dans le cadre de dossiers opérationnels d'évaluation de la menace par la DGSI ? Nous nous écartons là du chiffrement, mais nous nous intéressons aussi au renseignement d'origine sources ouvertes (Osint). Actuellement, la récupération de données volées constitue un recel en droit pénal. Ayant été attentifs à l'audition de Johanna Brousse et de Christophe Husson, vous n'ignorez pas que c'est un sujet qui nous préoccupe. Êtes-vous favorables à l'idée de permettre une telle récupération pour un motif légitime ? Comment concilier à la fois le droit pénal, le droit de propriété intellectuelle, la protection des données à caractère personnel et la cybersécurité en ce qui concerne l'Osint ? Plus largement, quelle est votre opinion sur le recours à l'Osint pour améliorer la cybersécurité ?

Mme Céline Berthon, directrice générale de la sécurité intérieure (DGSI). Nombre de questions dépassent le cadre de l'article 16 *bis* et portent sur des modalités d'action ou de recueil de renseignement, que je préfèrerais aborder à huis clos.

Pour le reste, il s'agit de rechercher un équilibre entre la protection des libertés individuelles et collectives et ce qui relève de la sécurité nationale. Nous devons tenir compte des évolutions technologiques et ne pas remettre en cause les règles de sécurité numérique dont nous bénéficions sans réduire à néant l'efficacité des services de renseignement – qui relèvent de mon champ de compétences – et des services d'enquêtes judiciaires.

Depuis des décennies, l'État dispose légalement du droit d'intercepter des communications téléphoniques. Il l'exerce de façon ciblée dans un cadre administratif pour ce qui relève des techniques de renseignement ou dans un cadre judiciaire pour ce qui concerne les interceptions de sécurité. Les interceptions s'effectuent sous le contrôle de la CNCTR dans le cadre administratif et sous l'autorité d'un magistrat dans le cadre judiciaire. Tous les services du monde – de renseignement ou judiciaires – sont cependant confrontés à une réalité : l'usage de plus en plus développé des messageries chiffrées rend cette technique obsolète. En conséquence, nous perdons de la visibilité sur les activités criminelles des cibles, la détermination de leur projet criminel et, ce qui préoccupe le plus la DGSI, la préparation de leurs projets violents.

Pour schématiser la situation avec mes mots, c'est-à-dire selon une approche qui n'est pas nécessairement technique, je dirais que l'objectif auquel nous devons concourir dans le cadre des travaux évoqués, c'est de tenter de voir si nous pouvons étendre les pratiques que nous avons actuellement avec les opérateurs téléphoniques à d'autres opérateurs, les plateformes de messagerie chiffrées. Pourrions-nous agir dans les mêmes conditions d'exigence légale et de contrôle que celles qui existent pour les interceptions téléphoniques ou les écoutes judiciaires, selon le cadre dans lequel on se place ? Ce sont ces travaux qu'il nous faut poursuivre. Les mutations technologiques nous imposent de trouver un nouvel équilibre technique et juridique entre le secret des correspondances et la protection de la sécurité nationale. Si le choix était fait de ne pas retrouver cet équilibre, il faudrait au moins être en mesure de l'assumer, en en mesurant les conséquences techniques, politiques et, pour ce qui me concerne, opérationnelles.

M. Pascal Chauve, directeur du groupement interministériel de contrôle (GIC). En effet, tout est question d'équilibre en cette matière. Nous l'avons trouvé avec les opérateurs de communication électronique, entre nécessité d'un accès et garantie de la protection de la confidentialité et de l'intégrité des communications. L'Agence nationale de la sécurité des systèmes d'information (Anssi) joue un rôle éminent à l'articulation entre ces deux mondes, l'article 226-3 du code pénal faisant la mesure entre les deux impératifs.

Tout est une question d'équilibre car les techniques de renseignement sont décidées par le premier ministre à la suite d'un examen de leur proportionnalité – l'atteinte au secret et à la vie privée versus l'impératif de sécurité nationale. Cet équilibre, que nous avons trouvé avec les opérateurs de communications électroniques, nous le cherchons encore avec les opérateurs d'extrémité ou lesdites plateformes.

