RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Commission nationale de contrôle des techniques de renseignement

CNCTR

6e Rapport d'activité 2021

SOMMAIRE

ANNEXES

Avant-propos

L'impact de la crise sanitaire sur l'activité de la Commission comme des services de renseignement s'est fortement atténué et 2021 a permis de retrouver un niveau proche de la période antérieure. Les données que l'on pourra consulter dans ce rapport le montrent. Elles mettent aussi en évidence la relative stabilité des éléments qui structurent cette activité.

L'une de ces données, particulièrement significative, est le nombre total des personnes qui ont été surveillées en utilisant les techniques de renseignement. Il reste à un niveau à peu près identique aux années précédentes (22 958 personnes ayant fait l'objet d'au moins une technique, contre 21 952 en 2020 et 22 210 en 2019).

De même, c'est la prévention du terrorisme qui continue à motiver la plus grande partie des demandes de techniques de renseignement, suivie de la prévention de la criminalité organisée. Toutefois, un facteur d'évolution déjà relevé dans le rapport pour 2019 a retenu toute l'attention de la Commission. C'est la part désormais substantielle (plus de 14%) prise par les demandes liées à la prévention des violences collectives. Peu spectaculaire du point de vue quantitatif, elle paraît cependant révéler des mutations sociales préoccupantes : d'un côté, de nouvelles formes d'activisme liées à l'adhésion croissante de certains individus à des thèses (survivalisme et autres) venues se substituer aux affinités idéologiques des siècles précédents ; de l'autre côté du spectre politique, la tentation, chez certains groupes pratiquant des formes « pacifiques » de désobéissance civile, de passer à des registres d'action plus radicale.

Face à une telle évolution, l'une des responsabilités cruciales et particulièrement délicates de la Commission est de faire la part entre, d'un côté, l'activisme politique, qui, à lui seul, ne saurait fonder l'emploi de techniques de renseignement, même lorsqu'il exprime et manifeste des idées extrémistes, et d'un autre côté, la nécessaire prévention des violences collectives, qui, elle, est un motif légitime de surveillance, y compris lorsque ces actions ont un fondement politique.

Réserve faite de ces quelques observations, l'année 2021 n'a pas connu d'évolutions majeures s'agissant de la mise en œuvre des techniques de renseignement. Elle a en revanche été marquée par de nouvelles et importantes modifications de leur encadrement législatif.

On trouvera dans le rapport une analyse détaillée de ces réformes transcrites pour l'essentiel dans la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Elles montrent à quel point le « droit du renseignement » est un chantier ouvert, voué à connaître d'autres évolutions, sous l'effet de plusieurs dynamiques concurrentes.

Une première dynamique est d'ordre structurel. Un cadre juridique qui, comme c'est le cas de la loi du 24 juillet 2015 relative au renseignement, ne s'en tient pas à l'énoncé de règles générales, mais s'attache à l'encadrement de techniques exhaustivement énumérées et précisément définies, doit nécessairement subir et accompagner l'impact des mutations que connaissent ces techniques. Elles sont particulièrement rapides, on le sait, dans le domaine des communications électroniques.

C'est ainsi que la nouvelle loi a dû prendre en compte, par exemple, l'impact de la 5G, ou le développement annoncé de constellations de satellites.

La deuxième dynamique, qui a connu des manifestations spectaculaires en 2021, vient de la jurisprudence des cours européennes. Elle est due en particulier à l'entrée en scène (que les États n'avaient guère anticipée) de la Cour de justice de l'Union européenne dans la définition d'un droit du renseignement qui lui échappait jusqu'à ce qu'elle s'en saisisse par le biais de la régulation des opérateurs de communications électroniques. Prenant alors appui sur la Charte des droits fondamentaux de l'Union, la Cour de justice a remis en cause dans son principe même la possibilité de conserver les données détenues par les opérateurs à des fins de police administrative et judiciaire.

Seul un dialogue nourri entre la Cour et le Conseil d'État français, par l'intermédiaire de questions dites « préjudicielles », a permis de trouver un nouvel équilibre. La contrepartie fut notamment un renforcement sensible des prérogatives combinées de la Commission (dont l'avis négatif pour l'usage d'une technique, simplement consultatif jusque-là, devient

bloquant) et du Conseil d'État (qui a désormais vocation à arbitrer en cas de désaccord entre la Commission et le Premier ministre). Cela ne devrait guère changer les pratiques – le Premier ministre s'est jusqu'ici toujours rangé aux avis défavorables de la Commission – mais marque une évolution vers une juridictionnalisation croissante du droit du renseignement.

Pendant ce temps, l'autre grande juridiction supranationale, la Cour européenne des droits de l'homme, poursuit sa démarche ambitionnant d'allier réalisme face aux exigences de sécurité et efficacité dans la protection des droits. Admettant la nécessité que les États développent leur capacité de défense, notamment dans le domaine de la surveillance et du renseignement, y compris en pratiquant une « surveillance de masse », considérant qu'elle n'a pas à interférer dans l'appréciation qui est la leur des moyens adéquats pour renforcer cette capacité, elle a, en contrepartie, entrepris au fil de ses décisions de construire une sorte de cahier des charges assurant l'existence de « garanties de bout en bout », quelles que soient les options nationales retenues par les États.

La décision *Big Brother Watch* s'inscrit dans cette dynamique jurisprudentielle. Demandant en particulier aux États que les pratiques consistant à partager des renseignements avec leurs homologues étrangers soient, dans un sens comme dans l'autre, assorties de garanties comparables à celles qui valent pour le recueil de renseignements par leurs propres services, elle n'a pas encore reçu de traduction dans la législation nationale.

Troisième dynamique, c'est bien le législateur national qui a choisi de sa propre initiative de renforcer les garanties applicables au partage de renseignements entre services français. Alors même que le Conseil constitutionnel avait jugé que les dispositions antérieures suffisaient à assurer le partage entre la loi et le règlement, la loi du 30 juillet 2021 a construit un régime nouveau, combinant procédure d'autorisation et de déclaration, qui vient renforcer dans une mesure encore difficile à déterminer les obligations des services et les responsabilités de la Commission.

Cette dernière ne peut que se féliciter de ce souci de perfectionnement du cadre protecteur des libertés. Mais elle se préoccupe aussi de la méthode mise en œuvre : ce n'est qu'une fois la réforme adoptée que l'on a entrepris de déterminer exactement son impact sur l'activité des

services, ainsi que sa compatibilité avec certaines pratiques antérieures essentielles à leur bon fonctionnement. Outre les conséquences de ce travail tardif sur les délais d'application de la loi nouvelle, la crainte est que ne se développent alors des dispositifs procéduriers sophistiqués, que les services n'avaient pas anticipés, et dont la Commission se verrait finalement reprocher la lourdeur, parce qu'il lui appartient de s'assurer que la loi nouvelle est pleinement, exactement et effectivement appliquée.

Aussi paraît-il très souhaitable qu'en cas de réforme, la Commission puisse être associée tout en amont à sa préparation, le Coordonnateur national du renseignement et de la lutte contre le terrorisme paraissant à même de fédérer cette préparation.

Sous la présidence de mon prédécesseur, Francis Delon, la Commission a su mettre en place avec une remarquable efficacité le dispositif d'autorisation prévu par la loi de 2015.

Il lui revient désormais de donner sa pleine efficience au contrôle *a posteriori* de l'usage des techniques : c'est l'alliance des deux temps du contrôle (*ex ante et a posteriori*) qui donne à la loi française sa force protectrice originale. Il convient à cet égard de construire une véritable stratégie des modes de contrôle.

Le contrôle « sur place », c'est-à-dire au contact direct des services de renseignement, est absolument indispensable car il permet à la fois d'éclairer tel aspect sensible ou complexe de leur activité, et de cultiver avec leurs agents une véritable relation de confiance. Toutefois, pour être pleinement efficaces, ces contrôles doivent être suffisamment sélectifs, bien ciblés et bien préparés. C'est pourquoi la Commission met l'accent sur un complément nécessaire, qui est le développement de ses capacités de contrôle à distance. C'est par la combinaison de ces deux modalités de contrôle, « sur place » et « en ligne », qu'elle peut inscrire son action dans un cercle vertueux, avec plusieurs effets utiles : économie de temps et de moyens, tout d'abord, grâce aux applications informatiques sécurisées qui lui permettent de vérifier, sans avoir à se déplacer, la régularité de certaines pratiques ; concentration des efforts, ensuite, sur les affaires qui méritent un suivi plus renforcé de sa part ; approfondissement du dialogue avec les services, enfin, en mettant à profit ses déplacements auprès d'eux, quelle que soit leur implantation sur le territoire national.

Or, cette dernière dimension importe d'autant plus que, on l'a dit, leur action s'exerce dans un paysage changeant, tant en ce qui concerne la nature des menaces que le cadre juridique de leur action. Ce dernier s'enrichit, devient plus protecteur et plus contraignant à la fois. Cette évolution se poursuivra. Dans ce contexte, le rôle de la Commission est non seulement d'accompagner sa mise en œuvre, mais aussi de vérifier que cette sophistication croissante ne conduit pas à une stratification des procédures. Ainsi paraît-il en particulier opportun d'envisager une revue régulière de ces procédures, qui soit fondée sur un bilan entre leur coût pour les services et leur apport à l'efficacité du contrôle, et permette, le cas échéant, d'envisager les simplifications légitimes.

Au moment où j'écris ces lignes, l'Europe renoue avec le tragique. La guerre met en cause sa sécurité. En même temps, le socle des libertés qu'elle a progressivement enrichi et consolidé est défié par certains, ébréché par d'autres. Ce sont des temps qui exigent plus que jamais une double efficacité : efficacité dans l'action des services chargés de la défense des intérêts fondamentaux de la Nation ; rigueur dans le respect des libertés, qu'il s'agisse de la protection de la vie privée ou de la liberté d'expression et d'opinion. La qualité des échanges entre la Commission et les services, combinant rigueur, fluidité et confiance sera déterminante.

Serge LASVIGNES

Conseiller d'État honoraire
Président de la CNCTR

Une modification de la composition de la CNCTR

Le collège de la CNCTR a connu un renouvellement de trois de ses membres en 2021.

Par décret du Président de la République en date du 27 septembre 2021, monsieur Serge LASVIGNES, conseiller d'État honoraire, nommé membre de la CNCTR par le vice-président du Conseil d'État, a été nommé président de cette commission.

Par ce même décret, monsieur Philippe DISTLER, ingénieur général des mines honoraire, a été nommé, sur proposition de la présidente de l'Autorité de régulation des communications électroniques et des postes, membre de la CNCTR en qualité de personnalité qualifiée pour ses connaissances en matière de communications électroniques.

En outre, madame Solange MORACCHINI, avocate générale honoraire à la Cour de cassation, a été nommée membre de la CNCTR conjointement par la première présidente et par le procureur général près la Cour de cassation.

Ces nominations ont pris effet à compter du 3 octobre 2021.

Ces trois nouveaux membres ont remplacé, respectivement, monsieur Francis DELON, conseiller d'État honoraire, président de la CNCTR, monsieur Patrick PUGES, personnalité qualifiée en matière de communications électroniques et madame Christine PÉNICHON, avocate générale honoraire à la Cour de cassation, dont les mandats étaient parvenus à leur terme.

À la fin de l'année 2021, le collège de la CNCTR était composé des neuf membres suivants :

- monsieur Serge LASVIGNES,
  conseiller d'État honoraire, président ;

- madame Chantal DESEYNE,
  sénatrice d'Eure-et-Loir ;

- monsieur Yannick VAUGRENARD,
  sénateur de la Loire-Atlantique ;

- madame Constance LE GRIP,
  députée des Hauts-de-Seine ;

- monsieur Jean-Michel CLÉMENT,
  député de la Vienne ;

- madame Françoise SICHLER-GHESTIN,
  conseillère d'État honoraire ;

- madame Solange MORACCHINI,
  avocate générale honoraire à la Cour de cassation ;

- monsieur Gérard POIROTTE,
  conseiller honoraire à la Cour de cassation ;

- monsieur Philippe DISTLER,
  personnalité qualifiée en matière de communications électroniques.

Le secrétariat général de la CNCTR se composait, à la même date, d'une secrétaire générale, d'un conseiller placé auprès du président de la commission, de onze chargés de mission et de quatre agents exerçant des missions de soutien.

Compte-rendu de l'activité de la CNCTR

1. Les modifications du cadre juridique en 2021 et les perspectives d'évolution : la CNCTR attentive à l'équilibre entre efficacité de l'action des services de renseignement et protection du droit au respect de la vie privée

1.1 Les modifications du cadre juridique intervenues en 2021 : une activité soutenue de conseil auprès du Gouvernement et du Parlement

1.1.1 La révision du cadre légal applicable au renseignement : une extension des compétences attribuées à la CNCTR

Le débat parlementaire sur le devenir de la technique expérimentale de l'algorithme, reporté en 2020 en raison de la crise sanitaire, a pu cette année avoir lieu.

L'examen de cette question a été l'occasion de dresser un bilan plus général du cadre juridique créé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement[1]. Près de six ans après son adoption, la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement[2] lui a apporté les ajustements nécessaires pour que les services de renseignement continuent de disposer de moyens

1 - Cette loi sera désormais mentionnée comme « la loi du 24 juillet 2015 ».

2 - Cette loi sera désormais mentionnée comme « la loi du 30 juillet 2021 ».

d'action adéquats et proportionnés face aux menaces, tout en renforçant les garanties qui s'appliquent à la mise en œuvre des techniques de renseignement.

La CNCTR a été saisie par le Premier ministre du projet[3] dont résultent les dispositions de la loi du 30 juillet 2021. Les délibérations n° 2/2021 du 7 avril 2021, n° 3/2021 du 14 avril 2021 et n° 4/2021 du 30 avril 2021 constituent les avis de la commission sur ces dispositions[4].

a) La modification et la pérennisation de la technique dite de l'« algorithme » prévue par l'article L. 851-3 du code de la sécurité intérieure

La loi du 30 juillet 2021 a précisé les conditions d'exécution des traitements automatisés et prévu l'extension aux « *adresses complètes de ressources utilisées sur internet* » du champ des données qui peuvent être utilisées en application de l'article L. 851-3. Elle a également pérennisé cette technique jusqu'ici autorisée à titre expérimental[5].

- Sur l'exécution des traitements automatisés

Lorsque les dispositions de l'article L. 851-3 du code de la sécurité intérieure sont entrées en vigueur le 3 octobre 2015, plusieurs modalités d'exécution des algorithmes avaient alors été étudiées par le Gouvernement, en concertation, notamment, avec les opérateurs de communications électroniques.

Par une lettre du 13 juillet 2016, le Premier ministre avait sollicité l'avis de la CNCTR sur un projet de dispositif expérimental consistant à dupliquer des flux sur les réseaux des opérateurs puis à les acheminer vers le groupement interministériel de contrôle (GIC), lequel se voyait chargé

3 - La saisine initiale adressée à la CNCTR le 8 mars 2021 a été complétée par deux saisines complémentaires datées des 7 et 26 avril 2021.

4 - Ces délibérations sont respectivement publiées en annexes n°1, n°2 et n°3 au présent rapport et sont disponibles sur le site Internet de la commission.

5 - Pour mémoire, cette technique avait été initialement autorisée jusqu'au 31 décembre 2018 par l'article 25 de la loi du 24 juillet 2015 relative au renseignement. Cette échéance a été reportée une première fois, à la demande du Gouvernement, au 31 décembre 2020 par la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, puis une seconde fois, au 31 décembre 2021 par 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, en raison de la crise sanitaire.

d'exécuter les traitements automatisés prévus par l'article L. 851-3 du code de la sécurité intérieure.

Dans sa délibération classifiée n°6/2016/SD du 28 juillet 2016, la commission avait estimé que ce dispositif n'était pas contraire à la loi. Elle avait 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 d'accéder aux données dupliquées puis stockées pour l'exécution des algorithmes ; les seules données susceptibles de leur être transmises devaient être celles qui déclenchent une alerte générée par l'algorithme et dont l'anonymat est préalablement levé par décision du Premier ministre prise après avis de la CNCTR ;
- le fonctionnement et la maintenance de l'ensemble du dispositif devaient être placés sous la responsabilité du GIC, service à compétence nationale du Premier ministre, qui n'est pas un service de renseignement. La CNCTR avait préconisé la mise en place de procédures devant notamment permettre la traçabilité des accès en tout point du dispositif. Elle avait recommandé que les administrateurs du système soient placés sous la seule autorité du GIC et sous le contrôle de la CNCTR. Les agents du GIC intervenant dans l'exécution du traitement automatisé devaient être individuellement habilités à cet effet, après avis de la CNCTR. En outre, la commission 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, soit strictement nécessaire pour permettre l'exécution des algorithmes ;
- enfin, la CNCTR avait recommandé au Premier ministre d'informer le Parlement des choix effectués pour l'expérimentation de cette technique, en précisant notamment que les traitements automatisés n'étaient pas exclusivement exécutés chez les opérateurs de communications électroniques.

L'ensemble de ces recommandations avaient été suivies par le Premier ministre. La CNCTR avait pu s'en assurer avant de donner, le 5 octobre 2017, un avis favorable à la première demande d'algorithme dont elle avait été saisie. Elle a depuis lors exercé un contrôle étroit sur le dispositif d'exécution des traitements automatisés qui n'a révélé aucune anomalie.

La loi du 30 juillet 2021 a tiré les enseignements de l'expérimentation menée sur cette technique ces cinq dernières années, en tenant compte des garanties dont la CNCTR avait exigé le respect en 2016 et du rôle exercé depuis lors par le GIC. Dans sa nouvelle rédaction résultant de cette modification législative, l'article L. 851-3 prévoit ainsi désormais que le GIC est « *seul habilité à exécuter les traitements et opérations mis en œuvre* (...)*, sous le contrôle de la Commission nationale de contrôle des techniques de renseignement* ».

La loi a par ailleurs limité 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[6].

- Sur l'utilisation des URL

Dans le rapport sur l'application de l'article L. 851-3 du code de la sécurité intérieure adressé au Parlement le 30 juin 2020 et dont la CNCTR a été rendue destinataire, le Gouvernement indiquait que les algorithmes mis en œuvre à cette date donnaient des résultats satisfaisants mais que leur utilisation pourrait être améliorée en y incluant, outre les données de connexion issues des communications téléphoniques, celles transitant par le réseau internet, dites « IP » (*internet protocol*), dont certaines URL (*uniform resource locator*). Il estimait 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.

Le Gouvernement entendait ainsi améliorer l'efficacité de la technique de l'algorithme en incluant « tous les types d'*URL* » parmi les données pouvant

6 - La commission renvoie, pour plus de précisions, au point 1.1.2 de sa délibération n°2/2021 du 7 avril 2021.

faire l'objet des traitements automatisés. Sont englobées dans cette catégorie de données à la fois celles 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 complètes de ressources sur internet* », qui peuvent quant à elles faire référence au contenu des informations consultées.

Dans sa délibération du 7 avril 2021, la CNCTR, après avoir constaté que la menace terroriste persistait à un niveau élevé et que le comportement d'auteurs d'actes de terrorisme était souvent caractérisé par une utilisation intensive d'internet, avait considéré que les besoins opérationnels des services de renseignement concernés, ainsi décrits par le Gouvernement, semblaient établis. Elle avait cependant estimé 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. Cette recommandation a été suivie par le Premier ministre et inscrite dans la lettre de la loi du 30 juillet 2021 qui fait ainsi référence aux seules « *adresses complètes de ressources utilisées sur internet* ».

- Sur la pérennisation de l'algorithme

La loi du 30 juillet 2021, en abrogeant 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, a pérennisé la technique de l'algorithme.

La CNCTR avait admis, dans son avis du 7 avril 2021, que les impératifs de sécurité nationale justifiaient que le dispositif de l'article L. 851-3 soit conservé. Elle avait également relevé que les modifications proposées pour encadrer l'exécution des traitements automatisés étaient de nature à renforcer les garanties applicables à ce dispositif et à limiter ainsi davantage les atteintes au droit au respect de la vie privée.

La commission avait cependant estimé souhaitable, compte tenu de la modification substantielle résultant de la possibilité d'utiliser les *URL*, de s'assurer, par une procédure d'évaluation, que l'atteinte portée à la vie privée soit effectivement justifiée par une meilleure protection contre le

risque terroriste. Suivant cette recommandation, le législateur a prévu que le Gouvernement adresse au Parlement un rapport sur l'application de l'article L. 851-3, au plus tard le 31 juillet 2024.

b) L'extension aux *URL* du champ des données pouvant être recueillies en temps réel sur le fondement de l'article L. 851-2 du code de la sécurité intérieure

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

Les nouvelles dispositions législatives ont inclus dans le champ des données pouvant faire l'objet de ce recueil en temps réel « *les adresses complètes de ressources sur internet utilisées* » par ces personnes et ont aligné 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. 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 législateur 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. Pour la CNCTR, ce choix constitue une garantie de nature à renforcer la protection de la vie privée et offre une contrepartie appropriée à l'extension aux URL du recueil autorisé par l'article L. 851-2.

Enfin, la loi a autorisé le recueil en temps réel des URL utilisées, non seulement par la personne ciblée à titre principal, mais par toute autre personne appartenant à son entourage. La commission, qui ne recommandait pas une telle extension, s'assurera que l'usage de cette faculté ne conduit pas à des atteintes disproportionnées au droit au respect de la vie privée de ces personnes.

c) Un pouvoir renforcé de la commission pour veiller à la bonne exploitation des données recueillies et aux conditions de leur partage entre les services

- L'exploitation des données recueillies : l'utilisation de données pour un autre motif que celui qui a justifié leur recueil initial

La loi autorise désormais expressément les services de renseignement à exploiter des données recueillies par la mise en œuvre d'une technique de renseignement alors qu'elles concernent d'autres motifs que ceux qui en avait permis la collecte.

