Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION NATIONALE DE CONTRÔLE DES TECHNIQUES DE RENSEIGNEMENT

Délibération n° 2/2021 du 7 avril 2021

Saisie pour avis par le Premier ministre[1] en application de l'article L. 833-11 du code de la sécurité intérieure, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a examiné un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement. La demande d'avis concerne les seules dispositions du chapitre II relatives au renseignement.

Les dispositions du chapitre II du projet de loi sont les suivantes :

- les articles 7 et 8 tendent à pérenniser et à modifier sur plusieurs points la technique dite de l'« algorithme » prévue par l'article L. 851-3 du code de la sécurité intérieure pour les seuls besoins de la prévention du terrorisme (point 1) ;
- l'article 9 prévoit d'étendre le champ des données qui peuvent être recueillies en temps réel, pour les seuls besoins de la prévention du terrorisme, en application de l'article L. 851-2 du code de la sécurité intérieure (point 2) ;
- l'article 10 précise les conditions dans lesquelles les services de renseignement peuvent exploiter les renseignements recueillis et les partager avec d'autres services (point 3) ;
- l'article 11 a pour objet d'autoriser les services de renseignement à conserver des renseignements recueillis, jusqu'à une durée pouvant atteindre cinq ans, à des fins de recherche et développement en matière de capacités techniques de recueil et d'exploitation desdits renseignements (point 4) ;
- l'article 12 aligne la durée d'autorisation de la technique de recueil de données informatiques sur celle de captation de données de même type (point 5) ;
- l'article 13 étend la faculté qu'a le Gouvernement, pour certaines techniques, de requérir la coopération des opérateurs de télécommunications électroniques (point 6).

Les observations qui suivent constituent l'avis de la CNCTR.

La saisine complémentaire du 7 avril 2021[2] introduisant des nouvelles dispositions dans le projet de loi (articles 13, 13 *bis* et 13 *ter*) n'a pas pu être prise en compte dans le présent avis, faute d'un délai suffisant pour l'instruire. Elle fera l'objet d'une délibération ultérieure de la commission.

---

[1] Voir le courrier du directeur, adjoint à la secrétaire générale du Gouvernement du 8 mars 2021.
[2] Voir le courrier du directeur, adjoint à la secrétaire générale du Gouvernement du 7 avril 2021.

1. Sur la technique dite de l'algorithme prévue par l'article L. 851-3 du code de la sécurité intérieure (articles 7 et 8 du projet de loi)

La technique dite de l'algorithme prévue par l'article L. 851-3 du code de la sécurité intérieure a été initialement autorisée à titre expérimental, jusqu'au 31 décembre 2018, par l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement[3]. Cette échéance a été reportée, à la demande du Gouvernement, au 31 décembre 2020 par l'article 17 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. En raison de la crise sanitaire résultant de l'épidémie de Covid-19, le Gouvernement a demandé au Parlement de reporter une nouvelle fois cette échéance d'un an. Saisie pour avis d'un projet de loi prévoyant la prorogation de l'application de l'article L. 851-3 du code de la sécurité intérieure jusqu'au 31 décembre 2021, la CNCTR a estimé, dans un avis du 20 mai 2020[4], que compte tenu à la fois du contexte sanitaire exceptionnel et du contrôle étroit qu'elle exerce sur cette technique, la proposition de nouvelle prorogation n'appelait pas d'observations de sa part. La loi n° 2020-1671 du 24 décembre 2020 relative à la prorogation des chapitres VI à X du titre II du livre II et de l'article L. 851-3 du code de la sécurité intérieure a autorisé la prorogation jusqu'au 31 décembre 2021.

L'article L. 851-3 du code de la sécurité intérieure prévoit que le Premier ministre peut, après avis de la CNCTR, imposer aux opérateurs de communications électroniques et aux fournisseurs de services sur internet la mise en œuvre sur leurs réseaux de traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste. Ces traitements automatisés, communément dénommés « algorithmes », ne peuvent porter que sur des données de connexion, recueillies de manière anonyme et non ciblée. Lorsque des données susceptibles de révéler une menace terroriste ont été détectées par un algorithme, le Premier ministre peut, après un nouvel avis de la CNCTR, autoriser l'identification des personnes auxquelles elles se rapportent. Dans une décision classifiée du 27 avril 2017, le Premier ministre a fixé les règles générales de mise en œuvre de ces algorithmes, en reprenant l'ensemble des observations et recommandations formulées par la CNCTR dans une délibération classifiée du 28 juillet 2016 (voir le point 1.1.1 ci-dessous).

Dans le rapport sur l'application de l'article L. 851-3 du code de la sécurité intérieure qu'il a adressé au Parlement le 30 juin 2020 et dont la CNCTR a été rendue destinataire, le Gouvernement indique que les trois algorithmes en œuvre à cette date donnent des résultats satisfaisants mais que leur utilisation pourrait être améliorée en y incluant des données de nature différente. Il précise en effet que ces algorithmes utilisent uniquement des données de connexion issues des communications téléphoniques et estime souhaitable qu'ils puissent également utiliser les données transitant par le réseau internet, dites « IP » (*internet protocol*), dont certaines *URL (uniform resource locator).*

L'article 8 du projet de loi précise, d'une part, les conditions d'exécution des traitements automatisés et prévoit, d'autre part, l'extension aux *URL* du champ des données qui peuvent être utilisées en application de l'article L. 851-3 du code de la sécurité intérieure.

L'article 7 du projet de loi propose de pérenniser le dispositif de l'algorithme qui, jusqu'à présent, n'est autorisé qu'à titre expérimental par la loi du 24 juillet 2015.

La technique demeure réservée à la seule prévention du terrorisme.

---

[3] Cette loi sera désormais désignée comme la loi du 24 juillet 2015.

[4] Cet avis est disponible sur le site internet de la CNCTR.

Les modifications proposées appellent les observations suivantes.

1.1 Sur l'exécution des traitements automatisés

1.1.1 L'expérimentation réalisée depuis 2015

Le caractère novateur et complexe de la technique dite de l'algorithme a conduit le législateur, en 2015, à soumettre sa mise en œuvre à une période d'expérimentation.

Comme l'indique l'étude d'impact accompagnant le projet de loi, plusieurs modalités d'exécution des traitements automatisés ont été étudiées, en concertation notamment avec les opérateurs de communications électroniques. Par une lettre du 13 juillet 2016, le Premier ministre a sollicité l'avis de la CNCTR sur un projet de dispositif expérimental consistant à dupliquer les flux de données de connexion sur les réseaux des opérateurs puis à les acheminer vers le groupement interministériel de contrôle (GIC), lequel se voyait chargé d'exécuter les traitements automatisés prévus par l'article L. 851-3 du code de la sécurité intérieure.

La commission a estimé, dans sa délibération classifiée du 28 juillet 2016 mentionnée ci-dessus, que ce dispositif n'était pas contraire aux dispositions du I de cet article. Elle a cependant recommandé au Premier ministre d'en subordonner la mise en œuvre à plusieurs conditions et garanties :

- le dispositif ne devait pas permettre aux agents des services de renseignement, quels qu'ils soient, d'accéder aux données dupliquées puis stockées pour l'exécution de l'algorithme. Les seules données susceptibles de leur être transmises seraient celles qui auraient déclenché une alerte générée par l'algorithme et dont l'anonymat serait levé par décision du Premier ministre prise après avis de la CNCTR. Le dispositif devait être placé sous l'entière autorité du GIC, service à compétence nationale du Premier ministre, qui n'est pas un service de renseignement. Les agents du GIC intervenant dans l'exécution du traitement automatisé devaient être individuellement habilités à cet effet, après avis de la CNCTR. D'une manière plus générale, l'action du GIC dans la mise en œuvre de l'algorithme devait être soumise au contrôle de cette dernière. A cette fin, un dispositif de traçabilité de tous les accès au dispositif devait être mis en place et la CNCTR devait disposer d'un accès permanent, complet et direct à ce mécanisme de traçabilité ;
- la durée de stockage des données soumises aux traitements automatisés devait être courte, strictement nécessaire pour permettre l'exécution de ces traitements. Elle avait ainsi pu être limitée à vingt-quatre heures pour le premier algorithme, eu égard aux caractéristiques de celui-ci.