Comment tout cela fonctionne-t-il ? Le GIC – et lui seul – adresse des réquisitions aux opérateurs de communications électroniques en application d'autorisations d'interception de sécurité prises par le premier ministre sur la base d'identifiants, c'est-à-dire des numéros de téléphone, des adresses IP ou n'importe quel sélecteur en fonction de l'autorisation délivrée et de l'utilisation qu'en fait la personne désignée dans l'autorisation. Les opérateurs de communications électroniques sont coopératifs avec les pouvoirs publics. Je profite d'ailleurs de l'occasion pour saluer les directions des obligations légales des opérateurs. Leurs agents sont soumis à des enquêtes de sécurité ; ils travaillent entourés de murs épais ; ils se rendent disponibles vingt-quatre heures sur vingt-quatre pour répondre aux réquisitions du GIC. Je les en remercie.

La suite, vous la connaissez : les opérateurs de communications électroniques se contentent désormais de transporter des flux qui leur sont impénétrables, car chiffrés de bout en bout. Ils dupliquent vers le GIC des communications chiffrées dont le chiffrement leur échappe puisqu'il est à la main des opérateurs d'extrémité ou des plateformes. Depuis les révélations d'Edward Snowden en 2013, le chiffrement s'est en effet généralisé. Il est activé par défaut. Nos logiciels nous alertent d'ailleurs par des pop-ups assez angoissants lorsqu'il n'est pas actif. Ce chiffrement des communications s'est traduit par une bascule économique majeure : les opérateurs de réseaux se sont trouvés privés de la valeur marchande que constituent nos données au profit des opérateurs d'extrémité qui les détiennent et qui en font un commerce lucratif.

Ces derniers connaissent, ou ont toute latitude pour connaître, notre vie privée et professionnelle – nous leur confions les deux. En revanche, les services de renseignement sont privés de leur outil de travail de base. Le législateur avait prévu en 2015, de façon encadrée, un recueil de données informatiques grâce auquel les services peuvent légalement récupérer le contenu des terminaux électroniques, là où les données sont en clair, conformément à l'article L. 853-2 du code de la sécurité intérieure. Or cette récupération est coûteuse et difficilement généralisable. C'est pourquoi la coopération des opérateurs de réseaux ou de transport ne suffit pas : il nous faut absolument celle des opérateurs d'extrémité, dits OTT, *over the top*, ou plateformes.

La coopération avec les opérateurs de réseaux fait l'objet de standards techniques. Elle est encadrée par l'article 226-3 du code pénal, et l'administration s'est organisée pour que tout fonctionne, au bénéfice des enquêtes judiciaires comme du renseignement. Les opérateurs sont dédommagés des surcoûts liés à leurs obligations, en application d'arrêtés tarifaires.

La coopération entre les pouvoirs publics et les plateformes existe, mais elle ne repose pas encore sur des standards techniques. Il n'y a d'ailleurs aucune offre industrielle d'interface normalisée pour accéder aux données des plateformes. Les textes d'application de l'article 226-3 du code pénal se concentrent sur les réseaux de transport. Si l'État s'est organisé pour ce qui est de la coopération avec les opérateurs de réseaux, il ne l'a pas encore fait de manière formelle s'agissant des plateformes, pour donner corps à la coopération. C'est un défi absolument considérable. Nous en sommes, pour l'instant, à examiner de grandes

orientations, qu'il faudra ensuite confronter à la réalité de chaque service de communication de chaque plateforme. Nous pourrons ensuite trouver avec ces acteurs un intérêt commun à élaborer et adopter des standards. Tout cela nécessite un travail posé et approfondi, comme l'a indiqué Nicolas Roche devant votre commission. À ce stade, nous ne sommes pas en mesure de décrire une solution. De toute façon, il n'en existera pas qu'une : le *one size fits all* (taille unique) ne vaut pas dans ce domaine.