L'article L. 822-3 du code de la sécurité intérieure prévoit ainsi que les services de renseignement peuvent transcrire ou extraire des renseignements « *utiles à la poursuite d'une finalité différente de celle qui a justifié le recueil* ». Le cas peut se présenter lorsque les renseignements recueillis au cours d'une surveillance révèlent des faits que le service concerné ne soupçonnait pas au moment où il avait formulé sa demande de technique de renseignement.

Une telle faculté n'est toutefois permise par la loi qu'à deux conditions :

- de tels renseignements ne peuvent être transcrits ou extraits que pour l'une des finalités relatives aux intérêts fondamentaux de la Nation qu'énumère limitativement l'article L. 811-3 de ce code ;
- leur exploitation doit uniquement s'inscrire dans l'exercice des missions du service mettant en œuvre la technique concernée.

Enfin, l'ensemble de ces opérations de transcription et d'extraction est placé sous le contrôle de la CNCTR. L'article L. 822-4 du même code prévoit, à cette fin, qu'outre la destruction des renseignements collectés par la mise en œuvre de techniques de renseignement, qui fait déjà l'objet de relevés tenus à la disposition de la commission, leur éventuelle transcription et extraction pour d'autres motifs que ceux en ayant permis le recueil doit également, et dans les mêmes conditions, donner lieu à l'établissement de relevés.

Dans son avis du 7 avril 2021, la CNCTR avait estimé que, si l'établissement de ces relevés était utile à l'exercice de son contrôle *a posteriori*, il

n'était pas suffisant pour garantir un contrôle effectif des conditions dans lesquelles les services de renseignement peuvent recourir à cette faculté particulière d'exploitation des données qu'ils recueillent. En effet, la commission n'a pas la capacité, lors des contrôles *a posteriori* auxquels elle procède, d'examiner la totalité des relevés établis par les services de renseignement. Pour exercer efficacement son contrôle sur ce type de transcriptions et d'extractions, elle a besoin d'en être spécialement informée par une transmission systématique et immédiate des relevés qui les concernent. Suivant cette recommandation, le législateur a prévu que la CNCTR, non seulement, dispose d'un accès permanent, complet et direct aux relevés de transcriptions et d'extractions effectuées pour une finalité différente, mais qu'elle en est aussi immédiatement destinataire.

■ Un cadre législatif pour le partage de renseignements entre services français

La loi du 30 juillet 2021 a défini les conditions dans lesquelles les services peuvent échanger des renseignements collectés, extraits ou transcrits par la mise en œuvre de techniques autorisées sur le fondement du livre VIII du code de la sécurité intérieure, y compris celles relatives à la surveillance des communications électroniques internationales.

Le partage de renseignements entre services français était antérieurement régi par les dispositions de l'article L. 863-2 du code de la sécurité intérieure qui prévoyait succinctement que les services de renseignement pouvaient « *échanger toutes les informations utiles à l'accomplissement de leurs missions* » et renvoyait à un décret en Conseil d'État la détermination des modalités et conditions d'application d'un tel régime. Ce décret n'a toutefois jamais été pris.

Les conditions de partage sont désormais définies par la loi. Le II de l'article L. 822-3 du code de la sécurité intérieure prévoit ainsi qu'un service de renseignement, qu'il s'agisse d'un service spécialisé de renseignement ou d'un autre service disposant d'une compétence en matière de renseignement, « *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 données brutes, mais également celle de transcriptions et extractions

issues de ces données. Elle trace cependant une limite aux échanges en interdisant qu'un service puisse se voir transmettre des renseignements relevant d'une finalité qui n'entre pas dans ses missions.

Dans deux cas particuliers, la transmission de renseignements à un autre service est subordonnée à la délivrance d'une autorisation préalable du Premier ministre après avis de la CNCTR :

- l'obtention de cette autorisation est nécessaire lorsqu'un service de renseignement souhaite transmettre des renseignements à l'état brut, c'est-à-dire avant tout traitement, à un service partenaire afin que ce dernier les exploite pour une finalité différente de celle qui en avait permis le recueil.
- elle est également requise pour la transmission 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 situation peut notamment se rencontrer lorsque le service destinataire appartient à la catégorie des services de renseignement du « second cercle », qui n'ont accès qu'à un nombre limité de techniques et de finalités.

La loi a par ailleurs déterminé les modalités de contrôle de ces échanges.

Outre 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, la loi a prévu qu'un contrôle externe soit assuré par la CNCTR.

L'article L. 822-4 du code de la sécurité intérieure prévoit à cet égard que les transmissions de renseignements font l'objet de relevés tenus à la disposition de la CNCTR qui précisent leur nature, leur date et leur finalité ainsi que le ou les services qui ont été destinataires des données transmises. Suivant la recommandation formulée par la commission, le législateur a également prévu que ces relevés lui soient immédiatement communiqués lorsque les transmissions poursuivent une finalité différente de celle au titre de laquelle la technique de renseignement a été autorisée. L'article L. 833-2 donne ensuite à la CNCTR un accès permanent, complet et direct à toutes

les transmissions de renseignements. Enfin, l'article L. 833-6 permet à la commission de recommander au Premier ministre, au ministre et au service concernés l'interruption de transmissions de renseignements lorsque celles-ci lui paraissent effectuées en méconnaissance de la loi.

La commission avait recommandé que, contrairement à ce que prévoyait le projet de loi, des garanties équivalentes soient prévus en cas de transmissions portant sur des renseignements issus de la surveillance des communications électroniques internationales. Cette recommandation a été prise en compte par la loi du 30 juillet 2021.

Les modalités d'application de ces nouvelles dispositions et les enjeux du contrôle confié à la CNCTR font l'objet de plus amples développements au point 2.2 du présent rapport.

d) La conservation de renseignements à des fins de recherche et développement

La loi du 30 juillet 2021 a prévu, aux articles L. 822-2 et L. 822-2-1 du code de la sécurité intérieure, que les services de renseignement et le GIC peuvent conserver des renseignements collectés au-delà des durées normalement applicables et jusqu'à cinq ans, à la seule fin de conduire des programmes de recherche et développement destinés à améliorer leurs capacités techniques de recueil et d'exploitation. Dans le projet transmis à la CNCTR, le Gouvernement avait justifié ces nouvelles dispositions par le besoin de mettre au point des outils dits d'« intelligence artificielle ». Il proposait, à travers ce dispositif dérogatoire de conservation, que de telles données puissent ainsi être stockées et utilisées pour entraîner, à des fins d'apprentissage automatique, des programmes informatiques spécialement dédiés aux activités de recherche et développement menées par ces services et par le GIC.

Suivant les recommandations formulées par la CNCTR dans sa délibération du 7 avril 2021, le législateur a rigoureusement encadré la mise en œuvre de ces nouvelles dispositions.

Il a, tout d'abord, restreint leur champ d'application aux seuls services spécialisés de renseignement, dits du « premier cercle », dont une partie seulement dispose à ce jour des compétences ainsi que des moyens techniques et humains nécessaires à la réalisation de programmes de recherche et développement.

Il a, ensuite, exclu toute utilisation de ces données à des fins de surveillance et précisé que ces dernières ne seront accessibles qu'aux seuls agents habilités pour cette mission de recherche et développement, à l'exclusion donc des agents chargés de l'exploitation et de l'analyse.

Enfin, le législateur a prévu que les paramètres techniques applicables à chaque programme de recherche, ainsi que toute modification substantielle de ces paramètres, doivent être soumis à une autorisation préalable du Premier ministre, délivrée après avis de la CNCTR. Dans sa délibération du 7 avril 2021, la commission avait interprété la notion de « programme de recherche » afin de délimiter les contours du contrôle qu'elle serait appelée à exercer dans ce domaine. Elle avait notamment indiqué que les demandes d'autorisation devraient renseigner les modalités précises de recueil, de conservation et d'utilisation des données dont la conservation pourrait être envisagée, la liste des agents habilités à les exploiter, les solutions retenues pour garantir que les personnes concernées ne puissent être identifiées, ainsi que la durée de conservation des données souhaitée en fonction des caractéristiques du programme.

La CNCTR avait, en outre, estimé souhaitable d'exercer un contrôle sur la mise en œuvre de ce dispositif dérogatoire de conservation des renseignements collectés et recommandé, à cette fin, que la loi précise qu'elle dispose d'un accès permanent, complet et direct à l'ensemble des données concernées. Cette mention a été intégrée aux dispositions de l'article L. 833-2 du code de la sécurité intérieure. Elle peut enfin adresser, à tout moment, au Premier ministre une recommandation tendant à la suspension ou à l'interruption d'un programme de recherche dont elle estime qu'il ne respecte plus les conditions posées par la loi.

e) La fusion des techniques de recueil et de captation de données informatiques prévues par l'article L. 853-2 du code de la sécurité intérieure

Le projet de loi transmis pour avis à la CNCTR proposait d'aligner la durée d'autorisation de la technique de recueil de données informatiques, alors fixée à trente jours, sur celle de la technique de captation de données informatiques, fixée à deux mois.

Dans sa délibération du 7 avril 2021, la commission avait émis un avis favorable à cette modification relevant, au demeurant, que le régime de conservation des renseignements collectés était le même pour les deux techniques.

Elle avait, en outre, suggéré, 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[7]. Suivant cette recommandation, le législateur a procédé à la fusion de ces deux techniques au I de l'article L. 853-2 du code de la sécurité intérieure.

f) 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

La loi du 30 juillet 2021 a étendu 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 aux recueils de données techniques de connexion par dispositifs de proximité dits « *IMSI catcher* » prévus par l'article L. 851-6 du même code ainsi qu'aux techniques de recueil et de captation de données informatiques prévus par l'article L. 853-2 de ce code. Cette liste était jusqu'alors 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).

Cette modification était notamment justifiée par les difficultés opérationnelles que le déploiement des réseaux mobiles de 5e génération, dits « 5G », pourrait entraîner et par la nécessité de prévenir toute atteinte au bon fonctionnement et à la sécurité des réseaux des opérateurs ainsi qu'à la qualité du service rendu à leurs clients.

7 - 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* (…) ».

Cette adaptation aux évolutions technologiques des réseaux de téléphonie mobile et des modes de communication électronique avait donné lieu à un avis favorable de la CNCTR dès lors qu'il n'apparaissait pas qu'elle augmente l'atteinte portée à la vie privée des personnes susceptibles d'être concernées.

g) La création, à titre expérimental, d'une nouvelle technique de renseignement autorisant l'interception des correspondances émises ou reçues par la voie satellitaire

La loi du 30 juillet 2021 offre désormais aux services de renseignement la faculté d'intercepter eux-mêmes, grâce à un dispositif de captation spécifique, des correspondances émises ou reçues par la voie satellitaire, sans avoir à solliciter le concours des opérateurs de communications concernés.

Le développement, à court et moyen termes, des communications empruntant la voie satellitaire, rendu prévisible par le déploiement actuel de nouvelles constellations de satellites conçus pour cet usage, a nécessité l'élaboration d'un cadre juridique adapté pour les activités de renseignement. En effet, les opérateurs concernés étant à ce jour tous étrangers, l'autorité administrative peut rencontrer des difficultés à obtenir leur coopération dans le cadre du droit commun des interceptions de correspondances applicable en France, voire renoncer à solliciter leur concours pour la surveillance des communications de certaines personnes ciblées par les services de renseignement.

Un dispositif propre aux interceptions satellitaires a ainsi été inscrit dans un nouvel article L. 852-3 du code de la sécurité intérieure. Suivant l'essentiel des recommandations formulées par la CNCTR dans sa délibération n° 3/2021 du 14 avril 2021, le législateur l'a soumis à un encadrement strict.

Il consacre, en premier lieu, le régime fixé par l'article L. 852-1 du code de la sécurité intérieure, qui repose sur le concours de l'opérateur de communications électroniques concerné pour réaliser l'interception, comme le régime de droit commun applicable en la matière. Ce n'est donc qu'à titre subsidiaire, lorsque ce concours n'est pas possible, que l'interception de communications satellitaires peut être réalisée par des

moyens techniques opérés par les services de renseignement eux-mêmes. À cet égard, la CNCTR avait préconisé que des modifications soient apportées au code des postes et des communications électroniques (CPCE) visant à préciser les obligations pesant sur les opérateurs étrangers et rendre plus aisée leur éventuelle réquisition en vue de mettre en œuvre l'interception de correspondances satellitaires dans les conditions de droit commun.

La nouvelle technique d'interception de correspondances est, en deuxième lieu, soumise à un contingentement : le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum fixé par le Premier ministre après avis de la CNCTR. Dans sa délibération du 14 avril 2021, la CNCTR avait considéré que ce contingent devrait être rigoureusement limité.

En troisième lieu, le recours à cette technique est, comme l'avait préconisé la commission, réservé aux seules finalités prévues aux 1°, 2°, 4° et 6° de l'article L. 811-3 du code de la sécurité intérieure, soit respectivement :

- l'indépendance nationale, l'intégrité du territoire et la défense nationale ;
- 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 ;
- la prévention du terrorisme ;
- et la prévention de la criminalité et de la délinquance organisées.

En quatrième lieu, par dérogation au régime de droit commun des techniques de renseignement qui prévoit que la durée maximale de leur mise en œuvre est de quatre mois[8], la loi du 30 juillet 2021 a limité cette durée à trente jours s'agissant des interceptions satellitaires. Suivant la recommandation de la CNCTR, le délai maximal de conservation des données recueillies se rapportant à la personne surveillée a également été restreint à trente jours. La loi a, en outre, prévu que les correspondances interceptées sont détruites dès qu'il apparaît qu'elles sont sans lien avec la personne concernée par l'autorisation et au plus tard dans un même

8 - En application de l'article L. 821-4 du code de la sécurité intérieure. Cette durée, éventuellement renouvelable, est applicable, sauf restriction particulière, aux autorisations d'interception de sécurité délivrées sur le fondement du I de l'article L. 852-1.

délai de trente jours. Ces délais, particulièrement courts, présentent une garantie renforcée pour la protection du secret des correspondances.

La loi a, en cinquième lieu, confié au GIC la mission d'organiser la centralisation des données recueillies et imposé que les opérations de transcription et d'extraction des communications interceptées soient réalisées dans les locaux de ce dernier. Elle a en outre précisé que la CNCTR dispose d'un accès permanent, complet, direct et immédiat à l'ensemble de ces opérations.

Enfin, ce dispositif a été créé à titre expérimental. Les dispositions concernées sont en effet applicables jusqu'au 31 juillet 2025. Le Gouvernement devra adresser au Parlement un rapport d'évaluation sur l'application de ces dispositions au plus tard six mois avant cette échéance.

Le législateur n'a pas retenu la recommandation de la CNCTR tendant à réserver aux seuls services spécialisés de renseignement, dits du « premier cercle », la participation à l'expérimentation. L'article L. 852-3 du code de la sécurité intérieure prévoit en effet que les services de renseignements dits du « second cercle », qui sont désignés par un décret en Conseil d'État pris après avis de la commission, pourront également y prendre part.

h) Les modifications résultant d'amendements parlementaires

Deux modifications ont, par ailleurs, été introduites par amendement au cours du débat parlementaire. Ces deux évolutions reprennent des propositions que la CNCTR avait formulées dans son troisième rapport d'activité pour l'année 2018[9] afin de renforcer la cohérence du cadre juridique applicable au renseignement.

La première modification a consisté à harmoniser la durée maximale de conservation des données collectées par les dispositifs de captation de paroles et ceux de captation d'images prévus à l'article L. 853-1 du code de la sécurité intérieure.

9 - Voir en particulier le point 1.2.2 de ce rapport.

Les durées maximales de conservation fixées aux 1° et 2° de l'article L. 822-2 du code de la sécurité intérieure, étaient alors de :

- trente jours à compter de leur recueil, pour les paroles prononcées à titre privé ;
- cent-vingt jours à compter de leur recueil, pour les images captées dans un lieu privé.

Dans son troisième rapport d'activité, la CNCTR avait considéré que le caractère éventuellement plus intrusif d'une technique par rapport à l'autre ne justifiait pas une distinction entre les durées maximales de conservation des données recueillies. Par ailleurs, elle avait souligné que cette distinction s'était révélée, à l'usage, problématique pour les services de renseignement, qui avaient parfois recours à des dispositifs captant à la fois les images et les paroles. Une exploitation différenciée des deux types de données collectées paraissait alors artificiellement contraignante.

Le législateur a choisi d'harmoniser la durée de conservation de ces deux techniques sur la durée la plus longue, c'est-à-dire cent-vingt jours.

La seconde modification a consisté à simplifier la procédure de contrôle préalable des demandes destinées à retirer ou à effectuer la maintenance de dispositifs de surveillance installés à l'intérieur d'un domicile.

Jusqu'ici, l'introduction d'agents des services de renseignement dans un lieu privé pour y mettre en place, utiliser ou retirer certains dispositifs de surveillance devait être autorisée par la formation collégiale, restreinte ou plénière, de la CNCTR lorsque le lieu était à usage d'habitation.

L'examen en formation collégiale, c'est-à-dire avec des garanties procédurales renforcées, des demandes d'introduction dans un lieu d'habitation pour y mettre en place ou y utiliser des dispositifs de surveillance est pleinement justifié. Cette procédure paraît en revanche inadaptée aux demandes qui ont pour seul but le retrait ou la maintenance de tels dispositifs. L'atteinte essentielle à la vie privée de la personne concernée a lieu au moment de l'installation d'un dispositif. En revanche, lorsque le service souhaite reprendre son matériel, la commission ne peut, dans les faits, qu'émettre un avis favorable puisque le retrait du dispositif de surveillance bénéficie à la vie privée de la personne intéressée.

Le législateur a, en conséquence, prévu que de telles demandes puissent être examinées, non plus par la formation collégiale, mais par l'un de ses membres ayant la qualité de magistrat et statuant seul.

Dans son troisième rapport d'activité, la CNCTR avait relevé que cette évolution permettrait à la procédure de gagner en rapidité. Un membre seul dispose en effet de vingt-quatre heures pour se prononcer, tandis que le collège de la commission peut statuer dans un délai de soixante-douze heures. Elle soulignait, en outre, que les formations collégiales de la CNCTR pourraient se concentrer davantage sur les demandes nécessitant une réelle délibération pour apprécier la proportionnalité de l'atteinte portée à la vie privée.

Cette faculté a été inscrite par la loi du 30 juillet 2021 à l'article L. 853-3 du code de la sécurité intérieure. L'article L. 832-3 du code prévoit, lui, que la formation plénière est informée des avis rendus sur le fondement de ces nouvelles dispositions lors de sa plus proche réunion.

1.1.2 Les adaptations du droit interne aux exigences de la Cour de justice de l'Union européenne : une nouvelle force des avis émis par la CNCTR

a) Le contexte créé par l'arrêt *Tele2 Sverige AB*

Dans un arrêt du 21 décembre 2016 dit *Tele2 Sverige AB*[10], la Cour de justice de l'Union européenne (CJUE) réunie en grande chambre, avait jugé, alors que quinze États membres[11] et la Commission elle-même étaient expressément intervenus en sens inverse et contrairement, en outre, au sens des conclusions de son avocat général, que le droit de l'Union[12] s'opposait à une « *réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au*

10 - CJUE, grande chambre, 21 décembre 2016, Tele2 Sverige AB c/ Post-och telestyrelsen, affaire C-203/15.

11 - Il s'agit des gouvernements suédois, britannique, belge, tchèque, danois, allemand, estonien, irlandais, espagnol, français, chypriote, hongrois, néerlandais, polonais et finlandais.

12 - Plus précisément l'article 15 paragraphe 1 de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, interprété à la lumière des stipulations de la Charte des droits fondamentaux de l'Union européenne.

trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ».

Cet arrêt condamnait ainsi potentiellement les législations de tous les États membres obligeant les opérateurs de communications électroniques et les fournisseurs de services en ligne à conserver, même pendant une durée limitée, des données de connexion de tous leurs abonnés, en vue de leur éventuelle réquisition par l'autorité judiciaire, par diverses autorités administratives investies de pouvoirs d'enquête[13] ou encore par les services de renseignement.

Eu égard aux difficultés soulevées, tant pour la conduite des enquêtes judiciaires que pour la recherche de renseignement, l'arrêt a suscité des inquiétudes parmi les autorités et professionnels concernés dans la plupart des États membres.

En France, plus de 2 millions de réquisitions judiciaires transitent chaque année par la plateforme nationale des interceptions judiciaires[14], auxquelles les opérateurs de téléphonie mobile et les fournisseurs d'accès à Internet répondent le plus souvent en quelques minutes, pour les besoins de plus de quatre enquêtes judiciaires sur cinq et, parmi elles, de 100 % des investigations en matière de criminalité et délinquance en bande organisée. Ce sont aussi plus de 50 000 demandes des services de renseignement autorisées par le Premier ministre après avis de la CNCTR, donnant lieu à la réquisition de centaines de milliers de données par l'intermédiaire du Groupement interministériel de contrôle (GIC)[15] aux fins de défendre et promouvoir les intérêts fondamentaux de la Nation[16].

13 - Telles que l'administration fiscale ou la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI), intégrée au sein de l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) depuis le 1er janvier 2022.

14 - Selon les chiffres communiqués par le Gouvernement, 1,8 millions en 2017, 2,2 millions en 2018, 2,4 millions en 2019 et 2,5 millions en 2020.