Toutes ces recommandations ont été admises par le Premier ministre.

La CNCTR s'est assurée que les conditions qu'elle avait posées étaient effectivement remplies avant de donner, le 5 octobre 2017, un avis favorable à la première demande d'algorithme dont elle a été saisie. Elle a depuis lors exercé un contrôle étroit, qui n'a révélé aucune anomalie, sur le dispositif d'exécution des traitements automatisés.

La CNCTR a, en outre, recommandé au Premier ministre, dans sa délibération du 28 juillet 2016, d'informer le Parlement des choix effectués pour la mise en œuvre à titre

expérimental de l'article L. 851-3 du code de la sécurité intérieure, en particulier du fait que les traitements automatisés n'étaient pas exclusivement exécutés chez les opérateurs de communications électroniques. Le Premier ministre a adressé un courrier classifié en ce sens au président de la délégation parlementaire au renseignement le 27 avril 2017.

1.1.2 Les dispositions contenues dans le projet de loi

L'article 8 du projet de loi indique que les traitements automatisés prévus à l'article L. 851-3 du code de la sécurité intérieure *« peuvent être autorisés, (...), sur les données transitant par les réseaux des opérateurs (...) »*. Il propose, en outre, d'ajouter un VI à l'article L. 851-3 aux termes duquel : « *Un service du Premier ministre est seul habilité à exécuter les traitements mis en œuvre sur le fondement du I et du IV, sous le contrôle de la Commission nationale de contrôle des techniques de renseignement.* » L'exposé des motifs du projet de loi précise que cette mission incombe au GIC.

Ces dispositions ont ainsi pour objet de préciser que les traitements automatisés sur les données transitant par les réseaux des opérateurs ne sont pas exclusivement exécutés par ces derniers et de fixer le rôle du GIC dans l'exécution des traitements.

La CNCTR considère que le Gouvernement tire ainsi les leçons de l'expérimentation menée sur les algorithmes depuis l'entrée en vigueur de la loi du 24 juillet 2015. Elle est favorable aux modifications proposées qui viennent préciser le cadre légal en prenant en compte les recommandations qu'elle a émises dès 2016 (voir le point 1.1.1 ci-dessus) afin de limiter au strict nécessaire les atteintes portées à la vie privée par l'exécution des algorithmes.

Le projet de loi contient également des dispositions relatives à la durée de conservation des données détectées par l'algorithme et dont la levée d'anonymat est autorisée par le Premier ministre. L'article L. 851-3 du code de la sécurité intérieure prévoit que ces données sont exploitées dans un délai de soixante jours à compter de leur recueil et sont détruites à l'expiration de ce délai, *« sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste attachée à une ou plusieurs des personnes concernées »*.

Le Gouvernement indique que l'expérimentation effectivement menée depuis 2017 a révélé que le délai normal de soixante jours apparaissait suffisant pour permettre aux services de renseignement de solliciter la mise en œuvre d'une technique ciblée sur la personne à laquelle se rapportent les données détectées par le traitement automatisé. Il entend donc renoncer à la possibilité de conserver au-delà de ce délai des données détectées par l'algorithme.

La commission est favorable à la modification proposée qui a pour conséquence de limiter à soixante jours, désormais sans extension possible, la durée de conservation des données détectées par l'algorithme comme susceptibles de caractériser l'existence d'une menace terroriste.

1.2 Sur l'utilisation des *URL*

L'article 8 du projet de loi prévoit, qu'en plus des données de connexion, puissent désormais être utilisées par les traitements automatisés *« les adresses complètes de ressources sur internet »*.

1.2.1 Dans sa délibération n° 1/2016 du 14 janvier 2016[5] rendue sur le projet de décret (devenu le décret n° 2016-67 du 29 janvier 2016) fixant les modalités d'application de l'article L. 851-1 du code de la sécurité intérieure, la CNCTR avait rappelé que les données de connexion, par opposition au contenu de correspondances échangées ou d'informations consultées, désignent le « contenant », c'est-à-dire les données permettant l'acheminement d'une communication électronique. Cette distinction de principe avait déjà été énoncée au cours des travaux qui ont conduit à l'adoption de la loi du 24 juillet 2015[6]. Le Conseil constitutionnel, dans sa décision n° 2015-713 DC du 23 juillet 2015, a précisé que la notion de données de connexion, telle qu'énoncée à l'article L. 851-1 du code de la sécurité intérieure, « *ne peut être entendue comme comprenant le contenu de correspondances ou les informations consultées* » (considérant 55).

L'interdiction d'accéder, par le biais d'un recueil de données de connexion, au contenu des correspondances échangées ou des informations consultées a été rappelée par les articles R. 851-5 et R. 851-9, introduits dans le code de la sécurité intérieure par le décret du 29 janvier 2016. L'article R. 851-5 définit les données de connexion par opposition au *« contenu des correspondances échangées ou des informations consultées »*. L'article R. 851-9 précise que « *les informations ou documents recueillis en application du présent chapitre ne peuvent, sans l'autorisation prévue à l'article L. 852-1[7], être exploités aux fins d'accéder au contenu de correspondances échangées ou d'informations consultées* ».

En examinant la liste des données de connexion figurant au I de l'article R. 851-5 du code de la sécurité intérieure, la commission a considéré que les données mentionnées au b) du 2°, à savoir celles « *relatives à l'accès des équipements terminaux aux réseaux ou aux services en ligne* », pouvaient comprendre les adresses internet ou *URL*. Tout comme la CNIL[8], elle a regardé les *URL* comme des données mixtes, susceptibles de comporter à la fois des données de connexion et des mots faisant référence au contenu de correspondances échangées ou d'informations consultées. Elle a dès lors souligné, dans sa délibération du 14 janvier 2016, que les accès administratifs aux données de connexion ne pouvaient permettre de recueillir un tel contenu et devaient avoir exclusivement pour objet de reconstituer, grâce aux seules parties d'*URL* pertinentes, le chemin informatique utilisé pour échanger des correspondances ou consulter des informations. Elle a ainsi admis le recueil d'*URL* dans le cadre d'accès administratifs aux données de connexion à la condition que seuls soient recueillis les éléments qui déterminent le chemin utilisé pour échanger des correspondances ou consulter des informations, les autres éléments devant être éliminés.

Il ressort de l'exposé des motifs du projet de loi que le Gouvernement entend améliorer l'efficacité de la technique de l'algorithme en incluant « tous les types d'*URL* » parmi les données pouvant faire l'objet des traitements automatisés. Sont englobées à la fois les données relatives à l'accès des équipements terminaux aux réseaux ou aux services en ligne, que le Gouvernement estime relever par nature des données de connexion, et les « *adresses*

---

[5] Cette délibération est disponible sur le site internet de la CNCTR.