L'essor des technologies de communication nous facilite la vie, mais il facilite aussi grandement le crime, les violences collectives, l'espionnage et le terrorisme. L'article 16 *bis* du projet de loi a certes pour but d'affirmer le principe absolument fondamental de la protection de la vie privée, mais cela dans le cadre d'une loi technique, portant sur un mécanisme particulier, le chiffrement, et en exigeant de lui une propriété qui n'est pas indispensable à la protection de la vie privée. Ce texte érige, en fait, le chiffrement en totem, ce qui tuera dans l'œuf toute discussion avec les plateformes, alors que celle-ci est nécessaire pour préserver des capacités d'enquête essentielles, dans un domaine où prévaut la recherche d'une solution équilibrée, de proportionnalité entre atteinte à la vie privée et sécurité nationale. En transcrivant sans nuance dans la loi une position à la fois technique et radicale, on briserait un équilibre savamment entretenu par la Constitution, le législateur, jusqu'à présent, et l'autorité indépendante qu'est la CNCTR, au quotidien. C'est pour ces raisons que le gouvernement vous a demandé de supprimer l'article 16 *bis* et de lui laisser le temps de travailler sereinement, avec les plateformes, à des solutions équilibrées.

Que se passerait-il si la loi sanctifiait le chiffrement ? D'une part, cela reviendrait à annoncer aux criminels que les outils de communication de M. Tout-le-monde leur permettent de préparer en toute impunité leurs actes. Le seul moyen qu'il nous resterait pour pénétrer les communications des criminels serait de pénétrer leurs moyens de communication, conformément à l'article L. 853-2 du code de la sécurité intérieure, ce qui irait à l'encontre des intentions des auteurs de l'article 16 *bis* du projet de loi, puisque cela nous donnerait accès à plus de données que ce qui nous serait nécessaire. En prenant le contrôle d'un smartphone, on n'accède pas seulement aux communications, c'est-à-dire au flux, mais aussi aux fichiers enregistrés, c'est-à-dire au stock, ainsi qu'aux brouillons, aux contacts, à l'appareil photo, au microphone, etc. Il en résultera donc automatiquement un effet pervers. Des techniques plus intrusives, que la loi réserve à des cas subsidiaires, lorsqu'aucun autre moyen n'est disponible, seront parfaitement justifiables sur le plan légal puisqu'il n'existera aucun autre moyen d'accéder aux communications. Par conséquent, au motif qu'on ne pourra pas accéder aux communications, on accédera potentiellement à bien plus.

D'autre part, la sanctuarisation du chiffrement augmentant la demande d'accès aux données en clair, une offre va se créer. Un autre équilibre prévaudra donc, celui de l'offre et de la demande. Nous verrons alors proliférer un secteur commercial lucratif, constitué de sociétés privées offrant des prestations ou des logiciels d'intrusion à des services de police judiciaire ou administrative. L'article 16 *bis* créera un business de la vulnérabilité et du hacking, dont nous devinons qu'il sera dominé par des acteurs dont nous ne voulons pas.

L'article 16 *bis* porte sur des moyens techniques, dont la place dans une loi peut être discutée. Il est absolutiste, puisqu'il ferait également tomber « tout autre mécanisme ». Le gouvernement, par la voix de la ministre chargée du numérique, a déjà alerté vos collègues sénateurs sur les effets de bord de cette disposition. L'article s'appliquera de façon indifférenciée aux enquêtes judiciaires et au renseignement et aura pour conséquence le développement d'un marché des vulnérabilités et du hacking, qui fera la part belle à des prestataires étrangers. Il conduira les services à mettre en œuvre des techniques de

renseignement plus intrusives, plus attentatoires à la vie privée. Il percutera, par ailleurs, les réflexions en cours au niveau européen – la Commission s'est saisie du sujet, comme l'a rappelé le secrétaire général de la CNRLT. Cela signifie que l'adoption de cet article conduira la France à s'exclure de la démarche engagée par l'UE. Enfin, il ruinera la coopération entre l'État français et les plateformes, qu'il est susceptible de faire reculer.

Mme Anne Le Hénanff, rapporteure. Je rappelle, tout d'abord, que l'article 16 *bis* n'est pas apparu dans le texte par hasard : c'était une réaction d'un collègue sénateur, Olivier Cadic, à l'introduction surprise d'une disposition autorisant des *backdoors* (portes dérobées) dans la proposition de loi dite narcotrafic.

