Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION NATIONALE DE CONTRÔLE DES TECHNIQUES DE RENSEIGNEMENT

Délibération n° 3/2021 du 14 avril 2021

Par une saisine complémentaire du 7 avril 2021[1], le Premier ministre a soumis pour avis à la Commission nationale de contrôle des techniques de renseignement (CNCTR) plusieurs dispositions qu'il propose d'ajouter au chapitre II, consacré au renseignement, du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement :

- un nouvel I ajouté à l'article 13 du projet de loi étend la liste des techniques spéciales d'enquête mentionnées dans le code de procédure pénale pour lesquelles l'autorité judiciaire peut requérir la coopération des opérateurs de télécommunications électroniques. Cette modification vient compléter les dispositions de la saisine initiale en matière de techniques de renseignement, sur lesquelles la CNCTR a déjà rendu son avis ;
- l'article 13 *bis* prévoit de créer, à titre expérimental, une nouvelle technique de renseignement autorisant l'interception des correspondances émises ou reçues par la voie satellitaire ;
- l'article 13 *ter* permet à l'autorité judiciaire de communiquer aux services spécialisés de renseignement ainsi qu'à l'agence nationale de sécurité des systèmes d'information (ANSSI) des informations utiles à la prévention de la cybercriminalité. Il étend cette faculté aux informations intéressant la prévention de la criminalité organisée pour les seuls services spécialisés de renseignement.

Les dispositions des articles 13 et 13 *ter*, qui concernent l'autorité judiciaire, n'appellent pas d'observations de la part de la CNCTR.

Les développements qui suivent concernent exclusivement l'article 13 *bis* du projet de loi.

[1] Voir, sur la saisine initiale, la délibération de la CNCTR n° 2/2021 du 7 avril 2021 disponible sur le site internet de la commission.

1. Le besoin de recourir à une nouvelle technique de renseignement pour intercepter les correspondances transitant par la voie satellitaire

L'étude d'impact accompagnant le projet de loi indique que les moyens de communication empruntant la voie satellitaire vont se développer à l'échelle mondiale sous l'influence du déploiement de nouvelles constellations de centaines, voire de milliers, de satellites placés sur des orbites situées à basse altitude.

La majorité des réseaux de satellites de communications électroniques s'appuient aujourd'hui sur un nombre limité de satellites placés sur une orbite géostationnaire[2] et répondent essentiellement à des besoins spécifiques de clients professionnels ou institutionnels, tels que la fourniture d'un accès internet à haut débit dans des zones non desservies par les réseaux terrestres. D'ores et déjà, ces réseaux sont cependant utilisés par des personnes qui peuvent constituer une menace pour la sécurité nationale.

Les projets de constellations de satellites en orbite basse, portés par des entreprises étrangères, ont pour ambition de satisfaire une clientèle plus nombreuse, allant jusqu'au grand public, en offrant des performances élevées en matière de débit et de temps de latence, à des conditions tarifaires comparables à celles des réseaux terrestres les plus avancés. L'étude d'impact souligne qu'apparaitra ainsi à relativement court terme une offre de télécommunications complète de nature à concurrencer les offres des opérateurs de communications électroniques traditionnels.

Le Gouvernement fait valoir que cette évolution nécessite d'adapter les capacités techniques de surveillance des services de renseignement pour qu'elles puissent s'exercer sur les communications satellitaires.

Sur le plan juridique, les interceptions de correspondances émises par la voie des communications électroniques sont régies par les dispositions du I de l'article L. 852-1 du code de la sécurité intérieure relatives aux interceptions de sécurité. La mise en œuvre d'interceptions de sécurité sur les correspondances émises ou reçues par la voie satellitaire se heurte toutefois à deux difficultés :

- les opérateurs de communications satellitaires sont étrangers et disposent rarement d'une représentation légale sur le territoire national. L'autorité administrative peut, dès lors, avoir des difficultés à requérir leur coopération pour mettre en œuvre ces interceptions ;

- les exigences particulières de confidentialité attachées à la surveillance de certaines cibles peuvent faire obstacle à ce que l'identité de ces cibles soit révélée à un opérateur étranger.

[2] L'orbite géostationnaire de la Terre se situe à une altitude d'environ 36 000 kilomètres.

Pour surmonter ces difficultés le Gouvernement propose de créer, à titre expérimental, un dispositif *ad hoc* permettant d'intercepter les correspondances émises ou reçues par la voie satellitaire sans sollicitation préalable de l'opérateur de communications satellitaires.