[6] Dès l'étude d'impact du projet de loi, le Gouvernement indiquait en effet : « *En application du nouveau régime juridique et comme cela était déjà le cas sous l'empire du régime précédent, l'accès aux données de connexion ne permet pas de connaître le contenu des échanges effectués par les personnes surveillées (...) Il ne s'agit donc que de la collecte de toutes les « traces » d'une connexion ou d'un appel, des factures détaillées dont dispose chaque abonné. Jamais l'accès au contenu d'une connexion ou d'un appel n'est permis* ».

[7] L'article L. 852-1 a trait aux interceptions de sécurité.

[8] Dans sa délibération n° 2015-455 du 17 décembre 2015 portant sur le projet de décret, la CNIL a décrit les *URL* comme *« nécessaire[s] à l'acheminement d'une communication » tout en étant « porteuse[s] par nature des informations consultées »*.

complètes de ressources sur internet », qui peuvent quant à elles faire référence au contenu des informations consultées. Le Gouvernement estime que leur recueil serait particulièrement utile à la prévention du terrorisme en ce qu'il permettrait de détecter les consultations d'informations présentant un lien avéré avec les activités terroristes puis, le cas échéant, d'identifier les individus à l'origine de ces connexions. L'étude d'impact accompagnant le projet de loi précise que le recueil d'« *adresses complètes de ressources sur internet* » ne pourra pas concerner le contenu des informations consultées.

1.2.2 En ce qui concerne la notion d'*URL*

Une *URL* est une chaîne de caractères alphanumériques qui se compose des éléments suivants :

- le type, qui correspond au protocole à utiliser pour accéder à la ressource (http ou https pour une page web) ;
- l'emplacement, qui correspond au nom de domaine du serveur ou à son adresse *IP*, et, le cas échéant, des données d'identification et d'authentification de l'utilisateur, et un numéro de port ;
- le chemin, qui correspond à la page précise que souhaite consulter l'utilisateur ;
- le cas échéant, d'autres données complétant la requête.

L'*URL* désigne ainsi l'adresse d'un contenu, sans pour autant constituer ce contenu.

Dans de nombreux cas, l'*URL* contient, dans ses troisième et quatrième parties, des mots faisant référence au contenu de correspondances échangées ou d'informations consultées.

A titre d'exemple, dans l'*URL* *https://www.google.com/search?client=firefox-b-e&q=cnctr* qui désigne une ressource informatique permettant de rechercher les pages internet faisant référence à la CNCTR :

- l'élément type est : *https ;*
- l'élément emplacement est : *www.google.com ;*
- l'élément chemin est : *search ;*
- les éléments complétant la requête sont : *client=firefox* (le navigateur utilisé) et *q=cnctr* (la chaine de caractères recherchée dans l'internet).

1.2.3 En ce qui concerne la locution « *adresses complètes de ressources sur internet* » utilisée par le projet de loi pour désigner les *URL*

La notion d'*URL* ne paraît pas avoir fait l'objet d'une définition juridique. La locution utilisée par le Gouvernement dans le projet de loi pour la désigner ne semble donc pas avoir de précédent.

La CNCTR relève par ailleurs que le Gouvernement n'a pas cherché à rattacher les *URL* aux données de connexion. Il en fait une catégorie *sui generis*.

Au regard de la locution « *adresses complètes de ressources sur internet* », la CNCTR s'est interrogée sur la pertinence de l'adjectif « *complètes* ». La portée de l'adjectif peut être examinée selon deux angles :

- une *URL* peut contenir des données de connexion et des données de contenu. Dans certains cas, elle pourra ne contenir que des données de connexion. Cependant, une adresse complète ou une *URL* comportera probablement des données de contenu ;
- d'un point de vue opérationnel, le recueil d'adresses complètes ou d'*URL* permet de cerner davantage l'intention de l'utilisateur dans sa consultation d'internet et de cibler avec une précision accrue une activité éventuellement liée à la préparation d'un acte terroriste.

Sous réserve de l'analyse juridique que mènera le Conseil d'Etat, la CNCTR n'émet pas d'objection à la formulation proposée.

Sur le fond, la CNCTR constate que la menace terroriste persiste à un niveau élevé et que le comportement d'auteurs d'actes de terrorisme est souvent caractérisé par une utilisation intensive d'internet. Le besoin opérationnel d'utilisation des *URL* dans le cadre de l'article L. 851-3 du code de la sécurité intérieure, pour détecter ces comportements et prévenir la commission d'actes de terrorisme, semble donc établi. Eu égard aux garanties apportées, en termes de protection du droit au respect de la vie privée, par les dispositions analysées au point 1.1 ci-dessus, la CNCTR n'a pas d'objections à la modification proposée. Elle estime cependant nécessaire de circonscrire les traitements automatisés aux *URL* ayant donné lieu à une consultation effective afin d'exclure celles qui, sans avoir été consultées, se trouveraient dans le contenu de correspondances échangées.

1.3 Sur la pérennisation de l'algorithme

En prévoyant d'abroger l'article 25 de la loi du 24 juillet 2015, qui avait soumis la mise en œuvre de l'article L. 851-3 du code de la sécurité intérieure à une période d'expérimentation initialement fixée à trois ans, l'article 7 du projet de loi propose de pérenniser la technique de l'algorithme.

La CNCTR constate que la menace terroriste perdure et qu'elle se traduit notamment par l'émergence de nouveaux profils d'individus isolés, sensibles aux messages de propagande incitant au passage à l'acte, dont le potentiel dangereux ne peut parfois être révélé qu'à travers leur activité numérique. Elle admet, dès lors, que les impératifs de sécurité nationale justifient que le dispositif de l'article L. 851-3 soit conservé dès lors que les modifications proposées concernant notamment l'encadrement de l'exécution des traitements automatisés renforcent les garanties visant à limiter les atteintes au droit à la protection de la vie privée.

La commission estime cependant que, eu égard à la modification substantielle résultant de la possibilité d'utiliser les *URL*, il est souhaitable de s'assurer, par une procédure d'évaluation, que l'atteinte portée à la vie privée est effectivement justifiée par une meilleure protection contre le risque terroriste.

La CNCTR recommande ainsi de prévoir dans la loi que le nouveau dispositif fera l'objet d'une évaluation par le Parlement à l'issue d'un délai de trois ans.

En conclusion, la CNCTR émet un avis favorable aux modifications envisagées par les articles 7 et 8 du projet de loi, sous les réserves énoncées aux points 1.2.3 et 1.3 de la présente délibération.

2. Sur les modifications apportées à la technique de recueil de données de connexion en temps réel prévue par l'article L. 851-2 du code de la sécurité intérieure (article 9 du projet de loi)

L'article L. 851-2 du code de la sécurité intérieure autorise, pour les seuls besoins de la prévention du terrorisme, le recueil en temps réel sur les réseaux des opérateurs des données techniques de connexion relatives à une personne préalablement identifiée susceptible d'être en lien avec une menace.

L'article 9 du projet de loi propose d'inclure dans le champ des données susceptibles de faire l'objet de ce recueil en temps réel « *les adresses complètes de ressources sur internet utilisées [par une personne préalablement identifiée susceptible d'être en lien avec une menace]* » et d'aligner leur durée de conservation sur celle applicable aux renseignements collectés par la mise en œuvre des techniques de captation ou de recueil de données informatiques prévues par l'article L. 852-3 du code de la sécurité intérieure. Le champ d'application de l'article L. 851-2 demeure limité à la seule finalité de prévention du terrorisme.

Les modifications proposées appellent les observations suivantes.