Vous nous demandez de vous laisser du temps, ce que je comprends totalement. Je n'ai pas, à ce stade, d'opinion sur l'article 16 *bis*, mais il me paraît bon de pouvoir discuter de ces questions dans le cadre du groupe transpartisan lancé par Florent Boudié – j'espère que vous y serez associés. Cela me paraît une bonne perspective temporelle.

Pouvez-vous préciser quelle est la part, parmi toutes les demandes d'accès aux données que vous adressez aux entreprises, de celles concernant la lutte contre la pédocriminalité et la lutte contre le narcotrafic ? Je crois savoir qu'elle est tout à fait négligeable, alors que la lutte contre le narcotrafic et la lutte contre la pédocriminalité étaient les deux arguments principaux pour justifier l'introduction de l'article 8 *ter* dans la proposition de loi « narcotrafic ».

La technique dite du fantôme, qui permet à un utilisateur invisible de participer à une conversation sur une messagerie chiffrée, ne constitue-t-elle, de votre point de vue, ni une vulnérabilité informatique ni un affaiblissement du chiffrement ?

Quid du filtre de détection de contenus spécifiques mis en place par Apple, notamment pour ce qui est des contenus pédopornographiques échangés sur WhatsApp ou Messenger ?

Que répondez-vous à celles et ceux qui estiment que l'introduction d'une vulnérabilité informatique permettant aux services de l'État d'accéder au contenu des messageries chiffrées pourrait être exploitée par des puissances étrangères à des fins de cyberespionnage ?

Comment expliquez-vous que la gendarmerie nationale ait réussi à accéder au contenu des messages échangés entre des criminels sur le réseau chiffré EncroChat ?

Êtes-vous associés, de près ou de loin, aux discussions qui ont lieu au niveau européen dans le cadre de la stratégie de sécurité intérieure ProtectEU ?

M. Pascal Chauve. La pédopornographie ne fait pas partie des finalités légales du renseignement au sens de l'article L. 811-3 du code de la sécurité intérieure. Il n'existe donc pas de demandes reposant spécifiquement sur ce motif. Le dernier rapport annuel de la Commission nationale de contrôle des techniques de renseignement, évoqué par M. Diarra, rend parfaitement compte de ces questions : la prévention de la criminalité organisée représente 16,1 % des finalités poursuivies par les techniques de renseignement en 2024. Je suis incapable de vous dire la part exacte de la lutte contre le narcotrafic, mais il est certain que celui-ci est au cœur de la criminalité organisée, qui entretient des mafias brassant un argent absolument considérable et qui est susceptible de porter atteinte aux intérêts

fondamentaux de la nation. C'est ce que recouvre, en très grande majorité, la sixième finalité de l'article L. 811-3 du code de la sécurité intérieure.

Mme Céline Berthon. En matière de renseignement, les finalités des réquisitions ne sont pas communiquées aux opérateurs. Dire pourquoi on s'intéresse à un numéro de téléphone – contre-terrorisme, contre-espionnage ou contre-ingérence – serait totalement contraire au principe de protection de l'activité de renseignement. Cela rend d'autant plus complexe l'identification précise des éléments en question.

M. Pascal Chauve. Cela protège non seulement l'enquête mais aussi la personne visée.

M. Mahamadou Diarra. Nous avons bien conscience du contexte dans lequel l'article 16 *bis* a été introduit, mais il me semble que l'article de la proposition de loi « narcotrafic » auquel vous avez fait référence n'a pas été adopté. Il constituait l'une des options possibles, avec l'article 16 *bis*.

Quand je demande de laisser du temps pour mener un travail de fond, c'est que les travaux en cours seraient entravés, ou en tout cas mis en difficulté, si cette disposition était adoptée. On aurait, en effet, tranché, de même que si d'autres dispositions étaient adoptées. La position de l'administration et des autorités dans la discussion avec les opérateurs serait extrêmement entravée.

Je confirme que les services de l'État sont impliqués dans les discussions européennes, la Commission s'étant saisie du sujet, notamment sous l'angle judiciaire, compte tenu des compétences qui sont les siennes. Nous participons à ces discussions, mais les travaux sur la doctrine de sécurité européenne, proposée par la Commission, en sont encore à leurs débuts.