15 - Le GIC est un service à compétence nationale du Premier ministre chargé de centraliser les demandes d'autorisation de mise en œuvre des techniques de renseignement. Il a l'exclusivité de la relation avec les opérateurs de communications électroniques et les fournisseurs de services sur Internet pour recueillir les données que ces derniers traitent, en application des autorisations prononcées. Il met ensuite ces données à la disposition des services de renseignement grâce à un maillage territorial étendu et contrôle leur exploitation.

16 - Il s'agit des intérêts fondamentaux énumérés par l'article L. 811-3 du code de la sécurité intérieure, à savoir : 1° l'indépendance nationale, l'intégrité du territoire et la défense nationale ; 2° 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 ; 3° les intérêts économiques, industriels et scientifiques majeurs de la France ; 4° la prévention du terrorisme ; 5° la prévention : a) des atteintes à la forme républicaine des institutions ; b) des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; c) des violences collectives de nature à porter gravement atteinte à la paix publique ; 6° la prévention de la criminalité et de la délinquance organisées ; 7° la prévention de la prolifération des armes de destruction massive.

L'impact de cet arrêt ne se limitait pas aux autorités, judiciaires ou administratives, sollicitant l'accès aux données de connexion conservées par les opérateurs. Les autorités nationales chargées du contrôle de ces accès étaient également concernées. La CJUE avait en effet jugé qu'il était « *essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante* » dont la décision est dotée d'un effet contraignant et ajoutait qu'« *en tout état de cause, les États membres doivent garantir le contrôle, par une autorité indépendante, du respect du niveau de protection garanti par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel (...)* ».

b) Les réactions des États : inviter la CJUE à reconsidérer sa position

Les juridictions nationales ont accueilli cette jurisprudence avec une réserve marquée. À l'occasion de litiges pendants devant eux, le Conseil d'État français[17], la Cour constitutionnelle belge et la juridiction britannique chargée de contrôler les activités de renseignement[18] ont ainsi saisi la CJUE de questions préjudicielles afin de l'inviter à réexaminer la solution retenue dans l'arrêt *Tele2 Sverige AB* à la lumière de considérations tirées de la gravité et du caractère diffus des menaces pouvant peser sur les États membres[19].

17 - Il s'agit de la plus haute juridiction de l'ordre administratif.

18 - Il s'agit de l'*Investigatory Powers Tribunal*.

19 - Avant même l'arrêt *Tele2 Sverige AB*, la Cour provincial de Tarragone (Espagne) avait saisi la CJUE, en avril 2016, d'une question préjudicielle présentée dans le cadre d'un recours introduit par le ministère public espagnol contre la décision du juge d'instruction n°3 de Tarragone portant refus d'autoriser l'accès de la police judiciaire à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques. La Cour a répondu à cette question dans l'arrêt : CJUE, grande chambre, 2 octobre 2018, *Ministerio Fiscal*, affaire C-207/16. Postérieurement à l'arrêt *Tele2 Sverige A*, la Cour suprême d'Estonie (Riigikohus) a également saisi la CJUE, au mois de novembre 2018, d'une question préjudicielle à l'occasion d'une procédure pénale engagée contre « H. K. » des chefs de vol, d'utilisation de la carte bancaire d'un tiers et de violence à l'égard de personnes participant à une procédure en justice. La Cour a répondu à cette question dans l'arrêt : CJUE, grande chambre, 2 mars 2021, *H.K c/ Prokuratuur*, affaire C-746/18. Une autre question préjudicielle lui avait été adressée par la Cour suprême d'Irlande (Supreme Court) dans le cadre d'une procédure civile visant à contester certaines dispositions de la législation nationale concernée régissant la conservation de données relatives au trafic et de localisation par les fournisseurs de services de communications électroniques. La CJUE y a répondu dans l'arrêt : CJUE, grande chambre, 5 avril 2022, *Commissioner of the Garda Síochána e.a.*, affaire C-140/20. À la connaissance de la CNCTR deux questions préjudicielles sont par ailleurs toujours pendantes devant la CJUE. L'une introduite par la Cour administrative fédérale allemande (Bundesverwaltungsgericht) en matière de renseignement. L'autre introduite par la Cour de cassation française en matière d'accès aux données de connexion par l'Autorité des marchés financiers.

Une question préjudicielle est, en application de l'article 267 du traité sur le fonctionnement de l'Union européenne (TUE), une demande d'éclaircissement que les juridictions nationales adressent à la CJUE lorsque, au cours d'un litige, survient une difficulté d'interprétation du droit de l'Union, dont dépend la solution du litige.

En l'espèce, le droit de l'Union avait déjà été interprété de manière claire par l'arrêt *Tele2 Sverige AB* de la CJUE. Ces questions préjudicielles s'appuyaient dès lors sur une conception originale du dialogue des juges, selon laquelle des juridictions nationales confrontées aux difficultés d'application d'une jurisprudence de la CJUE renvoient à celle-ci une question déjà tranchée dans l'espoir que la Cour réexamine sa position.

En France, le Conseil d'État a décidé, au mois de juillet 2018, de poser plusieurs questions préjudicielles de cette nature à la CJUE, à l'occasion de deux séries d'instances dans lesquelles des associations de défense des libertés sur Internet telle que « *La Quadrature du Net* » attaquaient, d'une part, les décrets définissant les données de connexion devant être conservées par les opérateurs de communications électroniques et les fournisseurs de services en ligne et, d'autre part, les cinq principaux décrets d'application de la loi du 24 juillet 2015 relative au renseignement.

En ce qui concerne l'obligation de conservation généralisée et indifférenciée de données de connexion, le Conseil d'État avait alors rappelé :

- l'utilité « sans équivalent » de cette conservation pour l'autorité judiciaire ;
- la circonstance que, selon la CJUE elle-même, cette conservation, qui ne révèle pas le contenu des communications, ne porte pas « atteinte au 'contenu essentiel' » du droit au respect de la vie privée ;
- la reconnaissance, par l'article 6 de la Charte des droits fondamentaux de l'Union européenne, du droit à la sûreté ;
- les garanties et le contrôle entourant l'accès aux données conservées ;
- les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres selon l'article 4 du traité sur l'Union européenne.

Il avait, en conséquence, demandé à la CJUE si l'obligation de conservation généralisée et indifférenciée ne devait pas être regardée comme une ingérence justifiée par le droit à la sûreté et les exigences de la sécurité nationale.

En ce qui concerne les techniques de renseignement, le Conseil d'État avait reconnu l'applicabilité du droit de l'Union européenne en litige aux seules techniques de renseignement mettant en œuvre des dispositions régissant les activités des opérateurs de communications électroniques et celles des fournisseurs de services en ligne. Il s'agissait, selon lui, des recueils de données de connexion en temps différé, des recueils de données de connexion en temps réel, des algorithmes traitant des données de connexion et des géolocalisations en temps réel[20].

Après avoir fait valoir « l'utilité opérationnelle sans équivalent » des données de connexion pour les services de renseignement, notamment face au risque terroriste, le Conseil d'État avait posé trois questions à la CJUE.

La première portait à nouveau sur la conservation généralisée et indifférenciée des données de connexion, en tant qu'elle permet aux services de renseignement de recueillir ces données. La deuxième portait sur la compatibilité avec le droit de l'Union de techniques de renseignement qui, tout en affectant les droits et obligations des opérateurs et fournisseurs, ne leur imposaient pas d'obligations spécifiques de conservation des données. La troisième portait sur la nécessité de prévoir une procédure d'information des personnes surveillées, une fois que cette information ne peut plus compromettre l'enquête[21].

20 - Ces techniques sont respectivement codifiées aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure.

21 - Le Conseil d'État avait concomitamment jugé que ni la conservation généralisée et indifférenciée des données de connexion, ni l'absence d'information des personnes surveillées ne méconnaissaient, par elles-mêmes, la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, notamment ses stipulations garantissant le droit au respect de la vie privée et le droit au recours effectif. Le Conseil d'État avait ainsi estimé que la jurisprudence de la Cour européenne des droits de l'homme permettait, eu égard à l'ensemble des garanties présentées par la législation française, les ingérences dans les droits fondamentaux que la CJUE avait déclarées dans tous les cas disproportionnées dans son arrêt *Tele2 Sverige AB*.

c) Les réponses apportées par la CJUE

Par deux arrêts[22] du 6 octobre 2020, la CJUE, réunie en grande chambre, a répondu aux questions préjudicielles que lui avaient posées les juridictions belge, britannique et française.

C'est l'arrêt *La Quadrature du Net et autres* qui livre les apports essentiels des réponses apportées par la grande chambre de la Cour et qui couvre le plus largement l'éventail des questions qui lui avaient été soumises.

Sans revenir sur le principe d'interdiction d'une conservation généralisée et indifférenciée des données de connexion, la Cour a admis l'importance des objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave, qui contribuent à la protection des droits et libertés d'autrui[23]. Elle a toutefois précisé que les mesures dérogatoires aux principes de confidentialité et d'effacement ou d'anonymisation des données devaient s'interpréter strictement et ne sauraient devenir la règle[24].

Après avoir posé ce cadre général, la Cour a élaboré un raisonnement conçu comme un tableau de concordance entre, d'une part, le niveau de gravité de l'ingérence que constitue l'obligation de conservation, selon le triptyque : « non grave », « grave », « particulièrement grave » et, d'autre part, la gravité de la menace qui justifie cette ingérence, selon le triptyque : « lutte contre la criminalité et prévention des menaces contre la sécurité publique en général», « lutte contre la criminalité grave et prévention des menaces graves pour la sécurité publique » et enfin « sauvegarde de la sécurité nationale ».

La Cour a ensuite appliqué cette grille de lecture à trois catégories de données de connexion distinctes.

Elle a considéré, en premier lieu, que les données relatives à l'identité civile des utilisateurs ne présentent qu'une très faible sensibilité, de sorte que leur conservation constitue une ingérence non grave. L'obligation de

22 - Il s'agit, d'une part, de l'arrêt *Privacy International* (affaire C-623/17) rendu sur les questions préjudicielles britanniques et, d'autre part, de l'arrêt *La Quadrature du Net et autres* (affaires C-511/18, C-512/18 et C-520/18) rendu sur les questions préjudicielles belges et françaises.

23 - Voir le point 122 de l'arrêt *La Quadrature du Net et autres*.

24 - Voir le point 111 du même arrêt.

conservation des données de cette nature peut dès lors être ordonnée, sans limitation de durée, pour les trois objectifs précédemment énumérés.

Elle a considéré, en deuxième lieu, que les adresse IP[25] sont des données plus sensibles que les précédentes et a qualifié l'ingérence dans les droits fondamentaux de « grave ». Elle en a conclu que la conservation générale et indifférenciée des adresses IP attribuées à la source d'une connexion n'est pas interdite en soi mais doit être réservée aux deux motifs les plus graves que sont la lutte contre la criminalité grave et la sauvegarde de la sécurité nationale, et limitée à une durée strictement nécessaire.

Enfin, pour toutes les autres données de connexion (c'est-à-dire, les données de trafic et les données de localisation), le principe demeure celui de l'interdiction de la conservation obligatoire à des fins de sécurité. Mais la Cour a modulé ce principe en fonction du motif poursuivi.

S'agissant de la lutte contre les infractions pénales ordinaires, le principe ne connaît pas d'exception[26].

S'agissant de la lutte contre la criminalité grave et la prévention des menaces graves pour la sécurité publique, la conservation généralisée et indifférenciée[27] est regardée comme excédant les limites du strict nécessaire et non justifiée dans une société démocratique. La Cour a toutefois envisagé deux exceptions :

- la première, déjà présente dans l'arrêt *Tele2*, est la conservation ciblée selon des critères personnel et géographique ;
- la seconde, qui est une innovation de l'arrêt *La Quadrature du net et autres*, est la conservation dite « rapide ». Cette notion, tirée de l'article 16 de la convention de Budapest sur la cybercriminalité

25 - L'adresse IP correspond au numéro unique attribué de façon permanente ou provisoire par le serveur du réseau à l'appareil qui accède à Internet.

26 - Seules les données d'identification peuvent ainsi donner lieu à une obligation de conservation pour ce motif.

27 - des données autres que celles d'identification.

du 23 novembre 2001[28] ratifiée ou approuvée par la quasi-totalité des États membres dont la France, signifie un gel immédiat des données[29].

S'agissant enfin de la sauvegarde de la sécurité nationale, la Cour a considéré, à la différence de l'analyse retenue dans l'arrêt *Tele2*, que la gravité de cette menace est telle que l'on puisse autoriser une obligation de conservation généralisée et indifférenciée de l'ensemble des données de connexion, sous réserve toutefois que trois conditions soient réunies :

- d'une part, il doit exister une menace grave, réelle et actuelle ou simplement prévisible pour la sécurité nationale ;
- d'autre part, la durée de l'obligation de conservation doit être limitée au strict nécessaire. La Cour précise que si son renouvellement « ne peut être exclu » en cas de persistance de la menace grave, elle ne saurait présenter un « caractère systématique »[30] ;
- enfin, une telle obligation doit être soumise au contrôle d'un juge ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant, qui vérifiera l'existence et la gravité de la menace, ainsi que le respect de conditions et garanties contre les abus.

Enfin, sur la question de l'information des personnes surveillées, la Cour a considéré que les autorités nationales devaient informer les personnes ayant fait l'objet d'une technique de renseignement « pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent à ces autorités »[31].

28 - La convention définit les données relatives au trafic comme « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ».

29 - La convention de Budapest fait obligation aux États de prévoir cette conservation rapide pour une durée maximale de 90 jours, éventuellement renouvelable, non seulement pour prévenir (son préambule indique que la convention « est nécessaire pour prévenir les actes » visés, « en facilitant la détection, l'investigation et la poursuite »), rechercher et poursuivre les infractions relevant de la cybercriminalité, mais, plus largement, pour sauvegarder les preuves électroniques de toute infraction pénale. Il résulte du c. du 2. de l'article 14 de la convention que la conservation rapide peut permettre la collecte des preuves électroniques de toute infraction pénale (et non pas seulement les infractions commises au moyen d'un système informatique ou relevant de la cybercriminalité au sens des articles 2 à 11 de la convention).

30 - Voir le point 138 de l'arrêt *La Quadrature du Net et autres*.

31 - Voir le point 190 de l'arrêt *La Quadrature du Net et autres*.

d) Les conséquences tirées en France des arrêts de la CJUE, une fois leur portée précisée par le Conseil d'État

Le 21 avril 2021, l'Assemblée du contentieux[32] du Conseil d'État s'est prononcée, dans une décision intitulée « *French data network et autres* »[33] sur les conséquences à tirer de l'arrêt rendu par la CJUE le 6 octobre 2020.

La plupart des cours suprêmes des États membres ont développé des mécanismes de contrôle, souvent qualifiés de « contre-limites » destinés à circonscrire la portée du principe de primauté du droit de l'Union afin de garantir le respect des dispositions du droit national ayant permis l'adhésion à l'Union ou de sauvegarder les valeurs fondamentales de leur ordre juridique national. En résumé, ces mécanismes peuvent être regroupés en deux types de contrôle : d'une part, le contrôle *ultra vires*, qui permet au juge national de faire obstacle à l'application d'une norme du droit de l'Union qui outrepasserait les compétences attribuées à l'Union européenne et, d'autre part, le contrôle de « l'identité constitutionnelle », qui conduit le juge national à écarter une norme européenne qui porterait atteinte aux exigences constitutionnelles de son ordre juridique interne.

Alors que le Gouvernement français l'y invitait à titre principal, l'Assemblée du contentieux du Conseil d'État a refusé de s'engager dans un contrôle *ultra vires*. Elle a, en revanche, appliqué un contrôle proche de celui de l'identité constitutionnelle consistant à s'assurer que la mise à l'écart du droit national au motif de sa contrariété au droit de l'Union n'aurait pas pour effet de priver de garanties effectives une exigence constitutionnelle.

Les exigences constitutionnelles invoquées par le Gouvernement français pour justifier la conservation des données de connexion étaient, en l'espèce, les objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme[34].

32 - Il s'agit de la formation de jugement la plus solennelle du Conseil d'État qui statue sur les affaires dont l'importance exceptionnelle (appréciée au regard de la portée juridique de la décision à rendre) justifie cette formation du plus haut niveau. Elle comprend 17 membres.

33 - Il s'agit de la décision rendue sur les requêtes nos 393099, 39492, 397844, 397851, 424717 et 424718. Cette décision est publiée en annexe n°4 au présent rapport.

34 - Exigences que l'on peut résumer par la formule « exigences constitutionnelles de sécurité ».

Après avoir retenu l'absence d'équivalence entre les principes européens et nationaux au motif que le domaine en cause échappait à la compétence de l'Union, puis jugé que la conservation générale et indifférenciée des données de connexion était nécessaire à la garantie effective des exigences constitutionnelles invoquées, le Conseil d'État a néanmoins considéré qu'une application bienveillante du cadre européen au droit national suffisait à ne pas remettre en cause ces exigences.

Le Conseil d'État a, en effet, estimé que la plupart des dispositions contestées étaient conformes au droit de l'Union. Il a écarté et annulé celles qu'il a estimées contraires au cadre européen après s'être assuré qu'il ne privait pas, ce faisant, les « exigences constitutionnelles de sécurité » de garanties effectives.

S'agissant de l'obligation de conservation généralisée et indifférenciée, le Conseil d'État a constaté que la France était confrontée à une menace pour sa sécurité nationale, appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation énumérés à l'article L. 811-3 du code de la sécurité intérieure, qui par son intensité revêtait un caractère grave et réel et qui était, à la date de sa décision, non seulement prévisible mais aussi actuelle. Il a fondé ce constat non seulement sur la persistance de la menace terroriste, mais également sur les risques d'espionnage et d'ingérence étrangère, et a relevé une augmentation de l'activité de groupes radicaux et extrémistes. Il en a conclu que l'état des menaces pesant sur la sécurité nationale était de nature à justifier l'obligation de conservation généralisée et indifférenciée des données de connexion.

Le Conseil d'État a, en revanche, annulé les dispositions contestées en tant qu'elles ne prévoyaient pas un réexamen périodique de l'existence de la menace pour la sécurité nationale et a enjoint au Gouvernement de modifier en ce sens ces dispositions dans un délai de six mois à compter de sa décision.

S'agissant de l'accès des autorités nationales aux données de connexion conservées, le Conseil d'État a rappelé que la CJUE exigeait que cet accès soit soumis, sauf en cas d'urgence dûment justifiée, à un contrôle préalable par une juridiction ou une autorité administrative indépendante dotée d'un pouvoir contraignant. Il a constaté, en l'espèce, que la mise en œuvre des

techniques de renseignement en litige, dont celles permettant aux services de renseignement de solliciter l'accès aux données de connexion conservées par les opérateurs, ne respectait pas ces exigences puisque la CNCTR n'émettait qu'un avis simple ou des recommandations non contraignantes et que la saisine du Conseil d'État ne lui était ouverte qu'après que le Premier ministre avait délivré l'autorisation, et il a dès lors annulé dans cette mesure les dispositions contestées. Après avoir relevé que, dans les faits, le Premier ministre n'avait jamais accordé une autorisation après un avis défavorable de la CNCTR, le Conseil d'État a considéré que l'annulation prononcée impliquait seulement, dans l'attente de l'intervention des textes nécessaires à la mise en conformité du droit national avec le droit de l'Union, qu'en cas d'avis défavorable de la Commission, le Premier ministre ne pourrait légalement autoriser la mise en œuvre des techniques de renseignement concernées avant l'intervention de la décision du Conseil d'État qu'il appartiendrait à la CNCTR de saisir.

La préparation, depuis déjà plusieurs mois à la date de la décision du Conseil d'État, d'un projet de loi « relatif à la prévention d'actes de terrorisme et au renseignement » a permis au Gouvernement français d'appliquer rapidement la décision du Conseil d'État. Le 26 avril 2021, la CNCTR a ainsi été saisie par le Premier ministre d'une lettre rectificative au projet de loi comportant deux articles additionnels destinés à tirer les conséquences de la décision rendue par l'Assemblée du contentieux du Conseil d'État le 21 avril 2021. La commission renvoie aux observations qu'elle a formulées dans sa délibération n°4/2021 du 30 avril 2021[35].

La loi du 30 juillet 2021 a, en premier lieu, modifié l'article L. 34-1 du code des postes et des communications électroniques (CPCE) et l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique organisant le régime de conservation des données relatives aux communications électroniques par les opérateurs, les fournisseurs d'accès à Internet et les hébergeurs de contenus pour prévoir, dans l'hypothèse d'une menace grave, actuelle ou prévisible pour la sécurité nationale, la possibilité pour le Premier ministre de leur enjoindre de conserver de manière générale

35 - Voir la délibération n°4/2021 du 30 avril 2021, publiée en annexe n°4 au présent rapport et sur le site Internet de la CNCTR

et indifférenciée, pendant une durée d'un an, certaines catégories de données de connexion. Cette injonction prend la forme d'un décret, soumis au contrôle du juge administratif, dont la durée d'application ne peut excéder un an[36]. L'injonction peut néanmoins être renouvelée si les conditions prévues pour son édiction continuent d'être réunies.