2.1 La CNCTR souligne, en premier lieu, que le recueil de données prévu par l'article L. 851-2 du code de la sécurité intérieure est ciblé. Il concerne « *une personne préalablement identifiée susceptible d'être en lien avec une menace* » terroriste[9]. Elle relève, en outre, que cette technique est soumise au principe du contingentement en application duquel le nombre maximal des autorisations de recueil pouvant être accordées simultanément est arrêté par le Premier ministre après avis de la commission. Le contingent a, en dernier lieu, été fixé à 720 par une décision du Premier ministre en date du 25 novembre 2019, prise après un avis rendu le 7 novembre 2019[10] par la CNCTR.

2.2 La CNCTR observe, en deuxième lieu, que le projet de loi prévoit d'ajouter aux données de connexion susceptibles d'être recueillies les « *adresses complètes de ressources sur internet utilisées* » par la cible, c'est-à-dire des *URL*. Comme elle l'a indiqué ci-dessus (voir le point 1.2 de la présente délibération), la commission regarde les *URL* comme des données mixtes, susceptibles de comporter à la fois des données de connexion et des mots faisant référence au contenu de correspondances échangées ou d'informations consultées.

La formulation retenue par le projet de loi fait référence aux adresses complètes de ressources sur internet « *utilisées* » par la personne surveillée. La CNCTR considère que cette précision doit être interprétée comme excluant le recueil des adresses de ressources sur internet qui, sans avoir été consultées, pourraient se trouver dans le contenu des correspondances échangées. Elle approuve cette restriction qu'elle souhaite voir étendue à l'utilisation d'*URL*

[9] Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.
[10] Cette délibération est disponible sur le site internet de la CNCTR.

dans le cadre des modifications proposées à l'article L. 851-3 du code de la sécurité intérieure (voir le point 1.2.3 ci-dessus).

2.3 La CNCTR constate, en troisième lieu, que le projet de loi envisage d'aligner la durée de conservation des *URL* recueillies sur celle applicable aux renseignements collectés par la mise en œuvre des techniques de captation ou de recueil de données informatiques prévues par l'article L. 853-2 du code de la sécurité intérieure. Cette durée de conservation est de cent vingt jours à compter du recueil, en application du 2° de l'article L. 822-2 du même code, alors qu'elle est de quatre ans pour les données de connexion.

Le Gouvernement a ainsi choisi de tirer les conséquences de la nature mixte des *URL* en leur appliquant un délai de conservation court, identique à celui prévu pour les données de contenu.

La CNCTR estime que ce choix constitue une garantie de protection de la vie privée et offre une contrepartie appropriée à l'extension aux *URL* du recueil autorisé par l'article L. 851-2.

2.4 La CNCTR rappelle, en dernier lieu, que l'article L. 851-2 dans sa rédaction issue de la loi du 30 octobre 2017 dite « SILT » citée précédemment prévoit que « *lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.* »

Elle considère qu'en dépit des garanties entourant la mise en œuvre de la technique de recueil de données de connexion en temps réel, décrites ci-dessus, l'extension du champ d'application de cette technique aux *URL* utilisées par des personnes appartenant à l'entourage de la personne concernée à titre principal porterait, au regard de l'objectif de prévention du terrorisme, une atteinte disproportionnée au droit au respect de la vie privée de celles-ci. Elle recommande donc de ne pas autoriser le recueil des *URL* pour les personnes appartenant à l'entourage de la personne suspectée d'être en lien avec une menace terroriste.

Sous cette dernière réserve, la CNCTR émet un avis favorable aux modifications proposées par l'article 9 du projet de loi.

3. Sur l'encadrement juridique de l'exploitation des renseignements recueillis et de leur partage entre services de renseignement français (article 10 du projet de loi)

L'article 10 du projet de loi fixe les conditions dans lesquelles un service de renseignement peut exploiter des données recueillies par la mise en œuvre d'une technique de renseignement alors que ces données se rattachent à une autre finalité légale que celle au titre de laquelle la technique a été autorisée. Il fixe également les conditions dans lesquelles un service de renseignement peut partager avec un autre service français les données qu'il a collectées par la mise en œuvre de techniques de renseignement prévues au titre V du livre huitième du code de la sécurité intérieure.

3.1 L'article 10 du projet de loi encadre l'exploitation, par les services de renseignement, des données recueillies par la mise en œuvre de techniques de renseignement.

L'article L. 822-3 du code de la sécurité intérieure dispose : « *Les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3. (...)* ».

Le I de l'article 10 du projet de loi a trait à la situation dans laquelle, à l'occasion de la mise en œuvre d'une technique de renseignement autorisée pour une finalité prévue par l'article L. 811-3 du code de la sécurité intérieure, un service de renseignement accède à des informations se rattachant à la poursuite d'une autre finalité légale. Il prévoit que : « *Lorsqu'un service spécialisé de renseignement mentionné à l'article L. 811-2 ou un service désigné par le décret en Conseil d'Etat prévu à l'article L. 811-4 obtient, à la suite de la mise en œuvre d'une technique mentionnée au titre V du présent livre, des renseignements utiles à la poursuite d'une finalité différente de celle qui a en a justifié le recueil, il peut les transcrire ou les extraire pour le seul exercice de ses missions.* ».

3.1.1 Lorsqu'un service de renseignement sollicite l'autorisation de réaliser une surveillance, il doit préciser dans sa demande le motif de cette surveillance, la finalité légale sur laquelle elle se fonde et la technique de renseignement sollicitée. L'autorisation qui lui est éventuellement délivrée par le Premier ministre, après avis de la CNCTR, vaut uniquement pour cette technique et cette finalité.

Il peut cependant arriver que les renseignements recueillis au cours de la mise en œuvre de la technique révèlent des faits que le service ne soupçonnait pas lorsqu'il a formulé sa demande de technique de renseignement. Il peut ainsi apparaître qu'une personne suspectée d'être impliquée dans la préparation d'un acte terroriste soit, en même temps, impliquée dans un trafic d'armes ou un trafic de stupéfiants commis en bande organisée. L'exploitation de la technique de renseignement autorisée sur le fondement de la finalité de prévention du terrorisme peut alors conduire à la découverte d'informations d'intérêt relevant de la finalité de prévention de la criminalité et de la délinquance organisées.

Le code de la sécurité intérieure ne prévoit pas de dispositions particulières sur ce point. Dans la pratique, l'exploitation et la conservation de renseignements se rattachant à une autre finalité que celle qui a fondé l'autorisation de recueil sont appréciées au cas par cas, sous le contrôle de la CNCTR.

Le I de l'article 10 du projet de loi prévoit d'autoriser expressément les services de renseignement à transcrire ou extraire des renseignements « *utiles à la poursuite d'une finalité différente de celle qui a justifié le recueil (...) pour le seul exercice de [leurs] missions* ».

Deux tempéraments à l'autorisation sont cependant prévus :

- En premier lieu, les services de renseignement continuent à ne pas être autorisés à transcrire ou extraire les renseignements qui ne se rattachent à aucune des finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure ;
- En second lieu, les services de renseignement ne sont autorisés à transcrire ou extraire les données recueillies par la mise en œuvre d'une mesure de surveillance que pour le seul exercice de leurs missions, fixées par les textes règlementaires régissant chaque service de renseignement. Ainsi, les services dits du « second cercle » qui n'ont accès qu'à un nombre limité de finalités et de techniques de renseignement précisées dans la partie réglementaire du code de la sécurité

intérieure, ne pourront transcrire ou extraire des renseignements se rattachant à une finalité légale que ces textes ne les ont pas autorisés à invoquer.