Les caractéristiques techniques précises des nouvelles constellations satellitaires ne sont pas connues. Mais il est probable que les identifiants numériques des équipements terminaux des utilisateurs seront modifiés à des fréquences élevées, ce qui rendra plus difficile, voire impossible, la détermination de l'identifiant utilisé par l'abonné que le service souhaite surveiller. Les dispositifs techniques actuellement disponibles devront être éprouvés et sans doute connaître des évolutions.

2. Le dispositif juridique proposé par le projet de loi

Le nouvel article L. 852-3 du code de la sécurité intérieure proposé par l'article 13 *bis* du projet de loi prévoit que, lorsque l'interception des correspondances émises ou reçues par la voie satellitaire *« ne peut être mise en œuvre dans les conditions prévues au I de l'article L. 852-1 »* du même code, un appareil ou un dispositif technique mentionné au 1° de l'article 226-3 du code de procédure pénale peut être utilisé pour réaliser l'interception.

Le principe posé est celui du recours au régime de droit commun des interceptions de sécurité, fondé sur le concours de l'opérateur de communications électroniques concerné pour réaliser l'interception. Ce n'est qu'à titre subsidiaire, lorsque ce concours n'est pas possible, que l'interception peut être réalisée par des moyens techniques opérés par les services de renseignement.

L'article 13 *bis* précise les conditions dans lesquelles l'interception peut être réalisée à titre subsidiaire par ces moyens techniques :

- une autorisation du Premier ministre, après avis de la CNCTR, est nécessaire. Elle est délivrée pour une durée maximale de trente jours et peut être renouvelée. Un décret en Conseil d'État, pris après avis de la CNCTR, devra désigner les services de renseignement autorisés à recourir à la nouvelle technique ;
- un contingentement est prévu, en application duquel le nombre maximal d'autorisations pouvant être délivrées simultanément est arrêté par le Premier ministre, après avis de la CNCTR ;
- les correspondances interceptées ainsi que les données techniques de connexion qui y sont associées sont centralisées par un service du Premier ministre, le groupement interministériel de contrôle (GIC). La centralisation intervient *« dès l'interception des communications, sauf impossibilité technique »*. En cas d'impossibilité technique, les données recueillies sont chiffrées dès leur collecte et jusqu'à leur centralisation effective au sein du GIC. La demande d'autorisation formulée par le service de renseignement doit préciser les motifs faisant obstacle à la centralisation immédiate ;
- les correspondances interceptées sont détruites dès qu'il apparaît qu'elles sont sans lien avec l'autorisation et au plus tard trente jours à compter de leur recueil ;
- les opérations de transcription et d'extraction des communications interceptées sont réalisées au sein du GIC. La CNCTR dispose d'un accès permanent, complet, direct et immédiat à l'ensemble de ces opérations.

L'article 13 *bis* du projet de loi prévoit enfin que l'article L. 852-3 du code de la sécurité intérieure est applicable, à titre expérimental, jusqu'au 31 juillet 2025 et que le Gouvernement

devra adresser au Parlement un rapport d'évaluation sur son application six mois au plus tard avant cette échéance.

3. Les observations de la CNCTR

3.1 Remarques de portée générale

La CNCTR observe, en premier lieu, que les correspondances émises ou reçues par la voie satellitaire sont des correspondances émises par la voie des communications électroniques qui peuvent faire l'objet d'interceptions de sécurité sur le fondement du I de l'article L. 852-1 du code de la sécurité intérieure. Les dispositions du I de l'article L. 852-1 sont donc d'ores et déjà applicables à ce type de correspondances.

Cependant, la mise en œuvre de ces dispositions pour l'interception de correspondances émises ou reçues par la voie satellitaire se heurte à une difficulté tenant au fait que les opérateurs de ce type de communications électroniques sont jusqu'à présent tous étrangers. Cette particularité peut affecter la capacité des pouvoirs publics à imposer à ces opérateurs l'installation sur leurs réseaux de dispositifs d'interception de correspondances ainsi que le respect d'injonctions de mise en œuvre de telles interceptions à l'égard d'un client de l'opérateur. Le service de renseignement concerné peut, en outre, estimer nécessaire, par souci de confidentialité, de ne pas révéler à un opérateur étranger l'identité de la personne qu'il souhaite surveiller (voir le point 1 ci-dessus). Il en résulte que, dans la plupart des cas, le dispositif de droit commun prévu par le I de l'article L. 852-1 du code de la sécurité intérieure est inadapté à ce type d'interception de correspondances.