La loi a, en second lieu, modifié les dispositions du code de la sécurité intérieure relatives au contrôle préalable de la mise en œuvre des techniques de renseignement pour prévoir désormais que lorsque le Premier ministre délivre une autorisation malgré un avis défavorable de la CNCTR, celle-ci doit immédiatement saisir le Conseil d'État qui statue dans un délai de vingt-quatre heures[37]. Pendant ce délai, la technique de renseignement en cause ne peut pas être mise en œuvre, sauf en cas d'urgence dûment justifiée et si le Premier ministre ordonne l'exécution immédiate de son autorisation. Le caractère d'urgence ne peut toutefois être invoqué pour toutes les techniques de renseignement[38] et est, pour certaines techniques, limité à un nombre réduit de finalités. Suivant la recommandation de la CNCTR, le législateur a, en outre, exclu la possibilité d'invoquer le caractère d'urgence lorsque la technique de renseignement concerne un parlementaire, un magistrat, un avocat ou un journaliste. La loi a par ailleurs abrogé l'article L. 821-5 du code de la sécurité intérieure qui permettait au Premier ministre, en cas d'« urgence absolue » et pour un nombre limité de finalités, de délivrer une autorisation de mise en œuvre d'une technique de renseignement sans avis préalable de la CNCTR.

1.1.3 Une septième modification du décret « second cercle » : cohérence du cadre réglementaire et développement des capacités des services

Le 8 janvier 2021, la CNCTR a été saisie par le ministre de l'intérieur d'un projet de décret en Conseil d'État consistant, pour l'essentiel, à prendre

36 - Voir le décret n° 2021-1363 du 20 octobre 2021 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion.

37 - La CNCTR rappelle que, jusqu'à présent, le Premier ministre n'a jamais autorisé la mise en œuvre d'une technique de renseignement après qu'elle ait émis un avis défavorable.

38 - Il n'est notamment pas possible d'invoquer l'urgence pour autoriser la mise en œuvre initiale ou le renouvellement de la technique de l'« algorithme ».

en considération la réforme des services territoriaux de la direction centrale de la police judiciaire ainsi que plusieurs réorganisations internes intervenues dans des services de la préfecture de police.

Dans un décret du 29 novembre 2021[39], le Gouvernement a suivi l'ensemble des préconisations formulées par la commission dans sa délibération adoptée le 4 février 2021[40].

a) Les modifications affectant les services de la direction centrale de la police judiciaire (DCPJ)

- La prise en compte de la réforme des services territoriaux de la DCPJ

Un décret du 30 décembre 2020[41] ayant modifié l'organisation des services territoriaux de la DCPJ, une évolution réglementaire était nécessaire pour que les nouveaux échelons locaux de la police judiciaire puissent continuer à recourir aux mêmes techniques de renseignement que ceux auxquels ils se sont substitués. La CNCTR a logiquement émis un avis favorable à une telle modification.

- L'attribution de nouvelles techniques de renseignement à certains services de la DCPJ

Le projet de décret prévoyait d'ouvrir le recours à la technique de recueil de données de connexion par *IMSI catcher* (L. 851-6 du code de la sécurité intérieure) aux services locaux de police judiciaire (SPJ), qui ont remplacé au niveau déconcentré les anciennes antennes de police judiciaire, et de permettre à leurs agents et à ceux des nouvelles directions territoriales de la police judiciaire (DTPJ) de s'introduire dans un lieu privé ne constituant pas un lieu d'habitation pour mettre en œuvre les techniques de captation de paroles ou d'images.

La CNCTR a émis un avis favorable à ces modifications après avoir constaté que les services concernés justifiaient de besoins opérationnels identiques

39 - Il s'agit du décret n°2021-1543 du 29 novembre 2021 relatif à la désignation des services relevant du ministère de l'intérieur autres que les services spécialisés de renseignement autorisés à recourir à certaines techniques de renseignement mentionnées au titre V du livre VIII du même code, pris en application du l'article L. 811-4 du code de la sécurité intérieure.

40 - Voir la délibération n°1/2021 du 4 février 2021, publiée en annexe n°5 au présent rapport et sur le site Internet de la CNCTR.

41 - Il s'agit du décret n°2020-1776 du 30 décembre 2020 portant organisation des services territoriaux de la direction centrale de la police judiciaire de la police nationale.

à ceux des autres échelons territoriaux, qu'ils faisaient un usage modéré de ces techniques, et, enfin, que les contrôles menés depuis plus de cinq ans révélaient que leurs agents démontrent une bonne maîtrise du cadre légal et utilisent les techniques de renseignement avec rigueur. La commission a toutefois préconisé que leur mise en œuvre soit réalisée avec le concours d'un opérateur spécialisé disposant de la compétence technique nécessaire, le service interministériel d'assistance technique (SIAT).

Le projet de décret prévoyait également d'ouvrir à l'office anti-stupéfiants (OFAST), service de la DCPJ ayant remplacé, le 1er janvier 2020, l'office central pour la répression du trafic illicite des stupéfiants (OCRTIS), le recours à la technique d'interception des communications émises par voie hertzienne (article L. 852-2 du code de la sécurité intérieure) au titre de la finalité de la prévention de la criminalité et de la délinquance organisées. L'OCRTIS étant jusqu'alors habilité à recourir à cette technique au titre de la même finalité, la CNCTR a estimé que l'OFAST devait également y avoir accès.

b) Les évolutions affectant les services de la préfecture de police

- La prise en compte d'adaptations organisationnelles intervenues au sein de plusieurs directions de la préfecture de police

Dans sa délibération du 4 février 2021, la CNCTR a pris acte de modifications intervenues dans l'organisation de la préfecture de police qui procédaient, à droit constant, à une simplification des modalités d'assistance technique pour la mise en œuvre des techniques de renseignement ainsi qu'à des changements relatifs à l'appellation de deux sous-directions de sa direction du renseignement.

- L'accès à de nouvelles techniques de renseignement ou à de nouvelles finalités pour plusieurs services de la direction régionale de la police judiciaire (DRPJ) de Paris

Le projet de décret prévoyait, en premier lieu, d'ouvrir le recours à la technique d'interception de correspondances échangées par voie hertzienne à plusieurs brigades de la sous-direction des brigades centrales (SDBC) et de la sous-direction des affaires économiques et financières

(SDAEF), au titre des finalités de la prévention du terrorisme et de la prévention de la criminalité et de la délinquance organisées.

À l'aune de la pratique observée depuis plus de cinq ans, la CNCTR a relevé que seules la brigade de répression du banditisme (BRB), la brigade des stupéfiants (BSP) et la brigade de recherche et d'intervention (BRI) de la sous-direction des brigades centrales (SDBC) utilisaient régulièrement les techniques de renseignement et justifiaient du besoin de recourir aux interceptions de sécurité hertziennes.

La CNCTR a, en conséquence, émis un avis favorable à ce que cette technique soit ouverte, au seul titre de la prévention de la criminalité et de la délinquance organisée, à ces trois brigades, sous réserve que sa mise en œuvre soit réalisée avec le concours du SIAT, mais elle s'est prononcée contre une telle extension s'agissant des autres entités pour lesquelles le besoin d'y recourir n'était pas établi.

Le projet de décret prévoyait, en deuxième lieu, de permettre à l'ensemble des brigades de la sous-direction des affaires économiques et financières (SDAEF) d'accéder à la finalité de la prévention du terrorisme.

La CNCTR n'a pas émis d'objection à ce que ces brigades aient accès à la finalité de prévention du terrorisme pour mettre en œuvre les techniques de renseignement auxquelles elles étaient déjà autorisées à recourir au titre de la prévention de la criminalité et de la délinquance organisées.

Le projet de décret prévoyait, en troisième lieu, d'ouvrir à la brigade de lutte contre la cybercriminalité (BLC) de la SDAEF le recours aux techniques de recueil de données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure) et d'introduction dans un lieu à usage d'habitation pour y mettre en place ou retirer un dispositif de recueil de données informatiques (1° du I de l'article L. 853-2 du code de la sécurité intérieure), au titre de la finalité de la prévention de la criminalité et de la délinquance organisées.

Après avoir souligné, d'une part, que la mise en œuvre de la technique de recueil de données de connexion en temps réel requérait des capacités d'analyse technique poussées dont peu de services de renseignement disposent et rappelé, d'autre part, que la BLC n'avait, jusqu'ici, sollicité

aucune autorisation de mettre en œuvre des techniques de captation ou de recueil de données informatiques dans un lieu privé ne constituant pas un lieu d'habitation, la CNCTR a estimé que le besoin d'y recourir n'était pas démontré et a, en conséquence émis un avis défavorable à une telle évolution.

- Le projet de désignation de la sûreté régionale des transports comme nouveau service de renseignement du « second cercle » autorisé à recourir aux techniques de renseignement

Le projet de décret proposait d'autoriser la sûreté territoriale des transports (SRT), service de la préfecture de police chargé de lutter contre la délinquance dans les transports en commun d'Ile-de-France, à recourir à des techniques de renseignement en appui de sa mission.

La CNCTR a relevé que ce service intervenait dans la plupart des cas sur saisine de l'autorité judiciaire ou à la suite de plaintes et avait, en conséquence, une vocation essentiellement judiciaire. L'exercice d'une mission de prévention relevant de la police administrative n'étant pas démontré dans le cas de ce service, non plus que la réalité de son besoin d'accéder à des techniques de renseignement, la commission a émis un avis défavorable à sa désignation comme nouveau service de renseignement.

1.2 Les perspectives d'évolution du cadre juridique : la prise en compte de la jurisprudence de la Cour européenne des droits de l'homme

1.2.1 Les apports des arrêts rendus par la grande chambre de la Cour européenne des droits de l'homme le 25 mai 2021 (*Big Brother Watch et autres contre Royaume-Uni*[42] et *Centrum för rättvisa contre Suède*[43])

Par deux arrêts récents relatifs aux régimes de surveillance britannique et suédois, la Cour européenne des droits de l'homme (CEDH) a, d'une part, défini les garanties que les régimes d'interception en masse de communications électroniques[44] par les services de renseignement doivent respecter pour être conformes aux exigences posées par la Convention européenne des droits de l'homme[45] et a, d'autre part, précisé les conditions d'échanges de renseignements entre services étrangers, qu'il s'agisse de « flux entrants » ou « sortants ». Après un premier examen en chambre, ces deux affaires avaient été renvoyées, à la demande des parties, devant la grande chambre, soit la formation la plus solennelle de la Cour.

- Dans les États parties à la Convention, les régimes d'interception en masse de communications électroniques doivent présenter des « garanties de bout en bout »

Tout en condamnant la Suède et le Royaume-Uni, la Cour a estimé légitime que les États parties à la Convention puissent recourir à la « surveillance de masse » des communications électroniques. Elle a notamment admis que « *l'interception en masse revêt pour les États contractants une importance vitale pour détecter les menaces contre la sécurité*

42 - Il s'agit de la requête n° 58170/13.

43 - Il s'agit de la requête n° 35252/08.

44 - Que ces interceptions portent sur le contenu des communications ou sur les seules « métadonnées » qui leur sont rattachables.

45 - En particulier à ses articles 8, 10 et 13.

nationale[46] », considérant par ailleurs que la Convention n'interdit pas aux États de recourir à de tels régimes d'interception pour protéger leurs intérêts nationaux essentiels et que les États jouissent à cet égard d'une large marge d'appréciation pour déterminer le type de régime d'interception dont ils ont besoin. Eu égard à l'atteinte qu'un tel dispositif est susceptible de porter au droit au respect de la vie privée, ce régime doit toutefois, selon la Cour, être encadré par des « *garanties de bout en bout* ». La nécessité et la proportionnalité des mesures prises doivent en particulier être appréciées, au niveau national, à chaque étape du processus de sa mise en œuvre. Il faut, en outre, que l'interception en masse soit soumise à une autorisation d'une autorité « indépendante » dès le départ, c'est-à-dire lors de la définition de l'objet et de la portée de l'opération d'interception, puis que cette opération soit placée, *a posteriori*, sous la supervision et le contrôle d'un organisme indépendant. Ces éléments sont, de l'avis de la Cour, « d*es garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8 de la Convention* »[47].

Pour vérifier que le cadre juridique en litige contient des garanties suffisantes contre d'éventuels abus et que le dispositif concerné est assujetti à des « garanties de bout en bout », la Cour a dégagé de nouveaux critères, venant compléter les six garanties « minimales » énoncées dans sa jurisprudence antérieure[48]. Elle recherche en particulier si le cadre juridique national définit clairement :

1. Les motifs pour lesquels l'interception en masse peut être autorisée ;
2. Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;
3. La procédure d'octroi d'une autorisation ;
4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;

46 - Voir le point 424 de l'arrêt *Big Brother Watch*.

47 - Voir le point 350 de l'arrêt *Big Brother Watch*

48 - La Cour a déterminé que pour prévenir les abus de pouvoir, la loi doit au minimum énoncer les éléments suivants : 1) la nature des infractions susceptibles de donner lieu à un mandat d'interception ; 2) la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées ; 3) la limite à la durée d'exécution de la mesure ; 4) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; 5) les précautions à prendre pour la communication des données à d'autres parties ; 6) les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites.

5. Les précautions à prendre pour la communication de ces éléments à d'autres parties ;
6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;
7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;
8. Les procédures de contrôle indépendant *a posteriori* du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

C'est à l'aune de ces nouveaux critères, que la Cour a considéré que les régimes britannique et suédois contestés devant elle souffraient de plusieurs carences.

- Le partage international de données entre services de renseignement doit être encadré par un organe indépendant et présenter des garanties dans la gestion des données concernées

La Cour, dans son arrêt *Big Brother Watch*, s'est par ailleurs prononcée sur les échanges de renseignements entre services étrangers. Si elle n'émet pas d'objection de principe à de tels partages d'informations, elle a cependant estimé nécessaire que les échanges soient encadrés par un certain nombre de garanties et soumis à un contrôle indépendant, qu'ils portent sur les renseignements reçus de partenaires étrangers (« flux entrants »), comme sur ceux susceptibles de leur être transmis (« flux sortants »).

S'agissant, en premier lieu, des « flux entrants », la Cour a noté que la protection accordée par la Convention se trouverait vidée de sa substance si les États pouvaient contourner leurs obligations conventionnelles en adressant à des États tiers des demandes d'interception de communications ou de remise de communications interceptées, voire même obtenir ces communications par un accès direct aux bases de données de ces derniers. Elle exige dès lors que les demandes adressées aux pays tiers aient un fondement en droit interne, accessible et prévisible quant à ses

effets, qui précise dans quelles circonstances et sous quelles conditions les autorités sont habilitées à formuler de telles demandes.

En outre, dès la réception des éléments interceptés, l'État destinataire doit, selon la Cour, avoir mis en place des garanties suffisantes pour leur examen, leur utilisation, leur conservation, leur transmission à des tiers, leur effacement et leur destruction. La Cour considère que ces règles doivent s'appliquer à l'ensemble des éléments reçus de services de renseignement étrangers qui pourraient être le produit d'une interception alors même que l'État destinataire en ignorerait l'origine exacte.

La Cour a par ailleurs souligné que « *tout régime autorisant des services de renseignement à demander à des États non contractants de procéder à une interception ou de leur transmettre des éléments interceptés doit être soumis à une supervision indépendante et doit également prévoir la possibilité d'un contrôle* a posteriori *indépendant* »[49].

Dans le cas du Royaume-Uni, c'est la coopération entre les services de renseignement britanniques et la National Security Agency (NSA) américaine qui était visée. La Cour a constaté que le droit interne posait des normes claires et précises, indiquant dans quelles circonstances et sous quelles conditions les services de renseignement étaient habilités à y avoir recours, y compris pour des renseignements émanant d'un État non contractant comme les États-Unis. Par ailleurs, la Cour a relevé l'existence de deux formes de contrôle sur ces échanges, l'un par le Commissaire à l'interception des communications, l'autre par le Tribunal des pouvoirs d'enquête (IPT). Dans ces conditions, elle a jugé qu'il existait des garanties suffisantes pour prévenir d'éventuels abus et empêcher les autorités britanniques de demander des éléments interceptés à des services de renseignement alliés dans le but de contourner leurs obligations découlant du droit interne ou de la Convention.

La Cour s'est, en second lieu, prononcée sur une question qu'elle n'avait pas examinée jusqu'alors : celle des flux sortants[50].

49 - Voir le point 499 de l'arrêt *Big Brother Watch*.

50 - Voir en particulier le point 362 du même arrêt.

La Cour a considéré que la transmission, par un État contractant, d'informations obtenues au moyen d'une interception en masse à des États étrangers ou à des organisations internationales est possible mais doit être limitée aux éléments recueillis et conservés d'une manière conforme à la Convention et soumise à certaines garanties supplémentaires relatives au transfert lui-même. Premièrement, selon la Cour, les circonstances dans lesquelles pareil transfert peut avoir lieu doivent être clairement énoncées dans le droit interne. Deuxièmement, l'État qui transfère ces informations doit s'assurer que l'État destinataire a mis en place, pour la gestion des données concernées, des garanties de nature à prévenir d'éventuels abus. L'État destinataire doit, en particulier, garantir la conservation sécurisée des données et restreindre leur divulgation à d'autres parties. Selon la Cour, cela ne signifie pas nécessairement qu'il doive garantir une protection comparable à celle de l'État qui transfère les informations, ni qu'une assurance doive être donnée avant chaque transfert. Troisièmement, des garanties renforcées sont nécessaires lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière[51]. Enfin, la Cour considère que le transfert d'informations à des partenaires de renseignement étrangers doit également être soumis à un contrôle indépendant.

Dans son troisième rapport d'activité pour l'année 2018, la CNCTR avait ouvert le débat sur un encadrement légal des échanges de données entre les services de renseignement français et leurs partenaires étrangers, et appelé à poursuivre la réflexion, au regard des conséquences potentielles que ces échanges peuvent engendrer sur la vie privée des Français et, de manière générale, de toute personne résidant en France. Elle renvoie le lecteur aux développements du point 1.2.4 de ce rapport. La commission estime que les exigences formulées par la Cour en la matière donnent à cet appel un caractère désormais plus pressant, en soulignant que cette jurisprudence est suffisamment claire, précise et solennellement affirmée.

51 - Par exemple s'il s'agit de communications journalistiques confidentielles.

1.2.2 Les instances toujours en cours devant la CEDH mettant en cause la loi du 24 juillet 2015

Comme la CNCTR le rappelait dans ses précédents rapports d'activité[52], quatorze requêtes introduites devant la CEDH entre le 7 octobre 2015 et le 21 avril 2017 par des avocats et des journalistes contre la loi du 24 juillet 2015 relative au renseignement sont toujours pendantes.

Pour mémoire, les requérants soutiennent, d'une part, que les techniques de renseignement n'ont pas de base légale suffisante. Ils se plaignent, d'autre part, d'une insuffisance des garanties procédurales et de l'absence de recours effectif, en méconnaissance des dispositions combinées des articles 8, 10 et 13 de la Convention[53].

Par un courrier du 22 juillet 2021, la Cour a accordé au Gouvernement français la possibilité de produire des observations complémentaires à celles précédemment transmises les 17 novembre 2017 et 23 mars 2018, à la lumière des arrêts rendus par la grande chambre dans les affaires *Big Brother Watch et autres c. Royaume-Uni* et *Centrum för rättvisa c. Suède*.

Le Gouvernement français a, en particulier, souhaité porter à la connaissance de la Cour les nouvelles dispositions issues de la loi du 30 juillet 2021. Il l'a, en substance, invité à prendre en considération le renforcement des garanties opéré par cette loi, qui encadre encore davantage la mise en œuvre des techniques de recueil de renseignement, tout en relevant que cette évolution législative venait entériner, sur plusieurs aspects, la pratique antérieure. Le Gouvernement a rappelé à cet égard qu'avant que le législateur français n'instaure, en 2021, un mécanisme de saisine immédiate du Conseil d'État en cas de désaccord entre la CNCTR et le Premier ministre sur une demande de mise en œuvre de technique de renseignement, celui-ci a toujours suivi les avis défavorables rendus par la commission sur de telles demandes depuis l'entrée en vigueur de la loi du 24 juillet 2015 relative au renseignement.

52 - Voir les points 1.2.2.2 des quatrième et cinquième rapports d'activité pour les années 2019 et 2020 de la CNCTR.

53 - Pour une description plus détaillée du contenu des requêtes, la CNCTR renvoie aux points 1.2.2.2 de son quatrième rapport d'activité pour l'année 2019.

Ces observations ont été transmises à la Cour au cours du mois d'octobre 2021. La décision de la Cour devrait intervenir avant la fin de l'année 2022 sans qu'aucune indication précise de calendrier soit disponible à la date de publication de ce rapport.

La CNCTR se gardera, cette année encore, d'émettre des hypothèses sur l'issue de ces requêtes. Elle relève toutefois que les deux arrêts rendus par la grande chambre le 25 mai 2021 témoignent d'une approche différente de celle retenue par la CJUE. Contrairement à cette dernière, lorsque la CEDH apprécie la conformité d'un régime de droit interne aux exigences de la Convention, elle adopte une vision globale de son fonctionnement. Elle estime de manière constante ne pas avoir pour mission d'examiner *in abstracto* la législation et la pratique pertinentes mais de rechercher si la manière dont celles-ci ont été appliquées au requérant ou l'ont affecté a effectivement donné lieu à une violation de la Convention. Elle considère que dans une matière telle que la défense et la sécurité nationale, chaque État dispose « *d'un large pouvoir d'appréciation* » : aucun système procédural n'est imposé dès lors que la qualité des garanties données répond aux critères de la Convention.

La CNCTR face à la crise sanitaire résultant de la pandémie de Covid-19

Comme en 2020, la CNCTR s'est employée, durant toute l'année 2021, à limiter le risque sanitaire pour ses membres et ses agents ainsi que pour les personnes à leur contact tout en assurant la continuité de son activité de contrôle. À aucun moment celle-ci n'a été interrompue.