La question de l'utilisateur fantôme fait partie du travail en cours sur les techniques qui pourraient permettre, ou non – nous partons du postulat que la discussion est ouverte –, d'avoir accès à des informations sans affaiblir le chiffrement. Il faudra que les administrations continuent d'y travailler pour que le gouvernement et le Parlement puissent, le moment venu, se reposer la question. Je n'ai pas à me prononcer sur des initiatives parlementaires, mais nous sommes prêts à concourir à la réflexion et à revenir devant vous si besoin.

Mme Catherine Hervieu, rapporteure. Je m'intéresse plus particulièrement à la nécessité pour les collectivités territoriales, les services publics et les entreprises de protéger leurs données, spécifiquement celles à caractère personnel, dans le cadre de leurs différentes activités. Pouvez-vous nous donner des éléments sur la manière dont ces acteurs sont accompagnés et conseillés face aux enjeux du chiffrement ?

M. Mahamadou Diarra. Le sujet de la protection fait l'objet d'une mobilisation de l'ensemble des acteurs, singulièrement le SGDSN, à travers l'Anssi. Vous avez parlé des collectivités territoriales, mais on pourrait également évoquer les hôpitaux, qui sont des acteurs sensibles, exposés aux enjeux concernant les données.

Des travaux de sécurité des systèmes d'information sont menés par l'Anssi. Son directeur général, que vous verrez prochainement, me semble-t-il, pourra y revenir. Par ailleurs, mais je m'exprime là sous le contrôle de ma collègue, les services de renseignement, la DGSI comme la DNRT, la direction nationale du renseignement territorial, mènent des

actions de sensibilisation envers les entreprises et les acteurs publics, notamment les collectivités territoriales, au sujet des messageries, sous l'angle de la protection – ne pas se faire piéger, sécuriser ses données, éviter les mésusages des téléphones personnels et professionnels lorsqu'on manie des données sensibles. Tout un écosystème est mobilisé, au sein duquel l'Anssi joue un rôle central, sous l'autorité du SGDSN et avec l'appui de la CNRLT et la mobilisation des services de renseignement sur le territoire national.

Mme Céline Berthon. Je crois qu'il ne faudrait pas prendre le risque de tomber dans une confusion entre, d'une part, ce qui relève de l'enjeu de la sécurité numérique générale, qui concerne la société dans son ensemble et doit nous conduire, eu égard à la place de l'outil informatique dans nos vies et dans les systèmes d'information de toutes les organisations, privées comme publiques, à intégrer des réflexes de sécurité numérique dans les comportements, y compris au sein des administrations publiques, des collectivités territoriales et des sociétés privées, dont un certain nombre sont effectivement couvertes et accompagnées par nous en matière de protection économique, et d'autre part ce dont il est question aujourd'hui, à savoir d'envisager et éventuellement d'accepter techniquement la construction d'un dispositif qui soit légalement autorisé, contrôlé et dirigé sur certaines personnes qui seraient des cibles au titre des finalités poursuivies, dans un cadre administratif ou judiciaire.

Les dispositifs que nous évoquons à demi-mot n'ont pas vocation à s'appliquer à M. et Mme Tout-le-monde. Nous en avons besoin pour les missions qui nous sont confiées en matière de protection de la sécurité nationale ou des intérêts fondamentaux de l'État, dans le domaine du renseignement, ou en matière de lutte contre les phénomènes majeurs de crime organisé qui ont été évoqués. Le rapport annuel de la Commission nationale de contrôle des techniques de renseignement illustre à quel point les mesures de surveillance technique que nous pourrons être amenés à mobiliser dans les services de renseignement français couvrent un nombre limité de personnes, dans un cadre réglementaire et légal très strict et extrêmement contrôlé *a priori* et *a posteriori*.

Je comprends tout à fait les enjeux de sécurité numérique qui s'appliquent à tous ; notre propos est d'essayer de vous convaincre de l'importance d'avoir un débat serein et le plus rationnel possible, afin de ne pas priver les appareils sécuritaires, judiciaires ou de renseignement d'un moyen de travailler de manière très ciblée sur des gens qui sont des dangers soit pour la sécurité nationale soit pour le vivre-ensemble en France.