Le développement, à relativement court terme, des communications empruntant la voie satellitaire, rendu prévisible par le déploiement prochain de nouvelles constellations satellitaires, rend pourtant nécessaire l'élaboration d'un cadre juridique adapté rendant possible la surveillance des communications satellitaires de personnes pouvant constituer une menace au regard de la sécurité nationale et des intérêts fondamentaux de la Nation. A défaut, le recours délibéré à ce mode de communications permettrait indument à ces personnes d'échapper de se soustraire à une surveillance.

La CNCTR constate, dès lors, que le besoin d'établir un cadre juridique adapté permettant d'intercepter les correspondances émises ou reçues par voie satellitaire est avéré.

Le choix retenu par le projet de loi de prévoir un régime juridique subsidiaire à celui fixé par le I de l'article L. 852-1 du code de la sécurité intérieure paraît approprié. La commission estime qu'il est en effet souhaitable de privilégier, lorsque cela est possible, l'application de des dispositions de droit commun des interceptions de sécurité car elles offrent des garanties éprouvées en matière de protection du droit à la vie privée.

Le dispositif juridique proposé soulève toutefois des interrogations.

Comme cela a été indiqué précédemment, le fonctionnement précis des nouvelles constellations satellitaires est encore inconnu à ce jour et la capacité technique d'interception des correspondances transitant par leurs réseaux est incertaine. Il est néanmoins probable que les caractéristiques techniques de ces constellations, comme celles des réseaux mobiles de 5ème génération dits « 5G », rendent plus complexe le ciblage de l'identifiant utilisé par la personne faisant l'objet de la surveillance. Ce ciblage nécessitera sans doute un échange avec

l'opérateur du réseau qui dispose, en temps réel, de l'équivalence entre les identifiants éphémères et les identifiants pérennes des abonnements ou équipements terminaux utilisés par la cible.

Si ces conditions de ciblage ne sont pas réunies, le dispositif technique prévu par l'article L. 852-3 du code de la sécurité intérieure interceptera toutes les correspondances émises ou reçues par la voie satellitaire dans son périmètre d'intervention, sans que l'étendue précise de ce périmètre puisse être évaluée à l'heure actuelle. Le service de renseignement devra ensuite opérer un tri dans cet ensemble de correspondances pour en extraire celles de la cible et détruire toutes les autres. Le dispositif juridique proposé par l'article 13 *bis* du projet de loi s'inspire de celui prévu au II de l'article L. 852-1 du code de la sécurité intérieure, relatif à l'utilisation d'*IMSI catchers* pour l'interception de correspondances, technique très rarement utilisée et soumise à un encadrement juridique strict reposant notamment sur la durée très courte de l'autorisation (quarante-huit heures) et la possibilité de solliciter la technique pour un nombre limité de finalités.

L'absence de dialogue et de coopération avec l'opérateur pour cibler les correspondances à intercepter risque donc d'entraîner une augmentation significative de l'atteinte portée au droit au respect de la vie privée.

La CNCTR estime ainsi souhaitable que soient étudiées d'éventuelles modifications du code des postes et des télécommunications visant à préciser les obligations pesant sur les opérateurs de communications électroniques étrangers afin de rendre plus aisée leur éventuelle réquisition en vue de mettre en œuvre l'interception de correspondances satellitaires dans les conditions de droit commun du I de l'article L. 852-1 ou, à défaut, pour obtenir de leur part un concours technique permettant de circonscrire l'interception des correspondances opérée par le dispositif technique prévu par l'article 13 *bis* du projet de loi.

La CNCTR observe par ailleurs que les dispositifs techniques envisagés pour réaliser les interceptions de correspondances émises ou reçues par la voie satellitaire ne sont pas encore complètement définis.

Au total, si le besoin de doter les services de renseignement de la capacité d'intercepter de telles correspondances paraît établi, les dispositions proposées à cet effet dans le projet de loi sont encore insuffisamment abouties, tant sur le plan technique que sur le plan juridique, pour permettre une mise en œuvre opérationnelle complète et immédiate.