La commission a conservé, jusqu'à la fin du mois de mai 2021, l'organisation mise en place à la sortie du premier confinement le 11 mai 2020, dans laquelle des membres et des agents étaient alternativement placés en réserve afin de pouvoir intervenir sur le site en cas d'indisponibilité de collègues affectés par le virus. Au total, de janvier à mai 2021, environ 40 % des effectifs de la commission ont ainsi eu recours, alternativement, à des formes de télétravail adaptées à la nature particulière des missions de la commission et aux exigences de confidentialité, ou ont bénéficié d'autorisations spéciales d'absence.

Durant cette période, les réunions collégiales ont été limitées au strict nécessaire (c'est-à-dire à deux réunions hebdomadaires sur site, au lieu de trois) et il a exceptionnellement été recouru, lorsque cela a été possible, aux modalités de l'article 7 du règlement intérieur de la CNCTR prévoyant l'adoption de délibérations au moyen de communications électroniques sécurisées.

Les déplacements de la commission, en particulier les contrôles *a posteriori* dans les locaux des services de renseignement, ont été temporairement suspendus durant le troisième confinement imposé, en Ile-de-France, du 20 mars au 3 mai 2021. L'accent a alors été mis sur le contrôle *a posteriori* exercé depuis les locaux de la commission grâce aux outils informatiques disponibles.

La reprise progressive de l'activité normale de la commission a débuté le 24 mai 2021. Le retour des membres et des agents s'est effectué de manière graduelle et maîtrisée, dans le strict respect des mesures barrières et dans des conditions assurant leur protection. Les contrôles *a posteriori* sur pièces et sur place ont progressivement retrouvé leur rythme habituel, selon un protocole sanitaire adapté.

2. Le contrôle *a priori* : un examen exhaustif de l'ensemble des demandes soumises à autorisation dont le périmètre a été étendu par le législateur

Aux termes de l'article L. 833-1 du code de la sécurité intérieure, la CNCTR veille à ce que les techniques de renseignement soient mises en œuvre sur le territoire national conformément au cadre légal qui les régit. Cette mission de contrôle porte également sur les mesures de surveillance des communications électroniques internationales, en application de l'article L. 854-9 du code de la sécurité intérieure.

En 2021, le contrôle préalable de la CNCTR a porté sur un volume total de demandes tendant à la mise en œuvre de techniques de renseignement supérieur de 10 % à celui constaté en 2020.

Comme les années précédentes, ce contrôle s'est exercé sur l'intégralité des demandes formulées par les services de renseignement. Aucune demande n'a en effet été présentée selon la procédure d'urgence absolue prévue, jusqu'à son abrogation par la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, à l'ancien article L. 821-5 du code de la sécurité intérieure qui dispensait alors le Premier ministre, dans des cas exceptionnels, de recueillir l'avis de la CNCTR avant d'autoriser la mise en œuvre de certaines techniques de renseignement.

Les moyens financiers et humains de la CNCTR

Composée d'un collège de neuf membres qui s'appuie sur un secrétariat général de dix-sept agents, la CNCTR dispose d'un budget propre qu'elle gère en toute indépendance.

Les crédits alloués par le Parlement à la CNCTR sont inscrits au budget général de l'État (mission « Direction de l'action du Gouvernement », programme n° 308 « Protection des droits et libertés », action n° 12 « Commission nationale de contrôle des techniques de renseignement »).

La loi de finances initiale pour 2021[54] a attribué à la CNCTR des montants d'un peu plus de 2,4 millions d'euros pour ses dépenses de personnel et de 365 000 euros pour ses dépenses de fonctionnement. Comme en 2020, ces crédits ont été presque entièrement consommés.

La CNCTR s'interroge aujourd'hui sur l'adéquation des moyens qui lui sont alloués au regard des missions qui lui sont confiées.

Elle rappelle à cet égard que sa compétence a été étendue par plusieurs lois depuis sa mise en place le 3 octobre 2015 :

- la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et celle n° 2017-258 du 28 février 2017 relative à la sécurité publique ont intégré le renseignement pénitentiaire dans le second cercle des services de renseignement et ouvert à des agents du ministère de la justice la faculté de recourir à des techniques de renseignement ;

- la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme a rénové le cadre juridique régissant la surveillance des communications empruntant la voie hertzienne en créant une nouvelle technique de renseignement soumise au droit commun et en réduisant à un champ d'application marginal les mesures pouvant être prises sans autorisation préalable du Premier ministre ;

54 - Voir la loi n° 2020-1721 du 29 décembre 2020 de finances pour 2021.

- la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 a rendu obligatoire le contrôle *a priori* de la CNCTR sur les demandes d'exploitation de communications électroniques internationales et a notamment prévu les conditions dans lesquelles des vérifications ponctuelles peuvent être réalisées, sous le contrôle de la commission, sur des communications passées à partir d'identifiants rattachables au territoire national ;

- la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice a élargi, tout en les assortissant de garanties renforcées, les possibilités de recours aux techniques de renseignement par les services du ministère de la justice chargés du renseignement pénitentiaire.

Enfin, ainsi que cela a été évoqué au point 1.1.1 du présent rapport, le cadre juridique créé par la loi du 24 juillet 2015 a été révisé par la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement afin de le préciser et de l'adapter aux besoins des services de renseignement.

Ces modifications législatives successives se sont traduites par un élargissement important des missions confiées à la CNCTR. Si ces extensions de compétences avaient, jusqu'à présent, pu être assumées à effectifs constants, les modifications introduites par la loi du 30 juillet 2021 auront, à court terme, un impact notable sur l'activité de la commission.

Pour accomplir ses missions, la CNCTR s'appuie sur une équipe de fonctionnaires et contractuels placés sous l'autorité du président, incluant un secrétaire général, un conseiller auprès du président, onze chargés de mission et quatre agents chargés de fonctions de soutien. Les chargés de mission de la commission sont recrutés pour leurs connaissances juridiques ou techniques.

Depuis son installation en 2015, la CNCTR s'est efforcée de perfectionner ses outils informatiques ainsi que ses procédures internes d'organisation du travail afin de faciliter et améliorer l'efficacité de son contrôle. Les marges de progression dans ce domaine se révèlent aujourd'hui limitées.

En outre, les défis technologiques majeurs auxquels doivent, en permanence, s'adapter les techniques de renseignement imposent à la

CNCTR, pour être en capacité d'exercer pleinement son contrôle, d'ajuster et relever son niveau de compétence technique.

Alors que le nombre de demandes de mise en œuvre de techniques de renseignement soumises au contrôle *a priori* de la commission ne cesse d'augmenter d'une année sur l'autre, la CNCTR doit poursuivre l'approfondissement de son contrôle *a posteriori*.

Dans ces conditions, il apparaît aujourd'hui nécessaire que la CNCTR bénéficie d'un renforcement de ses effectifs.

2.1 Une activité soutenue traduisant une reprise de celle des services dans un contexte de ralentissement de la pandémie de Covid-19

Comme dans ses précédents rapports d'activité, la CNCTR présente des éléments statistiques sur les techniques de renseignement relevant de la surveillance intérieure, c'est à dire concernant des personnes qui se trouvent sur le territoire national.

Ces éléments portent sur le nombre d'avis rendus par la commission sur les demandes d'autorisation de mise en œuvre de techniques de renseignement dont celle-ci a été saisie, sur les finalités invoquées à l'appui de ces demandes ainsi que sur le nombre de personnes surveillées.

Jusqu'à son cinquième rapport d'activité pour l'année 2020, la CNCTR avait fait le choix, afin de prévenir tout risque de divulgation d'informations susceptible de nuire aux intérêts fondamentaux de la Nation, en particulier certaines méthodes opérationnelles des services de renseignement, de publier une présentation statistique consolidée du nombre d'avis rendus par technique de renseignement. Cette présentation détaillait uniquement les données relatives aux accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), aux interceptions de sécurité mises en œuvre *via* le GIC (I de l'article L. 852-1 du même code) et aux géolocalisations en temps réel (article L. 851-4 de ce code) et regroupait, dans une catégorie unique, l'ensemble des « autres techniques de renseignement ».

À l'aune de l'expérience tirée de ses cinq premières années d'activité, la commission a finalement estimé que les données statistiques relatives à chacune des techniques de renseignement prévues par le titre V du livre VIII du code de la sécurité intérieure pouvaient être publiées sans que cela compromette le secret des méthodes opérationnelles des services de renseignement. Cette présentation, qui offre une information plus complète sur son activité de contrôle préalable, sera reconduite dans les rapports d'activité ultérieurs de la commission. Afin de permettre

au lecteur d'apprécier l'évolution de l'utilisation des techniques de renseignement, ces données seront, en outre, mises en perspective sur une période de cinq ans.

Par ailleurs, ainsi qu'elle le fait depuis son troisième rapport d'activité pour l'année 2018, la commission indique le nombre d'avis préalables qu'elle a rendus en 2021 sur les demandes relevant de la surveillance des communications électroniques internationales.

Les éléments statistiques figurant dans ce rapport sont le fruit d'un travail d'extraction et d'agrégation de données conduit par la CNCTR conjointement avec le GIC, puis de fiabilisation des résultats.

2.1.1 Les avis préalables rendus par la CNCTR en matière de surveillance intérieure : une nouvelle augmentation des demandes d'accès aux données de connexion accompagnée d'un recours accru aux autres techniques de renseignement par rapport à 2020

En matière de surveillance intérieure, les avis préalables rendus par la CNCTR se répartissent comme indiqué dans le tableau général ci-dessous.

Les chiffres indiqués dans ce tableau incluent l'ensemble des demandes présentées par les services de renseignement au titre des années 2017 à 2021.

	2017	2018	2019	2020	2021	évolution 2020/ 2021	evolution 2017/ 2021
Accès aux données de connexion en temps différé *(identification d'abonnés ou recensement de numéros d'abonnement) (article L. 851-1 du code de la sécurité intérieure)*	**30116**	**28741**	**25051**	**30758**	**32254**	**+ 4,9 %**	**+ 7,1 %**
Accès aux données de connexion en temps différé *(autres demandes, dont celles de « factures détaillées ») (article L. 851-1)*	**18512**	**17443**	**14568**	**18006**	**19974**	**+ 10,9 %**	**+ 7,9 %**

	2017	2018	2019	2020	2021	évolution 2020/ 2021	evolution 2017/ 2021
Accès aux données de connexion en temps réel *(article L. 851-2)*	115	278	1184	1644	1534	- 6,7 %	+ 1233,9 %
Géolocalisations en temps réel *(article L. 851-4)*	3751	5191	7601	8394	9920	+ 18,2 %	+ 164,5 %
Interceptions de sécurité *via* le GIC *(I de l'article L. 852-1)*	8758	10562	12574	12891	12736	- 1,2 %	+ 45,4 %
Interceptions des communications par *IMSI catcher* *(II de l'article L. 852-1)*	0	0	0	0	0	-	-
Interceptions de sécurité sur les réseaux exclusivement hertziens *(article L. 852-2)*	1	3	3	0	3	-	+ 200 %
Localisations des personnes ou des objets *(« Balisages »)* *(article L. 851-5)*	1330	1510	1793	1598	2006	+ 25,5 %	+ 50,8 %
Recueils de données de connexion par IMSI catcher *(article L. 851-6)*	277	272	288	311	583	+ 87,5 %	+ 110,5 %
Captations de paroles prononcées à titre privé et **captations d'images dans un lieu privé** *(article L. 853-2)*	2438	3003	3282	1564	2138	+ 36,7 %	- 12,4 %
Recueils et captations de données informatiques *(article L. 853-2)*	2518	3082	3591	2418	3758	+ 55,4 %	+ 49,2 %
Introductions dans des lieux privés *(article L. 853-3)*	2571	3206	3599	2021	2682	+ 32,7 %	+ 4,3 %

	2017	2018	2019	2020	2021	évolution 2020/ 2021	evolution 2017/ 2021
Ensemble des techniques de renseignement	70390	73298	73543	79605	87588	+ 10 %	+ 24.4 %

Ce tableau fait apparaitre qu'après être resté stable entre 2018 et 2019, le nombre total de demandes tendant à la mise en œuvre de techniques de renseignement, qui avait crû d'environ 8 % l'année dernière, enregistre en 2021 une augmentation de 10 %. Cette hausse concerne, dans des proportions plus ou moins marquées, la presque totalité des techniques de renseignement considérées.

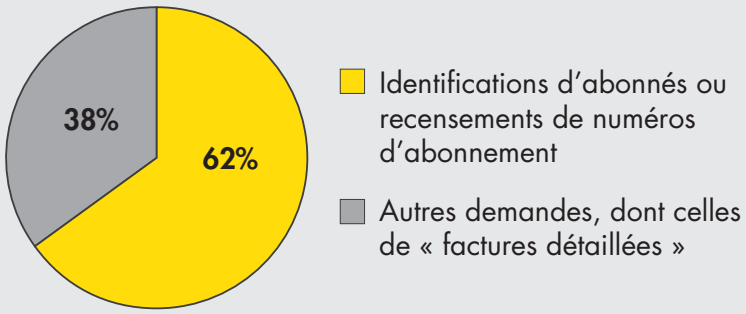
Technique de renseignement la plus utilisée mais la moins intrusive de toutes celles prévues au livre VIII du code de la sécurité intérieure, les demandes d'**accès aux données de connexion en temps différé** (article L. 851-1 du code de la sécurité intérieure) affichent en 2021 une hausse de 7 %, poursuivant ainsi la tendance observée en 2020[55].

Il est rappelé qu'en application de la méthode de comptabilisation de la commission, une demande présentée sur le fondement de l'article L. 851-1 du code de la sécurité intérieure est susceptible de porter sur plusieurs accès à la fois. Ainsi, une demande de recensement de numéros d'abonnement téléphonique d'une personne peut entraîner le recueil de plusieurs numéros auprès de plusieurs opérateurs de communications électroniques et, partant, l'émission de plusieurs réquisitions.

Comme le montre le graphique ci-dessous, la répartition entre prestations d'identification et autres prestations, parmi lesquelles les factures détaillées ou « fadets », s'inscrit dans une proportion approchant, respectivement, deux tiers/un tiers qui est stable depuis 2016.

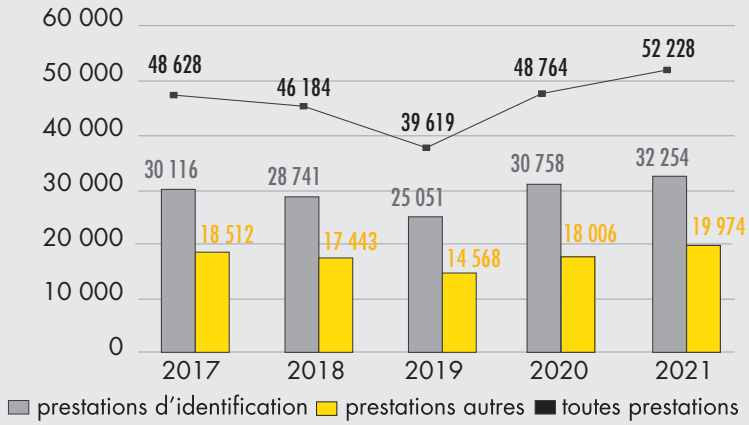
55 - En 2020, cette hausse était de près de 23 %. Voir le point 2.1.1. du cinquième rapport d'activité pour l'année 2020 de la CNCTR.

La répartition des demandes d'accès aux données de connexion en temps différé en 2021



L'évolution sur les cinq dernières années fait apparaître une hausse de 7 % du nombre total de demandes d'accès aux données de connexion en temps différé par rapport à 2017. Cette évolution affecte dans des proportions similaires les prestations d'identification (+ 7,1 %) et les « autres » prestations (+ 7,9 %).

Évolution de la répartition des demandes d'accès au données de connexion entre 2007 à 2021



Les demandes de **géolocalisations en temps réel** (article L. 851-4 du code de la sécurité intérieure) enregistrent en 2021 une hausse de 18 %, poursuivant ainsi leur progression de manière plus marquée qu'en 2020.

Cette technique de renseignement est celle qui a le plus significativement augmenté, aux côtés des demandes d'accès aux données de connexion en temps réel[56], durant la période 2017-2021 (+ 165 %).

Les demandes d'**interceptions de sécurité** réalisées via le GIC (I de l'article L. 852-1 du code de la sécurité intérieure), après avoir connu de fortes augmentations en 2018 et 2019 (de respectivement, 20 % et 19 %) demeurent à un niveau comparable à celui constaté en 2020 puisque leur nombre, passant de 12 981 à 12 736, s'infléchit de 1 %.

La volumétrie concernant les **autres techniques de renseignement** enregistre sur l'année écoulée une progression globale de 32 %. Cette hausse, importante, doit cependant être mise en relation avec la forte inflexion de cet agrégat de techniques de renseignement constatée en 2020, conséquence directe de la crise sanitaire résultant de l'épidémie de Covid-19.

Les demandes d'**accès aux données de connexion en temps réel** (article L. 851-2 du code de la sécurité intérieure), technique de renseignement peu intrusive et soumise à contingentement, constituent, avec les interceptions de sécurité réalisées *via* le GIC, la seule technique connaissant une diminution entre 2020 et 2021, leur nombre reculant de près de 7 %. À l'inverse, la variation sur cinq ans révèle une très forte augmentation de leur nombre. Celle-ci s'explique notamment par l'appropriation tardive par les services de renseignement de cette technique dont la mise en œuvre nécessite des capacités d'analyse technique poussée. Ainsi, son utilisation, très marginale jusqu'en 2018, ne s'est effectivement développée qu'au cours de l'année 2019 et a poursuivi sa progression l'année suivante.

Les demandes portant sur les **autres techniques de renseignement** prévues aux chapitres I à III du titre V du livre VIII du code de la sécurité intérieure ont connu, en 2021, une augmentation plus ou moins marquée selon les techniques concernées, qui doit toutefois être replacée dans le contexte de la crise sanitaire. En effet, les mesures de restriction des déplacements mises en œuvre pour lutter contre l'épidémie de Covid-19 avaient engendré en 2020 un recul, parfois significatif, du recours aux

56 - Voir ci-dessous.

techniques dites de proximité, c'est-à-dire réalisées physiquement au contact de la cible. La levée progressive de ces contraintes a permis aux services de renseignement de recourir davantage à ce type de techniques.

Ainsi, le nombre de demandes d'introduction dans un lieu privé augmente de 32 % en 2021, tout en demeurant inférieur à celui constaté en 2019. La CNCTR rappelle que l'introduction dans un lieu privé ne constitue pas à proprement parler une technique de renseignement autonome dans la mesure où elle ne permet pas, à elle seule, le recueil de renseignement. Elle constitue plutôt un accessoire de mise en œuvre d'autres techniques de renseignement énumérées par l'article L. 853-3 du code de la sécurité intérieure[57].

De même, les techniques de **captation de paroles prononcées à titre privé et de captation d'images dans un lieu privé** (article L. 853-1 du code de la sécurité intérieure) affichent cette année une hausse de 36,7 %, sans toutefois atteindre le volume constaté en 2019.

Les **recueils et captations de données informatiques** (article L. 853-2 du code de la sécurité intérieure) enregistrent en 2021 une progression de 55 % mais qui, par comparaison avec l'année 2019, se limite à 4 %.

Les demandes de **recueils de données de connexion par *IMSI catcher*** (article L. 851-6 du code de la sécurité intérieure) connaissent un accroissement important en 2021 (+ 87 %). Cette technique, également soumise à contingentement et dont la mise en œuvre requiert le déploiement d'opérations techniques complexes, a fait l'objet de 583 demandes en 2021.

S'agissant enfin de la technique de l'**algorithme** sur les données de connexion en vue de détecter une menace terroriste (article L. 851-3 du code de la sécurité intérieure), une nouvelle autorisation de mise en œuvre a été accordée en 2021. À la fin de l'année 2021, quatre algorithmes avaient donc été autorisés depuis l'entrée en vigueur du cadre légal le 3 octobre 2015 et étaient en fonctionnement.

57 - Elle ne peut en effet être utilisée que pour mettre en place, utiliser ou retirer les dispositifs techniques mentionnés aux articles L. 851-5, L. 853-1 et L. 853-2 du code de la sécurité intérieure, dans le respect du principe de subsidiarité, c'est-à-dire lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé.

Les avis défavorables rendus par la CNCTR en 2021

En 2021, la CNCTR a rendu, hors demandes d'accès aux données de connexion en temps différé prévues à l'article L. 851-1 du code de la sécurité intérieure, 398 avis défavorables, soit 1,1 % du nombre d'avis rendus.

Si ce taux connaît une très légère progression en 2021 (+ 0,2 point), après avoir constamment diminué depuis 2015[58], cette évolution ne témoigne pas cependant d'un relâchement des efforts accomplis jusqu'alors par les services de renseignement pour se conformer au cadre juridique en vigueur.

La commission ne l'attribue pas davantage à une moindre qualité du dialogue qu'elle entretient de façon continue avec les services demandeurs sur la mise en œuvre des techniques de renseignement.

Cette évolution du taux d'avis défavorables peut en revanche être analysée comme la conséquence logique de la reprise de certaines activités des services après la levée progressive des mesures de restriction adoptées dans le cadre de l'état d'urgence sanitaire. En témoigne un recours accru, par rapport à 2020, aux techniques dites de proximité, souvent les plus intrusives, sur lesquelles la commission exerce un contrôle particulièrement approfondi et vigilant, la conduisant à émettre davantage d'avis défavorables fondés sur la prise en compte des principes de proportionnalité et de subsidiarité.