M. Thomas Gassilloud (EPR). Je remercie les sénateurs de nous donner l'occasion d'échanger sur le chiffrement, même si tel n'est pas le premier objet du projet de loi.

Quelles sont les pistes qui s'offrent à nous, aux échelons national et européen, pour résoudre le problème ? Quel est le degré de coopération des messageries instantanées en matière d'accès ciblé à tel ou tel service ?

Quelles sont, hors de l'Union européenne, les modalités de coopération entre les autorités et ces messageries ? Certains États ont-ils imposé l'implantation de *backdoors* – portes dérobées – ou l'accès massif et automatisé à certaines données des messageries instantanées ?

Par ailleurs, vos observations étayent la nécessité de disposer d'une messagerie instantanée européenne. Ce sujet est-il à l'ordre du jour de la discussion avec nos collègues européens ?

M. René Pilato (LFI-NFP). Qui donne les ordres ? Est-il normal ou gênant que l'ordre vienne du premier ministre ? Faut-il opter pour une personnalité indépendante ou neutre ou pour des fonctionnaires du ministère de la justice ? Qui vous donne l'autorisation ?

La possibilité de déverrouiller un chiffrement au nom de la sûreté de l'État ne me pose aucun problème. Ce que je souhaite, c'est savoir qui décide quoi lorsque vous avez repéré quelque chose qui peut tourner mal. J'aimerais que nous discutions de la question de savoir qui, lorsqu'il s'agit de sécurité nationale, doit être habilité à donner les ordres quand vous détectez quelque chose de dangereux, afin de prévenir toute dérive politique, quelle que soit la personne au pouvoir.

M. Vincent Thiébaut (HOR). J'aimerais savoir, très naïvement, comment vous analysez l'impact sur la sécurité intérieure de vos difficultés à accéder à certaines données d'outils de messagerie, alors qu'aux États-Unis, leurs éditeurs agissent dans le cadre de la législation américaine « Cloud Act » qui leur impose des engagements auprès de l'État fédéral.

Mme Céline Berthon. La mise en œuvre des techniques de renseignement obéit à une procédure strictement encadrée par la loi du 24 juillet 2015 relative au renseignement. Elle prévoit notamment que, pour avoir recours à des techniques de renseignement, les services doivent émettre des demandes, qui sont préalablement examinées par la CNCTR, dont les membres sont notamment issus du haut de la hiérarchie de la juridiction administrative et de l'autorité judiciaire ainsi que du Parlement.

Elle se prononce de manière collégiale sur les techniques qui lui sont soumises. Son avis est transmis à l'autorité politique. Il incombe au premier ministre, sur cette base, d'autoriser ou non la mise en œuvre des techniques visées.

Par ailleurs, la loi fixe une liste limitative et précise des techniques et des finalités. Selon les domaines, les moyens sont mobilisables en totalité ou désignés de façon très limitative. Leur utilisation est bornée dans le temps.

Il s'agit donc d'une procédure très carrée, inscrite dans un cadre légal très clair. La CNCTR exerce son contrôle avec finesse et exigence. Elle n'autorise pas toujours la mise en œuvre des techniques demandées et rend compte de ses refus, de façon très transparente, dans son rapport annuel – le plus récent a été publié en avril dernier.

M. René Pilato (LFI-NFP). Si je comprends bien, la CNCTR est neutre et indépendante, mais le premier ministre peut passer outre son avis.

M. Pascal Chauve. Dans le processus qui vient de vous être décrit, la demande est formulée par un service, endossée par un ministre et visée par la CNCTR. C'est bien le premier ministre qui décide – il ne saurait, dans notre pays, en aller autrement dans ce domaine.

Si le premier ministre décide de passer outre l'avis négatif de la CNCTR et d'autoriser la mise en œuvre d'une technique de renseignement, le Conseil d'État est saisi de façon automatique, ce qui offre une garantie supplémentaire. L'alignement entre la commission et l'autorité décisionnaire est impératif, sous peine de déclencher un mécanisme très complexe, que n'avons jamais dû activer, de saisine du Conseil d'État contre le premier ministre.