La CNCTR approuve dès lors le choix du recours à une expérimentation de durée limitée proposé par l'article 13 *bis* du projet de loi. Mais, au regard des considérations développées ci-dessus, elle recommande que cette expérimentation obéisse à des conditions plus strictes que celles contenues dans le projet de loi :

- la durée de l'expérimentation devrait être réduite à trois ans, voire deux, au lieu de quatre ;
- seuls les services spécialisés de renseignement, dits du « premier cercle », pourraient y prendre part ;
- les finalités légales de nature à justifier les interceptions par des dispositifs particuliers seraient limitées à la défense et à la promotion des intérêts fondamentaux suivants : l'indépendance nationale, l'intégrité du territoire et la défense nationale (finalité 1), les intérêts majeurs de la politique étrangère, l'exécution des engagements

européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère (finalité 2), la prévention du terrorisme (finalité 4) et la prévention de la criminalité et de la délinquance organisées (finalité 6) ;

- le dispositif juridique serait complété par des dispositions visant à mieux l'encadrer et à faciliter le contrôle de la CNCTR. Ces dispositions sont précisées dans le point 3.2 ci-dessous.

La commission tient à souligner que, si les conditions ci-dessus énumérées lui paraissent justifiées pendant la période d'expérimentation, elles n'ont pas nécessairement toutes vocation à continuer de s'appliquer à l'issue de cette période, dès lors que ce dispositif aura pu être suffisamment éprouvé et amélioré, pendant la phase d'expérimentation, pour rendre possible une mise en œuvre opérationnelle pérenne. Il lui paraît ainsi envisageable que le champ des finalités légales soit alors élargi.

3.2 Observations détaillées

La CNCTR souhaite compléter ses remarques générales par des observations plus spécifiques portant sur certaines dispositions de l'article 13 *bis* du projet de loi.

3.2.1 L'article L. 852-3 du code de la sécurité intérieure proposé par l'article 13 *bis* du projet de loi prévoit que l'utilisation d'un dispositif technique opéré par un service de renseignement ne peut être autorisé que si l'interception des communications émises ou reçues par la voie satellitaire ne peut être réalisée dans les conditions de droit commun des interceptions de sécurité. La commission s'est à cet égard interrogée sur les hypothèses couvertes par la formule « *lorsque cette interception ne peut être mise en œuvre dans les conditions prévues au I de l'article L. 852-1* ». Il ressort des explications qui lui ont été fournies que trois hypothèses sont ici envisagées : impossibilité technique, absence de coopération de l'opérateur, impératifs de confidentialité.

La CNCTR estime que la formulation du projet de loi, qui conditionne l'autorisation de recourir à la nouvelle technique prévue par l'article L. 852-3, mériterait d'être précisée en distinguant l'impossibilité de nature technique du choix d'opportunité. Elle recommande, en outre, de préciser que la demande d'autorisation indique ce motif.

3.2.2 Comme elle l'a exposé ci-dessus (voir le point 3.1), la CNCTR estime souhaitable, afin de limiter les atteintes au droit au respect de la vie privée, d'utiliser de préférence le régime de droit commun du I de l'article L. 852-1 du code de la sécurité intérieure pour intercepter les correspondances émises ou reçues par la voie satellitaire. Dans cette perspective, elle recommande d'ajouter une référence à l'article L. 852-3 de ce code aux articles L. 871-6 et L. 871-7 du même code relatif, respectivement, aux opérations matérielles nécessaires à la mise en place des techniques de recueil de renseignement et à la compensation financière des surcoûts exposés par l'opérateur.

3.2.3 Le I de l'article L. 852-3 du code de la sécurité intérieure proposé par l'article 13 *bis* du projet de loi prévoit que l'appareil ou le dispositif technique utilisé pour l'interception des correspondances émises ou reçues par la voie satellitaire doit faire partie de ceux mentionnés au 1° de l'article 226-3 du code de procédure pénale. Les dispositions auxquelles il est ainsi fait référence soumettent la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou dispositifs permettant d'intercepter

des correspondances à une autorisation du Premier ministre délivrée après avis de la commission mentionnée à l'article R.226-2 du code de procédure pénale.