La CNCTR a par ailleurs rendu 237 avis défavorables sur les demandes d'accès aux données de connexion en temps différé, soit un ratio de 0,45 % des avis rendus sur cette technique. Ce chiffre est en hausse de 0,3 point par rapport à celui constaté en 2020.

Comme les années précédentes, le Premier ministre n'a accordé aucune autorisation malgré un avis défavorable de la commission en 2021. Depuis l'entrée en vigueur du cadre légal, le 3 octobre 2015, les avis défavorables de la CNCTR ont toujours été suivis par le Premier ministre.

58 - Ce taux était de 6,9 % en 2016, de 3,6 %, en 2017 de 2,1 % en 2018, 1,4 % en 2019 et 0,8 % en 2020.

2.1.2 Les finalités invoquées dans les demandes de techniques de renseignement relevant de la surveillance intérieure : la lutte contre le terrorisme toujours prédominante

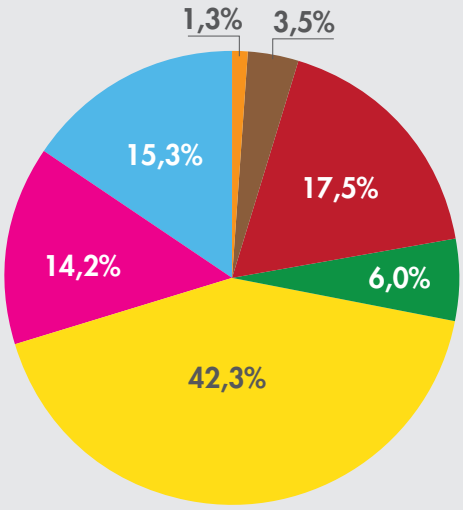
Les techniques de renseignement ne peuvent être mises en œuvre que pour la défense ou la promotion des intérêts fondamentaux de la Nation limitativement énumérés à l'article L. 811 3 du code de la sécurité intérieure[59].

Dans la continuité de la présentation retenue dans ses précédents rapports d'activité, la CNCTR mentionne, pour l'ensemble des demandes tendant à la mise en œuvre d'une technique de renseignement, la proportion de chacune des sept finalités mentionnées à l'article L. 811-3.

En outre, et ainsi que l'a rappelé la commission dans ses trois précédents rapports d'activité, le service national du renseignement pénitentiaire (SNRP), service du « second cercle » relevant du ministère de la justice, peut recourir, en application de l'article L. 855-1 du code de la sécurité intérieure, à une liste limitative de techniques pour des finalités qui lui sont propres, à savoir la prévention des évasions et le maintien de la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues. En 2021, ces finalités ont été invoquées dans 0,1 % des demandes de mise en œuvre de techniques de renseignement, cette proportion étant identique à celle constatée en 2020. Parce qu'elles ne concernent qu'un seul service de renseignement et qu'elles demeurent toujours marginales en volume de demandes, les finalités propres au SNRP ne figurent pas dans le diagramme ci-dessous.

59 - Cette liste est reproduite dans l'encadré consacré au résumé du cadre juridique en vigueur du présent rapport.

Les finalités fondant toutes les demandes de techniques de renseignement en 2021



- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- 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
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

La **prévention du terrorisme**[60], dont le premier rapport d'activité de la CNCTR avait montré qu'elle était devenue, dès janvier 2015, le fondement légal le plus fréquemment invoqué à l'appui des demandes d'interception de sécurité, est demeurée, les années suivantes, très nettement prédominante.

Si, en 2020, la proportion de cette finalité atteignait 46 %, elle régresse de 4 points en 2021 pour atteindre 42 %. Ce léger déclin ne résulte pas d'un recul de la menace terroriste, le nombre de demandes fondées sur cette finalité connaissant une hausse entre 2020 et 2021, mais d'une part plus importante prise par d'autres finalités légales dans le nombre global de demandes.

Suit, en deuxième position, avec un ratio de 22 %, le groupe de **finalités relevant des intérêts géostratégiques de la France** (indépendance et défense nationales, intérêts majeurs de la politique étrangère et prévention de toute forme d'ingérence étrangère, lutte contre la prolifération des armes de destruction massive[61]). Le recours à ces finalités est stable d'une année sur l'autre. Par comparaison, celles-ci représentaient, en 2019 et 2020, respectivement 18 % et 20 % du fondement légal des demandes.

En troisième position, viennent deux finalités invoquées dans des proportions comparables, à savoir, d'une part, **la prévention de la criminalité et de la délinquance organisées**[62] (15 %) et, d'autre part, **la prévention des violences collectives de nature à porter gravement atteinte à la paix publique**[63] (14 %). Par comparaison, ces taux étaient de 14 % en 2020.

La très légère progression de la finalité de prévention de la criminalité et de la délinquance organisées est à mettre en relation avec la levée progressive des mesures de restriction voire d'interdiction de déplacement adoptées dans le cadre de l'état d'urgence sanitaire. La proportion de cette finalité n'a cependant pas retrouvé en 2021 le niveau qu'elle atteignait avant la crise sanitaire (par comparaison ce taux était de 18 % en 2019).

60 - Prévue au 4° de l'article L. 811-3 du code de la sécurité intérieure.

61 - Soit les finalités respectivement prévues aux 1°, 2° et 7° du même article.

62 - Prévue au 6° du même article.

63 - Prévue au c) du 5° de cet article.

Après avoir constamment augmenté ces quatre dernières années, la proportion occupée par la finalité de prévention des violences collectives de nature à porter gravement atteinte à la paix publique s'est stabilisée à hauteur de 14,1 % en 2021 contre 14,2 % en 2020[64]. Le nombre de demandes fondées sur cette finalité, toutefois, a continué d'augmenter.

La CNCTR rappelle qu'elle se montre particulièrement vigilante sur ces demandes, considérant que la prévention des violences collectives ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, fussent-elles extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.

En quatrième et dernière position, la finalité relative à **la défense et à la promotion des intérêts économiques, industriels et scientifiques majeurs de la France**[65] représente cette année 6 % des demandes examinées par la CNCTR, en progression d'un point par rapport à 2020. Cette diminution marquée par rapport à la proportion constatée en 2019 (11 %) est, là encore, une conséquence directe de la pandémie de Covid-19 qui a entraîné une réduction drastique de l'activité économique. Bien que la tendance se soit inversée en 2021, la reprise de l'activité des services de renseignement en la matière est progressive.

2.1.3 Le nombre de personnes surveillées : une légère augmentation en 2021

Comme elle le fait chaque année, la CNCTR a repris l'indicateur qu'elle avait créé à l'occasion de son premier rapport d'activité[66] et a calculé le nombre de personnes ayant fait l'objet, en 2021, d'au moins une technique de renseignement prévue aux chapitres I à III du titre V du livre VIII du code de la sécurité intérieure. Comme les années précédentes, ce chiffre ne comprend pas les accès aux données de connexion en temps différé mentionnés au deuxième alinéa de l'article L. 851-1 du code de la sécurité

64 - Cette proportion est passée de 6,2 à 9,5 % en 2018, à 13,8 % en 2019 puis à 14,2 % en 2020.

65 - Prévue au 3° de l'article L. 811-3 du code de la sécurité intérieure.

66 - Voir le point 3.3 du premier rapport d'activité 2015/2016 de la CNCTR.

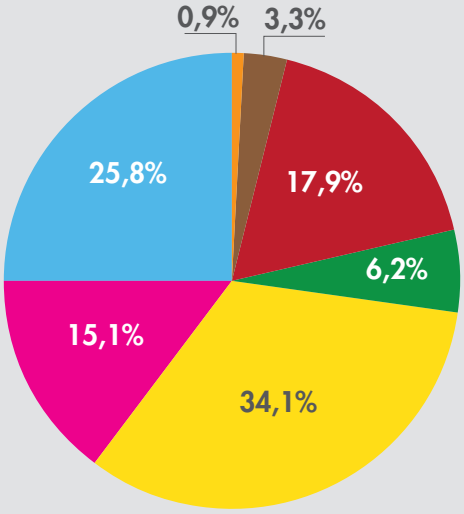
intérieure, c'est-à-dire les identifications d'abonnés ou les recensements de numéros d'abonnement[67].

Les éléments de calcul utilisés comportent une marge d'erreur, évaluée à moins de 10 %, dès lors que les demandes tendant à la mise en œuvre de techniques de renseignement sont présentées par technique et non par personne, que le traitement informatisé des demandes n'est pas entièrement harmonisé et, enfin, que certaines personnes faisant l'objet de surveillance ne sont pas nommément identifiées. Cependant, grâce aux développements informatiques constamment conduits par le GIC et à l'amélioration progressive des outils conçus par la commission lors de sa première année de fonctionnement, la fiabilité du calcul a été renforcée.

	2017	2018	2019	2020	2021	Évolution 2020/ 2021	Évolution 2017/ 2021
Nombre de personnes surveillées	**21386**	**22038**	**22210**	**21952**	**22958**	**+ 4,6 %**	**+ 7,4 %**
Dont, au titre de la **prévention du terrorisme**	**9 157** (42,8 % du total)	**8 579** (38,9 % du total)	**7 736** (34,8 % du total)	**8 786** (40 % du total)	**7826** (34,1 % du total)	**-10,9%**	**- 14,5%**
Dont, au titre de la **prévention de la criminalité et de la délinquance organisées**	**5 528** (25,8 % du total)	**5 416** (24,6 % du total)	**5 693** (25,6 % du total)	**5 021** (22,9 % du total)	**5932** (25,8 % du total)	**+ 18,1 %**	**+ 7,3 %**
Dont, au titre de la **prévention des atteintes à la forme républicaine des institutions ; des actions tendant au maintien ou à la reconstitution de groupements dissous ; ou des violences collectives de nature à porter gravement atteinte à la paix publique**	**Donnée non disponible**	**2116** (9,6 % du total)	**3021** (13,6 % du total)	**3238** (14,8 % du total)	**3466** (15,1 % du total)	**+7 %**	-

67 - La CNCTR considère en effet que les identifications d'abonnés et les recensements de numéros d'abonnement constituent moins une mesure de surveillance à proprement parler qu'un acte préparatoire à des mesures de surveillance. De telles mesures commencent, pour la CNCTR, dès l'obtention de « factures détaillées » de la personne concernée en application du même article L. 851-1 du code de la sécurité intérieure.

La répartition des personnes surveillées selon les finalités motivant leur surveillance



- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- 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
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

Le nombre de personnes surveillées, après avoir reculé entre 2019 et 2020, enregistre une progression d'un peu moins de 5 % en 2021. Par comparaison avec 2019, l'augmentation se limite à 3 %. Cette évolution est à mettre en relation avec la reprise de l'activité des services, notamment en matière de prévention de la criminalité et de la délinquance organisées, le nombre de personnes surveillées sur ce fondement légal connaissant cette année un accroissement de 18 %.

À l'inverse, le nombre de personnes surveillées au titre de la prévention du terrorisme diminue de 11 %. La proportion des personnes faisant l'objet d'une mesure surveillance pour ce motif atteint 34 %, soit la même valeur qu'en 2019.

De manière cohérente avec le diagramme présentant la répartition des finalités invoquées dans les demandes de techniques de renseignement, la proportion des personnes surveillées au titre de la prévention du terrorisme demeure prédominante. Elle est suivie par la prévention de la criminalité et la délinquance organisées qui justifie la surveillance de 25 % des cibles, là encore dans une proportion similaire à celle constatée avant la crise sanitaire.

On observe, par ailleurs, tout comme en 2019, une progression (de 14,8 % à 15,1 %) de la proportion de personnes surveillées sur le fondement de la prévention des violences collectives de nature à porter gravement atteinte à la paix publique. La part des personnes surveillées sur le fondement de la défense et de la promotion des intérêts économiques, industriels et scientifiques majeurs de la France est en légère hausse (de 4,5 % en 2020 à 6,2 % en 2021), de manière cohérente avec ce qui a été dit précédemment sur la part de cette finalité dans les demandes.

2.1.4 Les avis rendus par la CNCTR au titre de la surveillance internationale : une stabilisation du volume des demandes après trois années d'expansion

Comme elle le fait depuis 2018, la CNCTR publie le nombre de demandes d'autorisation en matière de surveillance des communications électroniques internationales sur lesquelles elle s'est prononcée en 2021.

Les autorisations d'exploitation prévues au III de l'article L. 854-2 du code de la sécurité intérieure peuvent concerner les communications ou les seules données de connexion émises ou reçues au sein d'une zone géographique, par une organisation, par un groupe de personnes ou par une seule personne.

L'autorisation prévue, depuis l'entrée en vigueur de la loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025, au V du même article ne concerne, quant à elle, qu'une seule personne. Elle permet l'exploitation des communications ou des seules données de connexion de cette personne lorsque celle-ci utilise un identifiant technique rattachable au territoire national, y compris lorsqu'elle l'utilise pour communiquer depuis la France.

Quelle que soit leur nature, ces autorisations d'exploitation ne peuvent être fondées que sur les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure[68].

En 2021, la commission a rendu 4 374 avis sur des demandes tendant à l'exploitation de communications internationales interceptées, contre 4 316 en 2020. Alors que le nombre des autorisations d'exploitation prévues au III de l'article L. 854-2 du code de la sécurité intérieure est toujours demeuré stable, les autorisations délivrées sur le fondement du V du même article affichaient une forte croissance depuis le dernier trimestre 2019. Il semblerait que le recours à cette technique, au demeurant soumise à contingentement, ait atteint un rythme moyen depuis 2020.

68 - L'autorisation prévue au V de l'article L. 854-2 du code de la sécurité ne peut être délivrée que pour les finalités mentionnées aux 1°, 2°, 4°, 6° et 7° de l'article L. 811-3 du même code.

2.2 Une nouvelle mission confiée par la loi à la CNCTR : le contrôle des échanges de renseignements entre services français

2.2.1 Un enjeu pour la CNCTR : faciliter les échanges tout en assurant la mise en œuvre effective du nouveau cadre législatif

■ Le nouveau régime juridique issu de la loi du 30 juillet 2021

Comme cela a été indiqué au point 1.1.1 du présent rapport, le partage de renseignements entre services français était, jusqu'à l'adoption de la loi du 30 juillet 2021, régi par les dispositions de l'article L. 863-2 du code de la sécurité intérieure qui prévoyait succinctement que les services de renseignement pouvaient « *échanger toutes les informations utiles à l'accomplissement de leurs missions définies au titre Ier du présent livre* » et renvoyait à un décret en Conseil d'État la détermination des modalités et conditions d'application de ce régime. Ce décret n'a toutefois jamais été pris.

Considérant que le partage de renseignements est l'une des conditions de l'efficacité de l'action des services de renseignement, le législateur a estimé nécessaire de le faciliter tout en l'encadrant de façon plus précise.

L'article L. 822-3 du code de la sécurité intérieure, qui régissait déjà la collecte, l'extraction et la transcription des renseignements, offrait à cet égard un cadre adapté.

Cet article, tel qu'il a été modifié par la loi du 30 juillet 2021, énonce ainsi désormais, dans un nouveau II, qu'un service de renseignement[69] « *peut transmettre à un autre* [service] *les renseignements collectés, extraits ou transcrits dont il dispose, si cette transmission est strictement nécessaire à l'exercice des missions du service destinataire* ».

69 - Qu'il appartienne au « premier cercle » ou au « second cercle » des services de renseignement.

Le législateur a néanmoins prévu, aux 1° et 2° du II de l'article L. 822-3, que certaines transmissions de renseignements soient 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.

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. Sont ici concernées à la fois les renseignements à l'état brut ainsi que les transcriptions et extractions réalisées à partir des données collectées.

Ce cas 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, définies par un décret en Conseil d'État, et qui peuvent varier selon la finalité poursuivie.

Relèvent également de ce second cas de figure les transmissions de données issues de la surveillance des communications électroniques internationales.

Le législateur a prévu 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. Cet agent doit en particulier garantir la destruction des données partagées au terme des délais légaux de conservation et assurer la traçabilité des transmissions. Il rend compte sans délai au responsable de son service de toute difficulté dans l'application des dispositions légales.

La loi a par ailleurs aménagé un dispositif de contrôle externe assuré par la CNCTR.

Une double mission de contrôle confiée à la CNCTR

Le contrôle des échanges de renseignements entre services, tout comme celui portant sur la mise en œuvre des techniques de renseignement, consiste pour la CNCTR à accomplir deux missions distinctes et complémentaires :

- une mission de contrôle *a priori* des transmissions soumises à l'autorisation préalable du Premier ministre dans les deux hypothèses mentionnées aux 1° et 2° du II de l'article L. 822-3 du code de la sécurité intérieure, détaillées ci-dessus ;

- une mission de contrôle *a posteriori* de l'ensemble des échanges effectués entre services : dans ce cadre, la commission doit, d'une part, s'assurer que les transmissions autorisées par le Premier ministre sont mises en œuvre conformément à ses décisions et, d'autre part, vérifier que les transmissions soumises, ou non, à son autorisation respectent les limites fixées par la loi.

Le dispositif de contrôle *a posteriori* conçu par le législateur s'appuie sur trois articles du code de la sécurité intérieure :

- une modification, introduite 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 doivent préciser leur nature, la date à laquelle elles ont été effectuées, leur finalité, ainsi que le ou les services qui en ont été destinataires. En outre, lorsque les transmissions poursuivent une finalité différente de celle au titre de laquelle les renseignements ont été recueillis, les relevés doivent être immédiatement transmis à la commission.

- une modification, introduite à l'article L. 833-2, ouvre à la CNCTR un accès permanent, complet et direct aux transmissions de renseignements.

- une modification, introduite 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.

Qu'il s'exerce *a priori* ou *a posteriori*, le contrôle de la CNCTR a donc pour objet de garantir que les services concernés respectent l'ensemble des obligations que leur impose la loi lorsqu'ils se transmettent des renseignements et qu'ils ne recourent à cette faculté qu'à des fins nécessaires et proportionnées aux buts recherchés.

La première condition posée par la loi est que la transmission doit être «*strictement nécessaire à l'exercice des missions du service destinataire*».

Cette précision 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 qu'il n'est pas autorisé à poursuivre.

Le respect de cette condition constituera le premier critère d'examen de la commission.

La CNCTR souligne, à cet égard, que ce type de manquement n'est pas hypothétique.

En effet, à l'occasion de l'un des contrôles *a posteriori* mené au cours de l'année 2021, la CNCTR a découvert un cas de transmission irrégulière de renseignements. Il s'agissait, en l'espèce, du partage de transcriptions issues de l'exploitation de deux interceptions de sécurité entre un service du « premier cercle » et un service du « second cercle ». Le Premier ministre avait autorisé, après avis favorable de la CNCTR, le service du « premier cercle » à mettre en œuvre ces deux techniques sur le fondement de la finalité prévue au 2° de l'article L. 811-3 du code de la sécurité intérieure, c'est-à-dire la défense et la promotion des 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. Cette finalité n'est accessible à aucun des services du « second cercle ». Le service destinataire a fait valoir, au cours du contrôle, que les transmissions étaient intervenues au titre de la finalité prévue au c) du 5° de l'article L. 811-3, c'est à-dire la prévention des violences collectives de nature à porter gravement atteinte à la paix publique. Après avoir examiné l'ensemble des transcriptions transmises à ce service, la CNCTR a cependant estimé qu'aucune des informations qui y étaient consignées n'était susceptible de se rattacher à une telle finalité.

La transmission litigieuse avait permis en conséquence à un service du « second cercle » d'exploiter des renseignements ne présentant pas de lien avec le champ de compétence que lui a attribué le pouvoir réglementaire. La découverte de cette irrégularité a donné lieu à la destruction de l'intégralité des transcriptions dont il avait été destinataire.

La commission sera vigilante à ce qu'une telle situation ne se réitère pas. Dans le cadre de son contrôle *a priori*, elle devra notamment s'assurer que les renseignements dont le partage est envisagé présentent un lien avec la finalité au titre de laquelle la transmission est sollicitée et que cette finalité est accessible au service destinataire. Elle effectuera un contrôle identique, *a posteriori*, sur les renseignements ayant déjà été transmis à un ou plusieurs services partenaires. Dans les deux cas, elle recherchera, en outre, si la transmission est ou était nécessaire à la prévention de la menace pour laquelle le service destinataire est compétent et si les renseignements à l'origine du partage ont été recueillis dans des conditions régulières.

Consciente de l'importance que revêtent ces échanges de renseignements pour l'efficacité de l'action des services, la CNCTR n'entend pas les freiner par un contrôle inutilement formaliste et procédurier. Elle veillera en revanche à ce que les demandes tendant à les autoriser, ainsi que les relevés réalisés lors des transmissions, comportent, même de façon succincte, les éléments concrets permettant d'en apprécier la légitimité.

La commission veillera, par ailleurs, en lien avec l'agent du service chargé du contrôle interne, 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. Chaque service de renseignement, qu'il soit l'émetteur ou le destinataire de renseignements, demeure en effet responsable de leur destruction et doit donc respecter les délais prévus à cet égard par la loi. L'article L. 822-3 précise notamment que ces transmissions sont sans effet sur la durée de conservation de chacun des renseignements collectés, qui court à compter de la date de leur recueil.

Enfin, lorsqu'elle examinera une demande d'autorisation de transmission, la CNCTR vérifiera que le partage concerné respecte le principe de proportionnalité[70].

La commission rappelle en effet que la loi du 24 juillet 2015 relative au renseignement a créé un cadre juridique destiné à garantir le respect de la vie privée dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile. L'atteinte susceptible d'y être portée par la mise en œuvre d'une technique doit par conséquent être proportionnée aux buts poursuivis par le service concerné. La nécessité d'une autorisation pour pénétrer dans un lieu privé, doublée de règles de procédure plus contraignantes lorsque ce lieu est à usage d'habitation, se rattache à la dernière composante, l'inviolabilité du domicile.