M. Mahamadou Diarra. Tout cela démontre la reconnaissance dont jouit la CNTCR auprès des autorités.

S'agissant des questions des membres de la commission, il nous sera impossible d'y apporter une réponse précise, même à huis clos.

M. Pascal Chauve. Je dirai, pour atténuer la frustration des membres de la commission spéciale, que nous avons choisi, en France, un système de supervision effective des techniques de renseignement. Le législateur a confié à la CNCTR un pouvoir énorme, en lui offrant un accès permanent, complet et direct aux renseignements recueillis et à ce que les services de renseignement en font.

J'ai l'honneur de diriger un service centralisant les techniques de renseignement pour le premier ministre, qui peut ainsi vérifier que les services de renseignement ont bien agi dans les limites qu'il a fixées dans son autorisation et dans les décisions qu'il a prises. Cette centralisation bénéficie à la CNCTR, qui peut exercer son contrôle *a posteriori* en disposant, comme le prescrit la loi, d'un accès permanent, complet et direct aux données.

M. Éric Bothorel, rapporteur général. Ce n'est pas parce que j'ai été l'un des artisans de la lutte contre l'article 8 *ter* de la proposition de loi sur le narcotrafic que je suis un fan absolu de l'article 6 *bis* en question. J'ai plutôt un avis assez tranché sur le fait que l'on ne répond pas aux excès d'une proposition de loi par les excès d'un projet de loi. À ce titre, je comprends les éléments que vous avez détaillés.

Vous dressez le constat qu'il est nécessaire d'opter pour une réponse technique faute de parvenir à collaborer avec les plateformes. N'aurions-nous pas pu parvenir à une telle collaboration grâce à un dialogue renforcé par l'intermédiaire d'outils tels que le groupe de contact permanent (GCP) ? Créé au lendemain des attentats de janvier 2015, il s'est réuni à de multiples reprises en 2015 et en 2016, très peu en 2017 et en 2018 et pour la dernière fois en 2019. Cette instance, à laquelle sont associées les plateformes, pourrait être un lieu de délibération des évolutions technologiques des uns et des autres ainsi que du rôle de chacun. Sa réunion régulière a été proposée après les émeutes urbaines de l'été 2023.

Je suis surpris que l'on dresse le constat définitif selon lequel nous ne parviendrons pas, par la collaboration, l'échange et le droit, à obliger les plateformes à collaborer et à participer à des coopérations judiciaires de même niveau que celles auxquelles participent les opérateurs téléphoniques au motif que les uns sont nationaux et les autres ne le sont pas. Le droit européen devrait nous aider à y parvenir, ainsi que des instances ne relevant pas du droit dur, telles que le GCP. Je fais partie de ceux qui s'étonnent que l'on fasse peu de cas du GCP, qui, à ses débuts, a porté ses fruits, et qui est désormais abandonné. Quel est votre sentiment à ce sujet ?

Mme Céline Berthon. Nous vous répondrons à huis clos.

La séance est suspendue à 14 heures 55.

***

La séance est reprise à 15 heures.

La commission spéciale a auditionné, à huis clos, MM. Mahamadou Diarra, secrétaire général de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) ; M. Pascal Chauve, directeur du groupement interministériel de contrôle (GIC) ; et Mme Céline Berthon, directrice générale de la sécurité intérieure (DGSI).

En raison du huis clos, la teneur des propos tenus au cours de cette réunion ne donne pas lieu à une retranscription écrite, ni à un enregistrement accessible depuis le portail vidéo de l'Assemblée nationale.

La séance est levée à 15 heures 40.

Membres présents ou excusés

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Réunion du mercredi 9 juillet 2025 à 14 h 05

Présents. - Mme Bénédicte Auzanot, M. Éric Bothorel, M. Mickaël Bouloux, M. Thomas Gassilloud, Mme Catherine Hervieu, M. Tristan Lahais, M. Philippe Latombe, Mme Anne Le Hénanff, M. René Pilato, M. Vincent Thiébaut, Mme Sabine Thillaye

Excusé. - Mme Marietta Karamanli

Assistait également à la réunion. - Mme Véronique Riotton