3.1.2 L'article 10 du projet de loi prévoit également un contrôle spécifique de la CNCTR sur les transcriptions et les extractions de renseignements se rattachant à une finalité différente de celle qui a justifié le recueil.

L'article L. 822-3 du code de la sécurité intérieure soumet les opérations de transcriptions et d'extractions au contrôle de la CNCTR. L'article L. 822-4 du même code prévoit, à cette fin, que les opérations de destruction des renseignements collectés, les transcriptions et les extractions font l'objet de relevés, tenus à la disposition de la commission.

Le II de l'article 10 du projet de loi, qui modifie l'article L. 822-4 du code de la sécurité intérieure, prévoit d'ajouter que ces relevés devront désormais préciser si les transcriptions ou les extractions ont été effectuées pour une finalité différente de celle qui en a justifié le recueil.

La CNCTR estime que, si le dispositif proposé d'établissement de relevés est utile à l'exercice de son contrôle *a posteriori,* il n'est pas suffisant, en l'état, pour garantir un contrôle effectif du bien-fondé du rattachement de transcriptions et extractions à une finalité légale différente de celle justifiant le recueil et de leur lien avec le seul exercice des missions du service. En effet, la commission n'a pas la capacité, à l'occasion des contrôles *a posteriori* auxquels elle procède, d'examiner la totalité des relevés établis par les services de renseignement en application de l'article L. 822-4 du code de la sécurité intérieure. Pour exercer effectivement son contrôle sur les transcriptions et extractions se rattachant à une finalité différente de celle qui a justifié le recueil, elle a besoin d'en être spécialement informée par une transmission systématique et immédiate des relevés relatifs à ces opérations.

La CNCTR préconise, en conséquence, d'inscrire dans la loi que les relevés de transcriptions et d'extractions effectuées pour une finalité différente de celle ayant fondé l'autorisation de recueil lui sont systématiquement et immédiatement transmis, et non, comme le prévoit le II de l'article 10, simplement tenus à sa disposition.

3.2 L'article 10 du projet de loi fixe, en second lieu, les conditions dans lesquelles les services peuvent échanger les renseignements qu'ils ont collectés par la mise en œuvre des techniques prévues au titre V du livre huitième du code de la sécurité intérieure.

Aux termes de l'article L. 863-2 du code de la sécurité intérieure : *« Les services spécialisés de renseignement mentionnés à l'article L. 811-2 et les services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 peuvent échanger toutes les informations utiles à l'accomplissement de leurs missions définies au titre Ier du présent livre. / (...) / Les modalités et les conditions d'application du présent article sont déterminées par décret en Conseil d'Etat.* ». Ce décret en Conseil d'Etat n'a toutefois pas été pris.

L'article 10 du projet de loi propose de fixer dans la loi les conditions dans lesquelles les services de renseignement peuvent échanger des renseignements collectés, extraits ou transcrits par la mise en œuvre de techniques autorisées sur le fondement du livre huitième du code de la sécurité intérieure, y compris celles relatives à la surveillance des communications électroniques internationales. Il fixe également les modalités de contrôle de ces échanges et comporte à cette fin plusieurs dispositions nouvelles :

- le I ajoute, à l'article L. 822-3 du code de la sécurité intérieure, un II fixant les conditions dans lesquelles ces échanges peuvent être opérés et suivis au sein de chaque service ;
- le II précise, à l'article L. 822-4 du code de la sécurité intérieure, que les transmissions de renseignement font l'objet de relevés tenus à la disposition de la CNCTR ;
- le III précise, à l'article L. 833-2 du code de la sécurité intérieure, que la CNCTR dispose d'un accès permanent, complet et direct aux relevés et aux transmissions ;
- le IV prévoit, à l'article L. 854-6 du code de la sécurité intérieure, que les services spécialisés de renseignement, dits du « premier cercle », peuvent échanger des renseignements issus de la surveillance des communications électroniques internationales entre eux et avec des services dits du « second cercle » ;
- le V prévoit, à l'article L. 833-6 du code de la sécurité intérieure, que la CNCTR peut adresser au Premier ministre, au ministre et au service concerné, des recommandations tendant à l'interruption de transmissions de renseignements si celles-ci lui paraissent être effectuées en méconnaissance de la loi.

Les échanges de renseignements sont, dans certains domaines tels que la prévention du terrorisme, une condition essentielle de l'efficacité de l'action menée par les services. Ils contribuent à la sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation. Ils doivent néanmoins, comme le recueil du renseignement, s'opérer dans un cadre légal que la CNCTR doit contrôler.

Les dispositions proposées appellent de la part de la CNCTR les observations suivantes.

3.2.1 Sur le cadre juridique proposé pour les échanges de renseignements

a) L'article 10 du projet de loi prévoit qu'un service de renseignement, qu'il appartienne au « premier cercle » ou au « second cercle », « *peut transmettre à un autre de ces services les renseignements collectés, extraits ou transcrits dont il dispose, si cette transmission est strictement nécessaire à l'exercice des missions du service destinataire.* »

Cette formulation recouvre à la fois la transmission de renseignements à l'état brut, c'est-à-dire tels qu'ils ont été recueillis avant toute exploitation ainsi que celle des transcriptions et extractions réalisées à partir des données recueillies[11].

La précision selon laquelle la transmission doit être « *strictement nécessaire à l'exercice des missions du service destinataire* » fixe la limite des échanges de renseignements. Elle fait notamment obstacle à ce qu'un service puisse se voir transmettre des renseignements relevant d'une finalité à laquelle il n'est pas autorisé à recourir. Elle fait écho à la limitation apportée par l'article 10 à la capacité, pour un service, de transcrire ou d'extraire des renseignements utiles à la poursuite d'une finalité différente de celle qui en a justifié le recueil. La commission renvoie sur ce point aux remarques qu'elle a formulées au point 3.1.2 de la présente délibération.

[11] La CNCTR rappelle que l'exploitation des données recueillies peut prendre la forme d'extractions, lorsqu'une partie de ces données, par exemple une image ou une parole, est prélevée, ou de transcriptions, lorsque des données brutes font l'objet d'une transformation destinée à en faciliter l'analyse.

S'agissant de la surveillance des communications électroniques internationales, le IV de l'article 10 du projet de loi prévoit une modification de l'article L. 854-6 du code de la sécurité intérieure qui a pour objet d'autoriser les services spécialisés de renseignement, dits du « premier cercle », à transmettre des renseignements transcrits ou extraits issus de cette surveillance à d'autres services du premier ou du second cercle. Les règles fixées par l'article L. 822-3 pour régir les transmissions sont applicables.

b) L'article 10 du projet de loi prévoit cependant que certaines transmissions de renseignements sont subordonnées à une autorisation préalable du Premier ministre délivrée après avis de la CNCTR.

Il s'agit, en premier lieu, des transmissions de renseignements collectés, réalisées pour une finalité différente de celle qui en a justifié le recueil. Cela concerne les renseignements à l'état brut, tels qu'ils ont été recueillis avant toute exploitation par le service intéressé.

Dans cette hypothèse la transmission porte sur l'intégralité des renseignements recueillis par la mise en œuvre d'une technique de renseignement et intervient pour une finalité différente de celle au titre de laquelle cette technique a été autorisée. La CNCTR estime, dès lors, comme le prévoit le projet de loi, qu'elle doit être soumise à autorisation du Premier ministre après avis de la commission, qui devra notamment vérifier que les renseignements collectés présentent un lien avec la finalité au titre de laquelle la transmission est sollicitée et veiller à ce que les durées de conservation des renseignements collectés fixées par l'article L. 822-2 soient respectées tant par le service à l'origine du recueil que par le service destinataire de la transmission.