Au stade de la transmission de données déjà collectées, toutefois, ce n'est plus la façon de les recueillir qui est en cause. L'intrusion est définitivement consommée. Ce qui importe alors, c'est l'appréciation de la sensibilité des données concernées par cette transmission au regard de la deuxième composante de la protection, c'est-à-dire la protection des données personnelles, lesquelles sont susceptibles de révéler le « contenu » essentiel de la vie privée. Il appartiendra donc à la commission d'apprécier la proportionnalité de l'atteinte que la divulgation de telles données porte au droit au respect de la vie privée au regard de la menace que le service destinataire entend prévenir.

La commission souligne que les axes de contrôle, au demeurant non exhaustifs, qui viennent d'être décrits devront toutefois être soumis à l'épreuve de la pratique. Aucun service de renseignement n'a été en mesure de lui fournir des indications, même approximatives, sur la fréquence et le volume des transmissions à venir. Dans ces conditions, les difficultés éventuelles qui n'avaient pu être anticipées lors de l'instauration de ce nouveau régime devront trouver une solution utile dans le cadre des contrôles réalisés par la CNCTR et du dialogue qu'elle entretient avec les services de renseignement.

70 - C'est-à-dire dans les cas prévus par le 2° du II de l'article L. 822-3 du code de la sécurité intérieure.

2.2.2 L'application du régime juridique des échanges : une définition progressive de ses modalités de mise en œuvre

Les dispositions de la loi du 30 juillet 2021 sont d'application immédiate et sont entrées en vigueur le 31 juillet 2021. Leur mise en œuvre concrète s'est néanmoins heurtée à deux séries de difficultés. Les premières, de nature juridique, portent sur l'interprétation et la portée qu'il convient de donner à certaines dispositions. Les secondes, d'ordre pratique, concernent l'adaptation des outils informatiques du GIC nécessaires, notamment, au traitement des demandes d'autorisation et à l'établissement voire, selon les cas, à la communication des relevés de transmissions. En outre, l'appropriation de ces nouvelles dispositions par les services de renseignement suppose des modifications importantes des procédures internes propres à chacun d'entre eux ainsi qu'une évolution des méthodes et des outils de travail qu'ils utilisent.

Au nombre des interrogations soulevées pour l'application de ce nouveau régime figuraient la délimitation du champ d'application des transmissions soumises à l'autorisation préalable du Premier ministre, mais aussi du contenu de ces autorisations ainsi que de leur portée et de leur durée. Les exigences de traçabilité imposées par le législateur pour répondre aux besoins de la CNCTR ont également nécessité que des précisions soient apportées concernant l'établissement des relevés de transmission ou, lorsque la loi le prévoit, les modalités pratiques de leur communication à la commission.

Dans ces conditions, il est apparu indispensable d'expliciter les modalités et les conditions d'application concrètes de ce nouveau régime. Une première réflexion a été lancée par le Premier ministre au mois de septembre 2021, associant le GIC et les services de renseignement, en vue d'élaborer un guide méthodologique à l'attention des agents des services. Ce document à visée pratique devait permettre d'expliquer le fonctionnement du nouveau cadre juridique en déclinant les obligations légales en consignes précises et concrètes. La CNCTR a été consultée sur cette démarche. Elle avait alors admis que la complexité du régime introduit par la loi du 30 juillet 2021 impliquait un délai de mise en œuvre

et s'était accordée avec le Gouvernement sur un calendrier. Ainsi, il avait été convenu qu'un projet lui serait transmis pour avis dans le courant du mois d'octobre 2021 en vue d'une mise en œuvre effective au 1er janvier suivant.

Au regard des nombreuses préoccupations exprimées par les services de renseignement quant à l'ampleur des adaptations à entreprendre pour la mise en œuvre du nouveau cadre juridique, ce travail de concertation a été retardé et a conduit le Gouvernement à solliciter l'intervention de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT).

En décembre 2021, la CNCTR a été informée des pistes envisagées par le Gouvernement au terme d'un dialogue mené avec les services de renseignement et les directions des affaires juridiques des ministères de tutelle concernés. Ces propositions ont ensuite été intégrées dans un document de travail transmis à la commission fin 2021 afin que celle-ci puisse lui faire connaître de façon informelle ses premières observations.

Enfin, le 4 février 2022, la commission a été formellement saisie pour avis par le Premier ministre d'un projet d'instruction classifié portant sur les modalités d'application du nouveau régime juridique relatif aux transmissions. Une saisine complémentaire lui a, en outre, été adressée le 25 février suivant.

Afin de ne pas retarder davantage l'application des dispositions légales entrées en vigueur près de sept mois auparavant, la CNCTR, réunie en formation plénière, a statué sur ces deux saisines dans des délais particulièrement brefs les 10 février et 23 mars 2022. Elle estime que la mise en œuvre du nouveau régime applicable aux échanges, eu égard aux difficultés d'adaptation qu'elle semble représenter pour les services, devra faire l'objet d'une mise au point régulière avec eux. La commission pourra ainsi apprécier le caractère opérant des nouvelles procédures et s'assurer de leur facilité d'appropriation par les services. Il en sera fait état dans son prochain rapport.

3. Le contrôle *a posteriori* : un renforcement des moyens et une adaptation des méthodes pour faire face à l'accroissement du volume des techniques mises en œuvre et de leur complexité

Comme elle l'indiquait dans ses précédents rapports d'activité, la CNCTR a recours à deux méthodes pour s'assurer de la conformité du recueil, de la transcription, de l'extraction[71] et de la conservation des renseignements aux dispositions du livre VIII du code de la sécurité intérieure.

D'application quotidienne, la première méthode consiste, pour la commission, à opérer des vérifications depuis ses locaux grâce aux outils informatiques mis à sa disposition par le GIC. Ces applications lui offrent, pour certaines techniques, un accès direct aux données recueillies, voire aux transcriptions et extractions réalisées à partir de ces données.

La seconde méthode consiste en la réalisation de contrôles sur pièces et sur place au sein des services de renseignements, ces contrôles pouvant porter sur l'intégralité des techniques entrant dans le champ de compétence de la commission.

Diligentés par une équipe composée de chargés de mission présentant des profils à la fois juridiques et techniques accompagnés d'un membre de la commission, ces contrôles sont, en moyenne, menés à un rythme de deux ou trois par semaine, tous services confondus.

71 - 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.

3.1 Le développement des contrôles et des accès à distance de la CNCTR : des capacités supplémentaires au soutien des contrôles réalisés dans les locaux des services

3.1.1 L'insuffisance des contrôles menés sur pièces et sur place face à la progression du nombre de techniques de renseignement autorisées

Le rythme des contrôles *a posteriori* avait été ralenti en 2020 en raison de la situation sanitaire. Les déplacements avaient été interrompus durant les deux périodes de confinement puis ont progressivement repris, à partir du mois de mai 2020, dans un format adapté au risque sanitaire et aux effectifs disponibles.

La relative amélioration de la situation sanitaire en 2021 a permis à la CNCTR de conduire un nombre de contrôles sur pièces et sur place comparable à celui atteint au cours des années antérieures à la pandémie de Covid-19.

Alors que les déplacements dans les locaux des services de renseignement ont été en partie suspendus durant la troisième période de confinement, ils ont été menés à un rythme soutenu lorsque les conditions sanitaires le permettaient. Ainsi, 117 contrôles sur pièces et sur place ont été réalisés en 2021, contre 76 en 2020. Ce chiffre est, en outre, supérieur à la centaine de contrôles comptabilisés en 2018 et 2019 et proche des 120 mis en œuvre en 2017. Plus d'une vingtaine de ces contrôles ont porté sur la surveillance des communications électroniques internationales.

La fréquence, élevée, de ces déplacements a notamment accompagné la reprise de l'activité des services décrite au point 2 du présent rapport.

Les contrôles dans les centres territoriaux du GIC ont également pu être à nouveau organisés. Si quatre déplacements seulement avaient eu lieu en 2020, huit ont été réalisés en 2021. En comparaison, dix visites avaient

été effectuées en 2019. Pour la deuxième année consécutive aucun déplacement ultra-marin n'a cependant pu être programmé compte tenu des incertitudes liées à l'évolution de la situation sanitaire dans les territoires concernés. La CNCTR a d'ores et déjà planifié une mission de contrôle en Outre-mer pour l'année 2022.

Ces rencontres sont conduites par des délégations du GIC et de la CNCTR respectivement composées, d'une part, du directeur du GIC ou de son adjoint et d'un ou deux responsables des cellules de soutien de la zone géographique concernée et, d'autre part, du président de la commission et/ou d'un membre du collège accompagné(s) d'un ou deux chargé(s) de mission. Elles permettent de rencontrer les responsables des services de renseignement déconcentrés[72] .

Ces réunions sont l'occasion d'échanger sur les problématiques territoriales spécifiques auxquelles les échelons déconcentrés sont confrontés, sur les difficultés d'ordre technique rencontrées ainsi que sur les interrogations juridiques suscitées par l'application du cadre légal. Un bilan des techniques mises en œuvre et des résultats obtenus est réalisé avec chaque service déconcentré, certains avis rendus par la commission sont évoqués et expliqués en même temps que les règles de droit sont rappelées.

Les contrôles sur pièces et sur place constituent la méthode privilégiée par la CNCTR. Elle offre en effet l'occasion de mener un dialogue utile et efficace avec les services et garantit à la commission une bonne connaissance du fonctionnement et des difficultés rencontrées par chaque service. Elle se heurte néanmoins à la progression continue du nombre de techniques mises en œuvre et à leur degré de complexité croissant alors que les moyens matériels et humains de la CNCTR sont restés stables depuis 2015.

Les évolutions technologiques et les transformations des modes de communication électronique ont contraint les services à adapter leurs méthodes et leurs outils de surveillance technique. Cela s'est traduit par le

72 - Il peut s'agir des services déconcentrés de la sécurité intérieure, de la police judiciaire, du renseignement territorial, de la gendarmerie nationale ou des enquêtes douanières.

recours à des dispositifs complexes de recueil de renseignements, dans des conditions parfois susceptibles de porter une atteinte importante à la vie privée des personnes concernées. La CNCTR est particulièrement attentive aux conditions de mise en œuvre de ces techniques et exerce sur elles un contrôle renforcé. Toutefois, le temps nécessairement limité consacré aux contrôles sur place et sur pièces, les conditions dans lesquelles ils sont réalisés et le nombre restreint d'outils mis à disposition de la commission par les services pour effectuer les vérifications nécessaires, ne permettent pas aux agents de la CNCTR de contrôler des volumes de données en rapport avec ceux générés par l'augmentation de l'usage des techniques.

En outre, les formats actuels dans lesquels sont menés les contrôles sur place et sur pièces ne permettent pas à la commission de bénéficier de toute la réactivité exigée par certains dossiers.

Dans ces conditions, la multiplication de ces contrôles, tels qu'ils sont pratiqués depuis 2015, ne suffirait pas à elle seule à pallier ces difficultés en raison notamment de la lourdeur qu'ils représentent pour les effectifs de la commission comme des services de renseignement, de l'inadaptation de leurs locaux à une présence accrue de la commission et d'un matériel dédié peu efficace voire inadapté à un usage fréquent et renforcé.

Ces contraintes peuvent sans doute être allégées. Toutefois, il apparaît aujourd'hui nécessaire que les contrôles sur pièces et sur place soient doublés d'un renforcement des possibilités de contrôle à distance de la commission.

3.1.2 Une réflexion à poursuivre sur le développement de nouvelles modalités de contrôle *a posteriori* à distance

En complément des contrôles menés sur pièces et sur place, en particulier durant la troisième période de confinement imposé, en Ile-de-France, du 20 mars au 3 mai 2021, la CNCTR a poursuivi sa démarche de renforcement des contrôles réalisés à distance, depuis ses locaux.

Comme l'année précédente, elle s'est efforcée d'exploiter l'ensemble des capacités offertes par les outils informatiques mis à sa disposition par le

GIC. Ces derniers offrent actuellement à la commission un accès exhaustif aux données recueillies par la mise en œuvre des techniques de recueil de données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), de géolocalisation en temps réel (article L. 851 4 du même code), de balisage (article L. 851-5 du même code), d'interception de correspondances émises par la voie des communications électroniques auprès des opérateurs (I de l'article L. 852-1 du même code) ainsi, plus récemment, qu'à celles recueillies grâce aux techniques de captation de paroles et d'images (article L. 853-1 du code) qui font désormais l'objet d'une centralisation effective par le GIC (voir les développements ci-dessous).

La CNCTR a ainsi mis à profit l'ensemble de ses accès à distance pour diligenter des contrôles, parfois exhaustifs, de certains dossiers. En outre, le recours à la procédure de suivi des « productions »[73], c'est-à-dire des transcriptions réalisées par les agents des services de renseignement au cours de l'exploitation des techniques de renseignement, a été multiplié. La sélection des dossiers contrôlés a reposé sur la combinaison de différents critères tenant, notamment, au profil de la cible surveillée, au caractère perfectible de la motivation de la demande d'autorisation ou encore à la durée des surveillances autorisées.

En 2020, la CNCTR avait par ailleurs essayé de mettre en œuvre de nouvelles modalités d'échanges avec les services de renseignement à partir des moyens de communication sécurisés qui leur sont communs. Elle leur avait ainsi adressé, par voie numérique sécurisée, des demandes de précisions pouvant porter sur des aspects très divers de l'activité.

Cette forme d'échanges s'est toutefois heurtée aux réticences de la majorité des services de renseignement. Cette difficulté n'a pas été surmontée au cours de l'année 2021.

La mise en place d'un accès direct à distance apparaît dès lors comme la condition nécessaire pour prendre en compte le manque de disponibilité des services, tout en évitant que l'effectivité du contrôle dont la loi

73 - Cette procédure fait l'objet d'une description détaillée au point 2.2.1 du cinquième rapport d'activité pour l'année 2020 de la CNCTR.

charge la commission ne dépende que de la bonne volonté de ceux-ci. Ce besoin s'impose tout particulièrement en matière de surveillance des communications électroniques internationales, pour laquelle la commission ne dispose actuellement d'aucun moyen de contrôle à distance.

La poursuite de l'essor des contrôles à distance est, en outre, rendue indispensable par l'accroissement des missions de contrôle confiées à la CNCTR au terme des modifications législatives successives. Si ces extensions de compétence avaient, jusqu'à présent, pu être assumées à effectifs constants, les modifications introduites par la loi du 30 juillet 2021 auront, à court terme, un impact notable sur l'activité de la commission. En effet, les nouvelles techniques ou facultés que cette loi offre aux services de renseignement afin d'améliorer l'efficacité de leur action sont, en contrepartie, placés sous le contrôle de la CNCTR[74]. La commission doit, dès lors, disposer des moyens lui permettant d'exercer la mission qui lui est assignée.

La commission rappelle à cet égard qu'elle s'appuie essentiellement, pour conduire ses contrôles, sur une équipe de onze chargés de mission recrutés pour leurs connaissances juridiques ou techniques[75]. Si la commission envisage un renforcement de ses effectifs, celui-ci devra être accompagné d'une amélioration de ses moyens techniques pour atteindre des résultats suffisants.

Au demeurant, le développement des contrôles à distance permettrait à la CNCTR de mobiliser efficacement ses moyens matériels et humains pour accomplir sa mission, ce dont les services tireraient également profit.

Les contrôles sur pièces et sur place gagneraient en effet en pertinence et seraient, en même temps, plus condensés et plus approfondis. Ils permettraient à la délégation de la CNCTR et aux représentants du service concerné de concentrer leurs échanges sur les seules questions de fond et de mener ainsi un dialogue utile sur les points de désaccord éventuels ou d'incompréhension.

74 - Pour une présentation des modifications introduites par la loi du 30 juillet 2021 et de leurs enjeux en matière de contrôle, voir les points 1.1.1 et 2.2 du présent rapport.

75 - Voir l'encadré consacré aux moyens financiers et humains de la CNCTR au point 2 du présent rapport.

Le contrôle à distance ne permettra pas à la commission de vérifier de manière exhaustive la mise en œuvre de l'ensemble des techniques autorisées. La CNCTR procédera toujours, comme elle le fait aujourd'hui, par sélection de dossiers et par sondage. Cette démarche permettra néanmoins d'affiner et d'enrichir cette sélection afin d'identifier les dossiers ou les sujets qui méritent une attention particulière, des explications complémentaires et, le cas échéant, une présentation de la part du service concerné.

En outre, ainsi qu'il a été dit, ces contrôles « dématérialisés » n'ont pas vocation à se substituer à ceux diligentés dans les locaux des services de renseignement, qui donnent l'occasion d'un dialogue fructueux avec les services. Ils constituent une modalité complémentaire d'exercice du contrôle permettant d'améliorer la qualité des contrôles menés sur pièces et sur place et de faire face à l'augmentation du volume de données recueillies par les services de renseignement.

3.2 Le contrôle du recueil et de l'exploitation des données issues des techniques de renseignement : quelques difficultés montrant le besoin d'une meilleure sécurisation juridique à différents niveaux de la chaîne du renseignement

Alors que la mise en œuvre des contrôles à distance a connu un résultat mitigé, la CNCTR dresse, à l'instar des années précédentes, un bilan positif des contrôles sur pièces et sur place et se montre satisfaite des conditions dans lesquelles ses délégations ont été accueillies.

3.2.1 Une maîtrise du cadre juridique par la plupart des acteurs

La pratique des contrôles *a posteriori* révèle que les cellules ou bureaux juridiques des services justifient d'une excellente maîtrise du cadre juridique en vigueur depuis 2015, qu'il s'agisse de celui applicable aux techniques de renseignement mises en œuvre sur le territoire national comme de celui régissant la surveillance des communications électroniques internationales. Néanmoins, comme les années précédentes, la CNCTR a relevé certaines irrégularités, parfois récurrentes. Force est de constater que le cadre juridique n'est pas assimilé par l'ensemble des acteurs intervenant dans le cycle de vie d'une technique de renseignement. Les services doivent dès lors poursuivre leurs efforts de formalisation et de diffusion du cadre d'emploi des techniques de renseignement, en particulier au stade de l'exploitation de ces techniques.

Dans son quatrième rapport d'activité pour l'année 2019[76], la commission indiquait que plusieurs services avaient notamment rédigé des guides méthodologiques pour chaque métier impliqué dans la mise en œuvre d'une technique de renseignement, de l'enquêteur ou de l'analyste sollicitant la

76 - Voir en particulier le point 3.1.3.2 du quatrième d'activité pour l'année 2019 de la CNCTR.

surveillance à l'agent technique et opérationnel la mettant en œuvre sur le terrain. Des démarches d'homogénéisation des outils informatiques devaient en outre assurer la centralisation et la traçabilité de l'exploitation des techniques de renseignement. Si ces évolutions s'inscrivent nécessairement dans la durée et ont été ralenties sous l'effet de la crise sanitaire, la commission souligne la nécessité qu'elles soient menées à leur terme.

Les irrégularités constatées au cours de l'année 2021 relèvent, pour l'essentiel, de catégories déjà constatées au cours des années précédentes.

La plupart d'entre elles ont été signalées aux services concernés au cours des contrôles et rapidement corrigées par leurs agents. Dans un cas cependant, la CNCTR a décidé de saisir formellement le chef du service par un courrier lui recommandant la destruction immédiate de certaines des données recueillies.

3.2.1.1 Les irrégularités constatées en matière de surveillance intérieure

La **première catégorie** d'irrégularités, constatées à trois reprises en 2021 (contre huit en 2019 et une en 2020), a consisté en un court dépassement de la durée légale de conservation des données brutes collectées par la mise en œuvre d'une technique de renseignement. La CNCTR rappelle qu'en application des dispositions de l'article L. 822-2 du code de la sécurité intérieure, les renseignements collectés doivent être détruits avant l'expiration d'un certain délai, dont la durée varie en fonction de la nature des données et de l'atteinte portée à la vie privée. Les opérations de destruction doivent être réalisées par des agents habilités et désignés à cet effet, et faire l'objet de relevés auxquels la commission dispose d'un accès permanent, complet et direct conformément au 2° de l'article L. 833-2 du code de la sécurité intérieure.

La **deuxième catégorie** d'irrégularités a trait au dépassement de la durée d'autorisation d'une technique de renseignement. Comme en 2020, une seule irrégularité de cette nature a été relevée en 2021 (trois en 2019). Le service avait, en l'espèce, omis d'interrompre une technique au terme d'une première période d'autorisation. La demande de renouvellement de cette surveillance était toutefois en cours d'instruction.

Dans les deux cas, la CNCTR a veillé à ce que les données irrégulièrement conservées ou les renseignements collectés en dehors des périodes d'autorisation soient détruits dans les plus brefs délais. La commission estime que les irrégularités précédemment décrites ne relèvent pas d'une démarche intentionnelle mais témoignent de négligences ou d'insuffisances dans la gestion et le suivi de la mise en œuvre des techniques de renseignement.

La **troisième catégorie** d'irrégularités observées en 2021 correspond à des retranscriptions de conversations obtenues par la mise en œuvre de techniques d'interceptions de sécurité ou de captation de paroles ne présentant aucun lien apparent avec l'une des finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure.