La CNCTR relève que l'utilisation de ces appareils ou dispositifs, dits de proximité, est déjà autorisée pour la mise en œuvre des techniques prévues par l'article L. 851-6 du code de la sécurité intérieure et par le II de l'article L. 852-1 du même code. L'article L. 851-6 prévoit que ces appareils ou dispositifs techniques font l'objet d'une inscription dans un registre spécial tenu à la disposition de la commission et qu'ils ne peuvent être mis en œuvre que par des agents individuellement désignés et habilités. La commission recommande que des dispositions similaires soient prévues pour les appareils et dispositifs techniques mentionnés à l'article L. 852-3. Elle propose qu'il en aille de même pour ceux mentionnés au II de l'article L. 852-1, qui sont de même nature que ceux prévus à l'article L. 851-6. Cela viendrait corriger un probable oubli lors de l'élaboration de la loi du 24 juillet 2015 relative au renseignement.

3.2.4 L'article L. 852-3 du code de la sécurité intérieure par l'article 13 *bis* du projet de loi prévoit la destruction des correspondances interceptées « *dès qu'il apparait qu'elles sont sans lien avec l'autorisation délivrée, dans la limite du délai prévu au 1° du [I] de l'article L. 822-2* », c'est-à-dire trente jours.

La commission estime que la formule « *sans lien avec l'autorisation délivrée* » mériterait d'être précisée. Elle l'interprète comme s'appliquant à toutes les correspondances et données de connexion qui ne sont pas émises ou reçues par la personne mentionnée dans l'autorisation délivrée par le Premier ministre.

Les difficultés précédemment évoquées (voir le point 3.1 ci-dessus) pour cibler l'identifiant technique utilisé par la personne faisant l'objet d'une surveillance imposeront probablement, dans de nombreux cas, le recueil de l'ensemble des correspondances interceptées dans le périmètre d'interception du dispositif technique. Un tri des données recueillies devra ensuite être opéré pour exploiter celles de la cible et détruire toutes les autres. Plus cette opération est réalisée rapidement, plus l'atteinte au respect de la vie privée s'en trouve réduite. Le délai maximal de trente jours imparti au service de renseignement pour détruire l'ensemble des données recueillies qui ne se rapportent pas à la personne surveillée est particulièrement court. La CNCTR estime cependant qu'il constitue une garantie contribuant à l'exigence de protection du secret des correspondances.

3.2.5 Le projet de loi ne comporte aucune indication sur la durée de conservation des données se rapportant à la personne surveillée.

La durée de conservation des renseignements recueillis avant toute exploitation est fixée par l'article L. 822-2 du code de la sécurité intérieure. En application du 1° du I de cet article, elle est de trente jours pour les correspondances interceptées dans les conditions de droit commun. Cette même durée doit s'appliquer aux correspondances interceptées au moyen du dispositif prévu par l'article L. 852-3. La CNCTR recommande en conséquence d'ajouter au 1° du I de l'article L. 822-2 du code de la sécurité intérieure une référence au nouvel article L. 852-3.

3.2.6 En application de l'article L. 821-4 du code de la sécurité intérieure la durée d'autorisation de droit commun des techniques de renseignement est de quatre mois. Elle est applicable, sauf restriction particulière, aux autorisations d'interception de sécurité délivrées sur le fondement du I de l'article L. 852-1.

Le Gouvernement propose d'instaurer une durée d'autorisation dérogatoire de trente jours pour les interceptions réalisées au moyen du dispositif technique prévu par le nouvel article L. 852-3 du code de la sécurité intérieure. Seules les techniques d'introduction dans un lieu privé et de recueil de données informatiques sont autorisées pour une durée aussi courte[3].

Compte tenu des particularités du dispositif proposé, la commission approuve le choix d'une durée d'autorisation limitée à trente jours qui lui semble opérer une conciliation équilibrée entre les objectifs de sécurité nationale poursuivis par la mise en œuvre de la technique et les atteintes que sa mise en œuvre porte au droit au respect de la vie privée.

3.2.7 Le GIC se voit confier la mission d'organiser la centralisation des données recueillies par la mise en œuvre de la technique prévue par l'article L. 852-3 du code de la sécurité intérieure qui précise que cette centralisation intervient « *dès l'interception des communications, sauf impossibilité technique* ».

La capacité technique de procéder à une centralisation immédiate, c'est-à-dire à un acheminement direct et en temps réel des flux interceptés vers les installations du GIC, dépend essentiellement du type de matériel utilisé pour procéder à l'interception et du niveau de protection dont bénéficieront les données interceptées.