Il s'agit, en second lieu, des transmissions de renseignements collectés, extraits ou transcrits qui sont issus de la mise en œuvre d'une technique de renseignement à laquelle le service destinataire n'aurait pu recourir au titre de la finalité motivant la transmission.

Cette formulation recouvre à la fois la transmission de renseignements à l'état brut ainsi que celle des transcriptions et extractions réalisées à partir des données recueillies. La transmission envisagée ne peut intervenir que pour une finalité à laquelle le service destinataire est autorisé à recourir.

Dans cette hypothèse la transmission porte sur des renseignements recueillis au moyen d'une technique que le service destinataire n'est pas autorisé à mettre en œuvre au titre de la finalité pour laquelle la transmission intervient. Cette situation peut notamment se rencontrer lorsque le service destinataire appartient à la catégorie des services de renseignement du « second cercle ». Ces services n'ont en effet accès qu'à un nombre limité de techniques de renseignement, qui peuvent varier selon la finalité invoquée.

La CNCTR est favorable au dispositif proposé qui lui permettra notamment de vérifier, lorsqu'elle rendra son avis, que les renseignements dont la transmission à un autre service est demandée ont été recueillis dans des conditions régulières et présentent un lien avec la finalité au titre de laquelle la demande a été formée.

3.2.2 Sur le contrôle des échanges de renseignements

a) L'article 10 du projet de loi prévoit un dispositif de contrôle interne reposant sur la désignation, au sein de chaque service de renseignement, d'un agent chargé de veiller au

respect du cadre légal des transmissions de renseignements. Le service « émetteur », qui met en œuvre la technique à l'origine du recueil des renseignements, devra rendre compte de leur destruction, au terme du délai légal, au service « destinataire ». Le service émetteur demeure ainsi responsable des renseignements qu'il a recueillis, même après leur transmission à un autre service.

La CNCTR est favorable à ce dispositif de contrôle interne.

b) L'article 10 prévoit également un dispositif de contrôle externe assuré par la CNCTR.

Ce dispositif s'appuie sur trois articles du code de la sécurité intérieure :

- une modification, proposée à l'article L. 822-4, prévoit que les transmissions de renseignements « *font l'objet de relevés tenus à la disposition de la [CNCTR] qui précisent : (...) 2° S'agissant des transmissions, leur nature, leur date et leur finalité, ainsi que le ou les services qui en ont été destinataires.* ».
  La CNCTR renvoie aux remarques qu'elle a formulées au point 3.1.2 ci-dessus, concernant les relevés de transcriptions et d'extractions effectuées pour une finalité différente de celle ayant justifié le recueil. Elle préconise d'inscrire dans la loi que les relevés de transmissions de renseignements lui sont systématiquement et immédiatement transmis, et non, comme le prévoit le II de l'article 10, simplement tenus à sa disposition ;
- une modification, prévue à l'article L. 833-2, ouvre à la CNCTR un accès permanent, complet et direct aux transmissions de renseignements. Elle n'appelle pas d'observations ;
- une modification, proposée à l'article L. 833-6, permet à la CNCTR de recommander au Premier ministre, au ministre et au service concerné l'interruption de transmissions de renseignements lorsque celles-ci lui paraissent effectuées en méconnaissance de la loi. Elle n'appelle pas d'observations.

S'agissant des transmissions de renseignements issus de la surveillance des communications électroniques internationales, le projet ne prévoit pas de dispositions équivalentes permettant à la CNCTR d'exercer sur elles un contrôle effectif. Dans la mesure où cette surveillance obéit à des règles spécifiques, mentionnées au chapitre IV du titre V du livre huitième du code de la sécurité intérieure, les dispositions des articles L. 822-4 de ce même code relatives aux relevés de transmissions, L. 833-2 relatives à l'accès permanent, complet et direct de la CNCTR aux relevés et aux transmissions et L. 833-6 permettant à la CNCTR de recommander l'interruption et la destruction de transmissions de renseignements ne sont en effet pas automatiquement applicables. La CNCTR estime dès lors nécessaire de compléter les dispositions des articles L. 854-6 et L. 854-9 du code de la sécurité intérieure afin de prévoir des garanties similaires à celles prévues par le projet de loi en matière de contrôle des transmissions de renseignements issus de la surveillance réalisée sur le territoire national. Pour les mêmes motifs que ceux exposés précédemment, la commission préconise, en outre, d'inscrire dans la loi que les relevés des transmissions de renseignements issus de la surveillance des communications électroniques internationales lui sont systématiquement et immédiatement transmis.

3.3 La commission n'a pas d'observations sur les autres dispositions de l'article 10 du projet de loi, notamment celles modifiant les dispositions de l'article L. 863-2 du code de la sécurité intérieure relatives aux modalités de transmission d'informations par les autorités

administratives aux services de renseignement, lesquelles n'entrent pas dans le champ du contrôle, exercé par la CNCTR, de la mise en œuvre des techniques de renseignement.

4. Sur la conservation de renseignements à des fins de recherche et de développement en matière de capacités techniques de recueil et d'exploitation (article 11 du projet de loi)

L'article 11 du projet de loi propose d'ajouter à l'article L. 822-2 du code de la sécurité intérieure, qui fixe les durées maximales de conservation des renseignements collectés selon le type de données recueillies, des dispositions nouvelles autorisant les services de renseignement à conserver des renseignements collectés, au-delà des durées normalement applicables et jusqu'à cinq ans, à des fins de recherche et développement en matière de capacités techniques de recueil et d'exploitation. Il propose, en outre, par un nouvel article L. 822-2-1, d'ouvrir cette faculté au GIC, aux mêmes fins et dans les mêmes conditions.

Le Gouvernement justifie ces nouvelles dispositions par la nécessité de permettre aux services de renseignement et au GIC d'utiliser les outils de l'intelligence artificielle, et plus particulièrement ceux de l'apprentissage automatique, pour améliorer et faciliter les capacités techniques en matière de recueil et surtout, d'exploitation, des données recueillies par la mise en œuvre de techniques de renseignement.

4.1 En ce qui concerne les services de renseignement, le Gouvernement fait valoir que ceux-ci ont besoin de disposer d'un stock important de données, captées par les techniques de renseignement, à partir desquelles ils pourront développer, améliorer et valider leurs capacités techniques de recueil et d'exploitation de ces données.

La CNCTR est consciente de la nécessité pour les services de renseignement, face au développement des techniques de chiffrement des communications électroniques, de concevoir des solutions techniques innovantes leur permettant de maintenir leurs capacités de recueil et d'améliorer leurs capacités d'exploitation afin de pouvoir disposer, en temps utile, des informations pertinentes.

Elle estime, néanmoins, que l'utilisation à des fins de recherche et développement de données issues de techniques de renseignement doit être rigoureusement encadrée et entourée de garanties fortes.

4.1.1 La commission s'est interrogée sur la nécessité de recourir aux données issues de techniques de renseignement à des fins de recherche et développement.

Les précisions qui lui ont été apportées ont montré que si les outils de recherche et développement envisagés peuvent, dans un premier temps, être utilisés sur des données émanant de « sources ouvertes », ces dernières ne permettent pas, à elle seules, d'atteindre le but recherché. Ces outils, pour être adaptés aux contraintes opérationnelles, doivent être mis en situation réelle à partir de données opérationnelles collectées. Ils doivent, en outre, trouver à s'exercer sur de grandes quantités de données, de diverses natures (texte, image, son, ...) De ces conditions dépendent la performance des programmes de recherche qu'il s'agit de concevoir.

4.1.2 La commission relève que l'article 11 du projet de loi autorise l'ensemble des services de renseignement à faire application du régime dérogatoire de conservation des données. Il apparaît pourtant que seuls certains services spécialisés de renseignement disposent des compétences et des moyens techniques et humains nécessaires à la conception d'outils de recherche et développement.

Dans ces conditions, la CNCTR recommande de restreindre le champ d'application du III de l'article L. 822-2 du code de la sécurité intérieure aux seuls services spécialisés de renseignement, dits du « premier cercle ».

4.1.3 La CNCTR a examiné les conditions de conservation, d'utilisation et de destruction des données envisagées par l'article 11 du projet de loi.

a) Concernant la conservation des données, le projet de loi prévoit qu'elle est opérée dans la mesure strictement nécessaire à l'acquisition des connaissances suffisantes pour développer, améliorer et valider les capacités techniques de recueil et d'exploitation. Il prévoit, en outre, qu'elle s'effectue dans des conditions qui occultent les motifs et les finalités pour lesquelles les données ont été collectées et qui garantissent l'impossibilité de rechercher l'identité des personnes concernées.

Les explications fournies à la CNCTR sur les opérations techniques qu'il est envisagé d'appliquer aux données conservées à des fins de recherche et développement lui apparaissent pertinentes. Toutefois l'application des règles fixées pour la conservation des données devra être appréciée pour chaque programme en fonction des dispositions prévues pour cette conservation et des moyens de contrôle correspondants. La CNCTR renvoie sur ce point aux développements du point 4.1.4 ci-dessous.

b) Concernant l'utilisation des données, le projet exclut tout usage à des fins de surveillance et précise que ces données ne seront accessibles qu'aux seuls agents habilités pour cette mission.

L'utilisation de données issues de techniques de renseignement à des fins de recherche et développement doit en effet, selon la commission, être réalisée dans des conditions garantissant que les agents des services de renseignement chargés de l'exploitation et de l'analyse de ces données ne puissent, pour quelque motif que ce soit, accéder aux dispositifs de recherche et développement en cours de fonctionnement ni au support de stockage des données conservées à cette fin. Les prescriptions de l'article 11 restreignant l'accès à ces données au personnel dédié à la recherche et développement vont dans ce sens.

Il serait cependant souhaitable de préciser que le stockage des données conservées à des fins de recherche et développement est matériellement et informatiquement cloisonné, de manière à prévenir tout risque de détournement à des fins de surveillance.

c) Concernant la destruction des données, le projet prévoit qu'elle est opérée dès que la conservation des données n'est plus indispensable à la validation des capacités techniques de recueil et d'exploitation et, au plus tard, cinq ans après leur recueil.

Le délai maximal de conservation de cinq ans proposé par le Gouvernement se situe entre la durée de conservation des données techniques de connexion et celle autorisée pour les données chiffrées, respectivement fixées à quatre et six ans par l'article L. 822-2 du code de la

sécurité intérieure. Elle est cependant bien supérieure à la durée légale de conservation des données de contenu, qui ne dépasse pas cent vingt jours.

L'apprentissage automatique permet d'entraîner un programme informatique sur des données (lors de la phase d'apprentissage ou d'entraînement) afin de définir leur comportement ultérieur (lors de la phase dite d'inférence ou de prédiction). Cet apprentissage peut être supervisé ou non. Lorsqu'il est supervisé, il consiste à entraîner le programme sur des données préalablement « annotées » ou « étiquetées » par une intervention humaine avant de lui soumettre des données inconnues de nature similaire sur lesquelles il doit formuler des propositions d'annotation.

Selon les informations fournies à la CNCTR, la phase d'apprentissage est longue et, surtout, l'apprentissage est continu. Entre deux phases d'inférence, le programme doit à nouveau être entraîné sur les données initiales afin de ne pas perdre les capacités précédemment acquises. Les allers et retours permanents entre les données initiales annotées et des données nouvelles nécessitent un délai de conservation de plusieurs années des données initiales.

Compte-tenu de ces éléments et eu égard aux précautions prévues pour éviter que les données conservées ne soient associées aux personnes concernées, la CNCTR estime que le délai maximal de conservation de cinq ans opère une conciliation équilibrée entre l'objectif d'amélioration des capacités techniques de recueil et d'exploitation des données issues de techniques de renseignement et le risque d'atteinte à la vie privée des personnes auxquelles ces données se rapportent.

Toutefois, le caractère proportionné du délai de conservation des données, dans la limite de cinq ans, devra être apprécié pour chaque programme en fonction de ses caractéristiques. La commission renvoie sur ce point aux développements du point 4.1.4 ci-dessous.

4.1.4 L'article 11 du projet de loi prévoit que les paramètres techniques applicables à chaque programme de recherche sont soumis à une autorisation préalable du Premier ministre, délivrée après avis de la CNCTR.

a) La commission estime qu'un contrôle préalable de chaque programme est en effet nécessaire pour s'assurer que la conservation de données issues de techniques de renseignement à des fins de recherche et développement est effectivement justifiée par les caractéristiques du programme.

La commission entend par « programme de recherche » un type de programme informatique destiné à assurer une fonction spécifique. Par exemple, la capacité de reconnaissance de la langue parlée constitue, selon elle, un programme de recherche. La capacité de reconnaissance du locuteur constitue un autre programme de recherche. Un programme de recherche est susceptible de porter sur plusieurs projets. Dans l'exemple du programme de reconnaissance de la langue, la reconnaissance de chaque langue correspondrait à un projet distinct.

Le contrôle préalable exercé par la CNCTR, avant décision du Premier ministre, portera ainsi sur l'architecture générale de chaque programme de recherche et développement conçu par un service de renseignement. La demande d'autorisation devra indiquer les modalités précises de recueil, de conservation et d'utilisation des données dont la conservation est envisagée, la liste des agents habilités à les exploiter ainsi que les solutions retenues pour garantir que les

personnes concernées ne pourront être identifiées. Elle devra également préciser la durée de conservation des données souhaitée en fonction des caractéristiques du programme.

Le dispositif proposé est comparable à celui prévu par l'article L. 851-3 du code de la sécurité intérieure pour l'autorisation de mise en œuvre des algorithmes. La CNCTR le juge pertinent.

b) La CNCTR estime néanmoins souhaitable d'exercer un contrôle sur la mise en œuvre de la conservation des données de renseignement à des fins de recherche et développement.

Elle recommande, en conséquence, de préciser dans la loi qu'elle dispose, pour les données conservées à des fins de recherche et développement, de l'accès permanent, complet et direct prévu par l'article L. 833-2 du code de la sécurité intérieure pour les données de renseignement. Elle souhaite également être informée des résultats obtenus par chaque programme de recherche autorisé afin de s'assurer de la pertinence de la poursuite de la conservation des données associées à chacun des programmes.

La CNCTR estime enfin qu'elle devrait être informée de toute modification substantielle affectant les modalités techniques de paramétrage de chaque programme de recherche et qu'elle devrait pouvoir émettre des recommandations tendant à la suspension ou à l'interruption d'un programme qui ne correspondrait plus au cadre légal.

4.2 L'article 11 du projet de loi prévoit par ailleurs, dans un nouvel article L. 822-2-1 du code de la sécurité intérieure, de permettre au GIC de conserver des données issues de techniques de renseignement, pour les mêmes fins et dans les mêmes conditions que celles prévues pour les services de renseignement.