L'article L. 852-3 prévoit que, lorsque la centralisation immédiate est impossible, les données recueillies font l'objet d'un chiffrement dès leur collecte et jusqu'à leur centralisation effective au sein du GIC. L'étude d'impact accompagnant le projet de loi explique qu'il s'agira d'un chiffrement « asymétrique », dont seul le GIC aura la clé. L'article L. 852-3 prévoit que, dans cette hypothèse, la demande d'autorisation formulée par le service de renseignement doit préciser les raisons faisant obstacle à la centralisation immédiate.

L'article L. 852-3 prévoit, en outre, que les opérations de transcription et d'extraction des communications interceptées doivent être réalisées au sein du GIC. Il précise que la CNCTR dispose d'un accès permanent, complet, direct et immédiat à l'ensemble de ces opérations.

La CNCTR rappelle que la centralisation est un principe essentiel de la loi du 24 juillet 2015, introduit à l'article L. 822-1 du code de la sécurité intérieure aux termes duquel : « (…) *Le Premier ministre organise la traçabilité de l'exécution des techniques autorisées en application du chapitre Ier du présent titre et définit les modalités de la centralisation des renseignements collectés.* (…) ». Selon la commission, cette exigence légale conditionne la pertinence et la précision des contrôles *a posteriori* dont la loi l'a chargée. En effet, pour qu'elle puisse réellement disposer, comme la loi le prévoit[4], d'un accès permanent, complet et direct aux renseignements collectés ainsi qu'aux extractions et transcriptions réalisées et, partant, qu'elle puisse effectivement contrôler la mise en œuvre des techniques autorisées, la centralisation des données recueillies est indispensable.

La CNCTR est favorable au principe d'une centralisation immédiate des flux interceptés par le nouveau dispositif prévu par le projet de loi. Elle considère que l'obligation imposée aux services de renseignement de réaliser les opérations de transcriptions et d'extractions dans des

---

[3] L'article 12 du projet de loi propose d'aligner la durée d'autorisation de la technique de recueil de données informatiques sur celle de la technique de captation de données informatiques fixée à deux mois. Dans sa délibération n° 2/2021 du 7 avril 2021, la commission a émis un avis favorable à cette modification.

[4] Voir le 2° de l'article L. 833-2 du code de la sécurité intérieure.

locaux administrés par le GIC constitue une garantie. Elle constate cependant que les modalités concrètes de la centralisation sont encore vagues à ce stade et qu'elles devront être précisées dans le cadre de l'expérimentation.

La CNCTR considère que l'accès immédiat aux données recueillies par la mise en œuvre du dispositif technique prévu à l'article L. 852-3 lui permettra notamment de veiller au respect de l'obligation de destruction des données ne présentant aucun lien avec la personne surveillée et de s'assurer que seules les données relatives à la cible sont conservées et exploitées.

3.2.8 L'article L. 852-3 du code de la sécurité intérieure proposé par l'article 13 *bis* du projet de loi prévoit que la nouvelle technique d'interception de correspondances prévue par ce texte est soumise à un contingentement en application duquel le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum fixé par le Premier ministre après avis de la CNCTR.

La commission rappelle que le contingentement est conçu comme une incitation pour les services de renseignement à mettre un terme aux autorisations devenues inutiles avant de pouvoir en obtenir de nouvelles et, de manière générale, à ne recourir à la technique concernée que « *dans les seuls cas de nécessité d'intérêt public prévus par la loi* », ainsi que l'énonce l'article L. 801-1 du code de la sécurité intérieure à propos des atteintes que l'autorité publique peut légalement porter à la vie privée dans le cadre de la politique de renseignement.

Un contingent est déjà prévu pour les interceptions de sécurité réalisées dans les conditions de droit commun, sur le fondement du I de l'article L. 852-1 du code de la sécurité intérieure. Il s'applique donc aux interceptions de correspondances émises ou reçues par la voie satellitaire opérées selon les dispositions de droit commun des interceptions de sécurité.

Le contingent prévu par le projet de loi s'applique quant à lui spécifiquement aux interceptions de correspondance émises ou reçues par la voie satellitaire et réalisées par le dispositif technique prévu par l'article L. 852-3 du code de la sécurité intérieure. Eu égard aux atteintes susceptibles d'être portées au droit au respect de la vie privée par la mise en œuvre de ce dispositif et au fait qu'il sera mis en œuvre dans le cadre d'une expérimentation, la commission considère que ce contingent devra être rigoureusement limité.

Délibéré en formation plénière le 14 avril 2021

Francis DELON

Président de la Commission nationale
de contrôle des techniques de renseignement