4.2.1 En tant que service à compétence nationale chargé de la centralisation des demandes d'autorisation de mise en œuvre des techniques de renseignement et de celle de l'exploitation des données recueillies, le GIC justifie de besoins en matière de développement et d'amélioration des capacités techniques d'exploitation des données issues de techniques de renseignement.

La commission n'émet donc pas d'objection à ce que ce service du Premier ministre soit autorisé à conserver des données recueillies par les services de renseignement et centralisées par lui, pour les seuls besoins de recherche et développement en matière d'amélioration des capacités techniques d'exploitation de telles données.

4.2.2 Le nouvel article L. 822-2-1 du code de la sécurité intérieure prévu par l'article 11 du projet de loi précise que le GIC peut conserver les renseignements dont il organise la centralisation « *dans les conditions prévues au III de l'article L.822-2* ».

La commission estime souhaitable de préciser que les données qui seront conservées par le GIC à des fins de recherche et développement fassent l'objet d'un stockage spécifique, matériellement et informatiquement cloisonné.

En conclusion, la CNCTR émet un avis favorable sur l'article 11 du projet de loi, sous les réserves énoncées aux points 4.1 et 4.2 de la présente délibération.

5. Sur l'alignement des durées d'autorisation des techniques prévues par l'article L. 853-2 du code de la sécurité intérieure (article 12 du projet de loi)

L'article 12 du projet de loi propose d'aligner la durée d'autorisation de la technique de recueil de données informatiques prévue par le 1° du I de l'article L. 853-2 du code de la sécurité intérieure sur celle de la technique de captation de données informatiques prévue par le 2° du I du même article.

Ces durées d'autorisation, prévues par le II de l'article L. 853-2 du code de la sécurité intérieure sont aujourd'hui respectivement fixées à trente jours et à deux mois. Le Gouvernement propose une harmonisation à deux mois.

La CNCTR rappelle qu'en application des dispositions en vigueur, le recueil de données informatiques vise à permettre d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre alors que la captation de données informatiques vise à permettre d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles que celui-ci les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques.

Le législateur a considéré, en 2015, que le degré d'atteinte à la vie privée de la technique permettant d'accéder au « stock » des données informatiques contenues dans un système informatique était supérieur à celui de la technique permettant d'accéder au « flux » des données de même type, telles qu'elles s'affichent sur un écran ou sont reçues ou émises par des périphériques. Ce raisonnement se fondait notamment sur le volume de données susceptibles d'être recueillies.

La CNCTR n'a cependant pas observé, dans l'exercice de son contrôle, de différence notable entre les deux techniques en termes d'atteinte à la vie privée, dans toutes ses composantes. La pratique a révélé que la frontière entre les deux dispositifs était ténue. La nature des données recueillies est la même dans les deux hypothèses. Les modalités techniques de mise en œuvre font souvent appel au même matériel. L'intensité de l'atteinte portée à la vie privée semble dépendre davantage des habitudes et des comportements des individus faisant l'objet de la surveillance que de la technique utilisée elle-même.

En revanche, comme le fait valoir le Gouvernement, la commission a constaté que la mise en œuvre de la technique de recueil de données informatiques se heurtait régulièrement à des difficultés, le délai d'autorisation de trente jours ne prenant pas suffisamment en considération les contraintes opérationnelles rencontrées par les services.

La commission estime, en conséquence, que le maintien d'un régime de durée d'autorisation différencié n'apparaît pas justifié alors, en outre, que le régime de conservation des renseignements collectés est le même pour les deux techniques (la durée de conservation a été fixée à cent vingt jours par le 2° de l'article L. 822-2 du code de la sécurité intérieure).

Au regard de l'ensemble de ces éléments, la commission émet un avis favorable à la modification envisagée par l'article 12 du projet de loi soumis à son examen.

La commission considère en outre qu'il pourrait être opportun, pour des motifs d'intelligibilité et de cohérence de la loi, de supprimer la distinction entre ces deux techniques, sur le modèle de ce que prévoit le code de procédure pénale[12].

6. Sur la faculté de requérir la coopération des opérateurs de communications électroniques pour la mise en œuvre des techniques prévues par les articles L. 851-6 et L. 853-2 du code de la sécurité intérieure (article 13 du projet de loi)

L'article 13 du projet de loi prévoit de modifier la liste des techniques de renseignement pour lesquelles l'article L. 871-6 du code de la sécurité intérieure permet de requérir la coopération des opérateurs de communications électroniques afin qu'ils procèdent aux opérations matérielles nécessaires à la mise en œuvre de ces techniques sur leurs réseaux.

Cette liste est actuellement limitée aux recueils de données de connexion en temps différé (article L.851-1 du code de la sécurité intérieure) et en temps réel (article L. 851-2), à la mise en œuvre de traitements automatisés dits « algorithmes » (article L. 851-3), aux géolocalisations en temps réel (article L. 851-4) et aux interceptions de sécurité (I de l'article L. 852-1). Le Gouvernement propose d'y ajouter les recueils de données techniques de connexion par dispositifs de proximité dit « *IMSI catcher* » prévus par l'article L. 851-6 du même code ainsi que les techniques de recueil et de captation de données informatiques prévus par l'article L. 853-2 de ce code.

6.1 En ce qui concerne les recueils de données techniques de connexion par « *IMSI catcher* », le Gouvernement fait valoir les difficultés que suscitera le déploiement des réseaux mobiles de 5ème génération dits « 5G ». Les caractéristiques techniques de ces réseaux auront notamment pour effet de modifier, à des fréquences élevées, les identifiants numériques échangés entre les équipements terminaux des utilisateurs et les antennes de ces réseaux. Dans ces conditions, seul l'opérateur du réseau 5G utilisé pourra faire le lien entre les identifiants éphémères et les identifiants pérennes des abonnements ou des équipements terminaux concernés et déterminer quel abonné utilise tel identifiant particulier à un instant donné.

A la lumière de ces explications, la CNCTR comprend que la faculté de requérir la coopération des opérateurs de communications électroniques deviendra indispensable pour que cette technique conserve un intérêt opérationnel.

6.2 En ce qui concerne les techniques de recueil et de captation de données informatiques, le Gouvernement indique qu'elles sont mises en œuvre selon deux modalités : soit par accès direct au support informatique concerné, soit par l'intermédiaire des réseaux des opérateurs de communications électroniques. Il fait valoir que, dans cette seconde hypothèse, la coopération des opérateurs permettrait de prévenir toute atteinte au bon fonctionnement et à la sécurité de leurs réseaux ainsi qu'à la qualité du service rendu à leurs clients.

---

[12] L'article 706-102-1 du code de procédure pénale, dans sa rédaction issue de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, dispose en effet : « *Il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques. (...)* ».

La commission constate que l'évolution proposée a pour objet d'adapter la mise en œuvre opérationnelle des techniques prévues par les articles L. 851-6 et L. 853-2 du code de la sécurité intérieure aux évolutions technologiques des réseaux de téléphonie mobile et des modes de communication électronique. En l'état des éléments portés à sa connaissance, il n'apparaît pas que cette évolution augmente significativement l'atteinte portée à la vie privée des personnes pour la surveillance desquelles ces techniques sont susceptibles d'être autorisées.

Dans ces conditions, la commission émet un avis favorable aux modifications proposées par l'article 13 du projet de loi.

Délibéré en formation plénière le 7 avril 2021

Francis DELON

Président de la Commission nationale
de contrôle des techniques de renseignement