La commission rappelle qu'en complément des vérifications opérées par le GIC sur l'ensemble des transcriptions réalisées par les agents des services au cours de l'exploitation des techniques de renseignement, les agents de la CNCTR examinent également eux-mêmes ces « productions », pour la préparation des contrôles menés sur pièces et sur place ou lorsqu'ils réalisent des contrôles dématérialisés depuis les locaux de la commission, afin d'apprécier leur pertinence au regard des finalités motivant l'autorisation à laquelle elles se rapportent.

Comme indiqué précédemment, la CNCTR a généralisé le recours à cette procédure au cours de l'année 2021 et l'a même systématisé pour les dossiers inscrits à l'ordre du jour des contrôles programmés dans les locaux des services. En outre, la commission a vérifié l'intégralité des transcriptions réalisées à partir des techniques de renseignement mises en œuvre à l'égard des personnes exerçant l'une des professions ou mandats « protégés » par l'article L. 821-7 du code de la sécurité intérieure[77] afin de s'assurer du caractère nécessaire et proportionné des atteintes portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats.

Lorsqu'une irrégularité de ce type est détectée, la CNCTR engage systématiquement un dialogue approfondi avec le service concerné afin de recueillir ses observations. Elle détermine ensuite si, à la lumière des

77 - C'est-à-dire les parlementaires, les magistrats, les avocats et les journalistes.

précisions apportées, les transcriptions litigieuses apparaissent justifiées ou doivent, au contraire, être détruites. En général, le constat d'irrégularité est partagé avec le service concerné et tout ou partie des transcriptions concernées sont détruites dans de brefs délais.

La **quatrième catégorie** d'irrégularités, constatées à deux reprises en 2021, concerne des extractions ou des transcriptions de données ne présentant aucun lien avec la cible faisant l'objet de la technique de renseignement. Dans un cas, les données irrégulièrement conservées ont été détruites dans les plus brefs délais. Dans l'autre, la CNCTR a estimé nécessaire d'exercer de manière formelle son pouvoir de recommandation, en application des dispositions de l'article L. 833-6 du code de la sécurité intérieure.

Au cours d'un contrôle sur pièces et sur place, la CNCTR avait signalé aux représentants du service concerné que plusieurs extractions, en l'espèce des photographies, réalisées à partir de trois techniques de renseignement ne présentaient aucun lien apparent, ni avec la cible placée sous surveillance, ni avec l'un des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code de la sécurité intérieure.

Un courrier électronique sécurisé invitant le service à faire valoir les motifs susceptibles de justifier la conservation des extractions avait ensuite été adressé. Alors que les explications fournies n'avaient pas permis d'établir le caractère indispensable des extractions à la poursuite de l'une des finalités légales, le service entendait néanmoins les conserver.

Dans ces conditions, le président de la CNCTR a adressé au chef du service concerné, au ministre de tutelle ainsi qu'au Premier ministre une recommandation de destruction immédiate des extractions en litige, où qu'elles se trouvent, sous forme d'impression papier ou de fichier informatique.

La CNCTR a pu s'assurer que sa recommandation avait été intégralement mise en œuvre sans qu'il soit besoin de faire usage de la faculté, permise par les dispositions de l'article L. 833-8 du code de la sécurité intérieure, de saisir le Conseil d'État d'un recours.

La **cinquième catégorie** d'irrégularités décelées en matière de surveillance intérieure concerne la traçabilité de l'exploitation des données recueillies. Dans une vingtaine de cas en 2021, contre une dizaine l'année précédente, des extractions ou des transcriptions issues de techniques de renseignement n'ont pas été signalées à la commission et ne lui ont pas été rendues immédiatement accessibles. Le plus souvent, la CNCTR a été informée de leur existence par les exploitants des services de renseignement rencontrés au cours des contrôles sur place. Lorsque la commission a souhaité consulter les extractions ou les transcriptions sur les applications informatiques des services concernés, celles-ci ne s'y trouvaient pas. La CNCTR a alors exigé que les transcriptions manquantes lui soient communiquées dans les plus brefs délais et qu'elles soient, en outre, intégrées dans les applications informatiques dédiées.

La CNCTR rappelle qu'elle dispose en effet, en application du 2° de l'article L. 833-2 du code de la sécurité intérieure, d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions. Cet accès est garanti par la loi, quels que soient les supports, fichiers ou documents comportant des éléments obtenus grâce à la mise en œuvre d'une technique de renseignement.

Par ailleurs, l'article L. 822-4 du même code prévoit que les transcriptions et les extractions font l'objet de relevés tenus à la disposition de la commission. En outre, depuis l'entrée en vigueur de la loi du 30 juillet 2021, cet article impose désormais que les relevés précisent si les transcriptions et extractions ont été effectuées pour une finalité différente de celle qui en a justifié le recueil et, dans cette éventualité, qu'ils soient immédiatement transmis à la CNCTR[78].

La commission considère, à ce stade, que les anomalies relevées ne témoignent pas d'une volonté délibérée de dissimulation ou de contournement du cadre légal. Leur portée ne doit, toutefois, pas être sous-estimée. Elles constituent, en pratique, une limite à l'efficacité du contrôle *a posteriori* de la CNCTR. Elles mettent en évidence les difficultés d'appropriation des bonnes pratiques par certains agents des services de renseignement. En dépit des efforts déployés par les équipes juridiques de ces services pour formaliser, expliquer et diffuser

78 - Voir les points 1.1.1 et 2.2 du présent rapport.

le cadre d'emploi des techniques de renseignement, les procédures internes visant à centraliser l'ensemble des extractions et transcriptions réalisées dans des applications informatiques accessibles à la CNCTR ne sont pas encore correctement appliquées.

La situation est, en revanche, satisfaisante s'agissant de la traçabilité de la mise en œuvre des techniques de renseignement autorisées[79]. Les efforts constatés par la CNCTR en 2020 ont été confirmés en 2021. Comme l'année précédente, aucune divergence entre les mentions portées dans une fiche de traçabilité et la mise en œuvre effective de la technique correspondante n'a été constatée. De même, aucune carence dans la production de ces fiches n'est à signaler. Des retards subsistent encore mais diminuent.

Enfin, dans un seul cas constitutif de la **sixième catégorie** d'irrégularités, un service de renseignement a procédé au retrait d'un dispositif de balisage sans avoir sollicité l'autorisation, requise, de s'introduire dans un lieu privé. Cette carence a été spontanément signalée par le service concerné. Il ressort des explications fournies à la CNCTR que l'opération, telle qu'elle était initialement envisagée par le service, ne nécessitait pas de s'introduire dans un lieu de cette nature. Une opportunité opérationnelle de procéder, sans risque, au retrait du matériel en s'introduisant dans un tel lieu s'est cependant présentée. Les techniciens présents sur place n'avaient pas conscience de l'irrégularité de leur intervention. Au demeurant il s'agissait, en l'espèce, de retirer un matériel de surveillance, autrement dit de mettre un terme à l'atteinte portée à la vie privée de la personne ciblée. La CNCTR a néanmoins recommandé au service de solliciter systématiquement, à l'avenir, une autorisation d'introduction dans un lieu privé pour des opérations semblables afin de prévenir la réitération d'un tel dysfonctionnement. Elle a également rappelé que, dans des circonstances exceptionnelles caractérisées par l'urgence, une autorisation peut être sollicitée selon la procédure prioritaire et validée, le cas échant, en moins d'une heure. La commission a, en outre, invité le service à lui présenter en détail le circuit interne de validation et de suivi

79 - La commission rappelle qu'en application de l'article L. 822-1 du code de la sécurité intérieure, un relevé de mise en œuvre de chaque technique de renseignement, mentionnant les dates de début et de fin de mise en œuvre ainsi que la nature des renseignements collectés, doit être établi. Ce relevé, plus couramment désigné « fiche de traçabilité », est tenu à la disposition de la commission qui peut y accéder de manière permanente, complète et directe quel que soit son degré d'achèvement.

des demandes de techniques afin d'identifier le stade au cours duquel l'erreur a pu se produire et déterminer les mesures correctrices adaptées.

Pour ce qui concerne, en tout dernier lieu, la transmission de renseignements entre services, la CNCTR rend compte, dans le point 2.2.1 de ce rapport, d'une irrégularité détectée lors d'un contrôle effectué dans un service du « second cercle ». Le lecteur est invité à s'y reporter.

3.2.1.2 Les irrégularités constatées en matière de surveillance des communications électroniques internationales

Comme en matière de surveillance intérieure, la CNCTR réalise des contrôles réguliers des conditions de recueil, de conservation et d'exploitation des données issues de la surveillance des communications électroniques internationales, en application de l'article L. 854-9 du code de la sécurité intérieure.

En l'absence d'accès direct, depuis ses locaux, à ces données, tous les contrôles sont réalisés sur pièces et sur place, au sein des services de renseignement. Ces contrôles mettent en évidence, depuis 2015, une appropriation progressive et désormais solide par les services, du cadre légal applicable en matière de surveillance dite « internationale », en dépit de sa complexité.

La CNCTR a relevé, au cours de l'année 2021, des irrégularités se répartissant en trois grandes catégories. Les deux premières avaient déjà été exposées dans le rapport d'activité de la commission pour l'année 2020. La plupart d'entre elles ont été signalées aux services concernés au cours des contrôles et rapidement corrigées.

La **première catégorie** d'irrégularités concerne des consultations et des exploitations réalisées sur le fondement d'une autorisation inappropriée. Aux termes de l'article L. 854-2 du code de la sécurité intérieure, le Premier ministre peut délivrer différents types d'autorisation d'exploitation des données (de connexion ou de contenu) interceptées par les réseaux de communications électroniques internationales. Ainsi, il peut autoriser l'exploitation non individualisée des données de connexion interceptées (II du même article), l'exploitation des communications ou des seules données de connexion, relatives à des zones géographiques, à des organisations, à des groupes de personnes ou à des personnes (III) ou

encore l'exploitation des communications ou des seules données de connexion, de numéros d'abonnement ou d'identifiants techniques rattachables au territoire national dont l'utilisateur communique depuis ce territoire (V).

L'exploitation de ces données est réalisée par des agents spécialisés, à partir d'applications informatiques spécifiques dont les droits et les conditions matérielles d'accès sont strictement limités et contrôlés.

La CNCTR a découvert, à plusieurs reprises, que des consultations ou des exploitations de données avaient été informatiquement rattachées à une autorisation erronée alors que l'autorisation pertinente était en cours de validité. Ce type d'anomalies, déjà constaté les années précédentes, est encore fréquent. Les explications fournies par les services révèlent que ces anomalies résultent de négligences de la part des agents exploitants ou d'erreurs de manipulation de l'outil informatique, lequel assiste l'utilisateur en lui proposant, à chaque nouvelle requête, la précédente autorisation sélectionnée. Les formations dispensées aux agents ainsi que les nombreux rappels effectués par les équipes juridiques des services de renseignement permettent de réduire progressivement ces irrégularités.

La **seconde catégorie** d'irrégularités concerne des exploitations de données réalisées cette fois sur le fondement de la bonne autorisation mais excédant les limites qui lui sont attachées. Quelques difficultés ont été rencontrées en 2021. D'une part, la CNCTR s'est aperçue que des transcriptions issues de l'exploitation de communications utilisant un identifiant technique rattachable au territoire national avaient été réalisées au titre d'une finalité légale non autorisée. L'autorisation prévue au V de l'article L. 854-2 du code de la sécurité intérieure ne peut en effet être délivrée que pour la défense ou la promotion des finalités mentionnées aux 1°, 2°, 4°, 6° et 7° de l'article L. 811-3 du même code. À une reprise en 2021 (contre deux en 2020), la CNCTR a constaté que les éléments transcrits et conservés par le service concerné se rattachaient à une finalité différente, non prévue dans cette liste, de celle ayant servi de fondement à l'autorisation délivrée par le Premier ministre. Le service concerné a admis le caractère irrégulier des transcriptions et a procédé à leur destruction dans les jours qui ont suivi les contrôles au cours desquels elles ont été détectées. D'autre part, la CNCTR a découvert, plusieurs fois, une

exploitation de données se rapportant à des cibles expressément exclues par l'autorisation délivrée par le Premier ministre. Si ces irrégularités n'ont pas révélé une intention délibérée de contournement de l'autorisation accordée, leur répétition a cependant conduit le président de la CNCTR, au tout début de l'année 2022, à formellement demander au service concerné de venir lui exposer les procédures mises en œuvre pour prévenir leur renouvellement.

Une **troisième catégorie** d'irrégularités a concerné ce que le IV de l'article L. 854-2 du code de la sécurité intérieure désigne comme des « vérifications ponctuelles ». Il s'agit d'une exploitation individualisée réalisée aux seules fins de détecter une menace pour les intérêts fondamentaux de la Nation liée aux relations entre des numéros d'abonnement ou des identifiants techniques rattachables au territoire français et des zones géographiques, organisations ou personnes faisant l'objet d'une surveillance. Les recherches constituant la vérification ponctuelle ne peuvent excéder une certaine durée. Or, à plusieurs reprises, la CNCTR a constaté que cette durée n'avait pas été respectée. À la suite des recommandations formulées par la commission, le service concerné étudie la possibilité de développer un processus informatique automatisé empêchant toute vérification au-delà d'un certain délai.

Le constat d'une irrégularité, quelle que soit la suite que la CNCTR entend lui réserver, donne systématiquement lieu à un échange approfondi entre la commission et le service concerné. Il permet d'identifier précisément la ou les étapes des processus internes au cours desquelles est survenue l'irrégularité afin de déterminer les éventuels ajustements à apporter pour prévenir toute réitération.

La commission estime en effet que, si elle a la faculté d'adresser une recommandation formelle au service concerné, au ministre de tutelle ainsi qu'au Premier ministre tendant à l'interruption d'une technique de renseignement et à la destruction de renseignements indûment collectés, sa mission est d'abord préventive. Elle cherche ainsi à accompagner et, dans certains cas, à guider la mise en œuvre de bonnes pratiques au sein des services de renseignement pour assurer le plein respect du cadre légal.

En outre, les développements informatiques déployés par certains services de renseignement, en concertation avec la CNCTR, ont permis d'améliorer la traçabilité des actions effectuées par les exploitants et, ce faisant, d'approfondir et faciliter les contrôles de la commission.

3.2.2 Des améliorations encore nécessaires pour renforcer la centralisation des données recueillies et la traçabilité de leur exploitation

La CNCTR rappelle régulièrement l'importance de deux exigences légales dont dépendent l'efficacité et la pertinence des contrôles *a posteriori* qu'elle réalise : d'une part, la centralisation du recueil et de l'exploitation des données issues des techniques de renseignement ; d'autre part, la traçabilité de la mise en œuvre des techniques et de l'exploitation des données recueillies.

3.2.2.1 La centralisation des données : des enjeux renouvelés par la révision du cadre législatif applicable au renseignement

La centralisation des données recueillies est indispensable à l'exercice du contrôle *a posteriori* dont la commission a été chargée par la loi. Comme elle avait pu le souligner dans ses précédents rapports d'activité, la CNCTR voit ses capacités d'accès immédiat, c'est-à-dire depuis ses locaux, s'étendre depuis 2017.

En 2019, le GIC a entrepris la centralisation, dans son système d'information, des paroles et des images captées sur le fondement des dispositions de l'article L. 853-1 du code de la sécurité intérieure[80].

La centralisation de la technique de captation de paroles, devenue effective dans le courant de l'année 2020, présentait toutefois quelques dysfonctionnements susceptibles d'affecter la réactivité opérationnelle des services. Ces difficultés ont été surmontées en 2021. Désormais, l'ensemble des services, à l'exception de la direction générale de la sécurité extérieure (DGSE) et de la direction générale de la sécurité intérieure

80 - Voir le point 3.1.3.1 du quatrième rapport d'activité pour l'année 2019 de la CNCTR.

(DGSI) qui disposent de leurs propres dispositifs de centralisation, ont adopté la solution technique fournie par le GIC.

L'accès aux données « brutes » collectées par la mise en œuvre de cette technique est possible depuis les locaux des services de renseignement ou depuis les centres d'exploitation à distance du GIC. L'exploitation de ces données, par la réalisation de transcriptions ou d'extractions, s'effectue prioritairement dans les locaux du GIC. Les services disposant d'espaces et de systèmes d'information répondant aux normes de sécurité définies dans l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale peuvent néanmoins solliciter l'installation de postes informatiques fournis et administrés par le GIC dotés d'une application sécurisée leur permettant d'exploiter les données au sein de leurs locaux. Dans les deux cas, les données sont centralisées dans le système d'information classifié du GIC.

En outre, l'ensemble des transcriptions et extractions réalisées par les services sont soumises à la validation du GIC, ainsi qu'au contrôle de la CNCTR. La commission bénéfice en effet d'un accès direct et immédiat, depuis ses locaux, à l'ensemble des renseignements collectés, transcriptions et extractions.

La centralisation de la technique de captation d'images, qui était en cours de finalisation à la fin de l'année 2020, est devenue pleinement opérationnelle en 2021. Elle s'opère dans les mêmes conditions et selon les mêmes modalités que la technique de captation de paroles.

Ces avancées sont un outil précieux pour l'exercice des contrôles menés par la CNCTR. Il convient toutefois de préciser que la centralisation de ces données n'est réellement effective que pour les dispositifs d'enregistrement sonore ou vidéo en continu. Dans ce cas, les données recueillies sont soit directement renvoyées, à distance, sur les serveurs du GIC, soit, lorsque des contraintes techniques ou opérationnelles y font obstacle, manuellement injectées dans le système d'information du GIC au moyen de postes d'import spécifiques installés dans les centres « GIC » ou dans les locaux de certains services. Dans d'autres cas, notamment lorsque la surveillance se limite à la prise de clichés photographiques ou à des opérations ponctuelles et mobiles de captation sonore, les données sont conservées et exploitées au sein des locaux des services de renseignement. Les indications portées

dans les relevés de mise en œuvre, plus couramment dénommés « fiches de traçabilité »[81], permettent à la CNCTR d'avoir connaissance des modalités de mise en œuvre des techniques et des matériels utilisés. Ces opérations ne peuvent toutefois être contrôlées qu'à l'occasion d'un déplacement dans les locaux des services concernés.

La plupart des techniques de renseignement sont ainsi couvertes par le dispositif de centralisation du GIC, à l'exception encore des techniques de recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) et de celles de recueil ou de captation de données informatiques (article L. 853-2 du même code), toutes deux caractérisées par une collecte décentralisée et des modalités diverses de stockage des données recueillies.

Les projets de développement de réseaux informatiques sécurisés capables d'acheminer les données volumineuses recueillies et d'organiser leur centralisation ont peu avancé cette année encore, laissant ainsi subsister un stockage décentralisé au sein des directions centrales ou d'échelons territoriaux des services de renseignement. Si la CNCTR a, comme les années précédentes, mené plusieurs contrôles sur pièces et sur place dans des unités territoriales des services de renseignement, les moyens matériels et humains limités dont elle dispose ne lui permettront pas de contrôler un volume de données en rapport avec ceux générés par l'augmentation à venir du recours aux techniques de recueil de données de connexion par *IMSI catcher* et de recueil ou de captation de données informatiques[82].

Dans ces conditions, l'accès à distance, c'est-à-dire depuis ses locaux, de la CNCTR aux données recueillies par la mise en œuvre de ces techniques pourrait devenir une contrepartie appropriée et nécessaire à l'absence de centralisation.

Par ailleurs, la CNCTR rappelle que la loi du 30 juillet 2021 ouvre aux services de renseignement la possibilité d'intercepter des correspondances émises ou reçues par la voie satellitaire à l'aide d'un dispositif de captation spécifique, lorsque cette interception ne peut être mise en œuvre avec le concours des opérateurs, selon le régime de droit commun des

81 - Voir le point 3.2.2.2 du présent rapport.

82 - Voir les développements du point 3.1 du présent rapport.

interceptions de sécurité. Le GIC se voit confier la mission d'organiser la centralisation des données recueillies par la mise en œuvre de la technique désormais 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* ». En cas d'impossibilité technique, les données recueillies sont chiffrées dès leur collecte et jusqu'à leur centralisation effective au sein du GIC. Le législateur a, en outre, précisé que les opérations de transcription et d'extraction des communications interceptées doivent être réalisées au sein du GIC.

Dans sa délibération n° 3/2021 du 14 avril 2021[83], la CNCTR soulignait l'importance d'une centralisation immédiate, c'est-à-dire d'un acheminement direct et en temps réel des flux interceptés vers les installations du GIC, mais constatait que les modalités concrètes étaient encore vagues.

La capacité technique de procéder à une centralisation immédiate dépendra essentiellement du type de matériel utilisé pour procéder à l'interception et du niveau de protection dont bénéficieront les données interceptées. Quoi qu'il en soit, des développements sont attendus au cours de l'année 2022 afin de permettre le déploiement d'un dispositif technique présentant les garanties voulues par le législateur pour permettre à la CNCTR d'exercer un contrôle efficace et pertinent.

3.2.2.2 Une situation globalement satisfaisante pour la traçabilité de la mise en œuvre des techniques ; des difficultés récurrentes, en revanche, dans la traçabilité de l'exploitation

L'efficacité et la pertinence des contrôles *a posteriori* dépendent également de la traçabilité de la mise en œuvre et de l'exploitation des techniques de renseignement.

S'agissant de leur mise en œuvre, la CNCTR constate que la tendance positive constatée à compter de 2017 n'a cessé de progresser depuis lors.

Pour mémoire, chaque technique de renseignement autorisée doit donner lieu à l'établissement d'un relevé ou « fiche de traçabilité » indiquant si la technique a pu ou non être mise en œuvre et mentionnant les dates de

83 - Cette délibération est publiée en annexe n°3 au présent rapport et disponible sur le site Internet de la commission.

début et de fin de mise en œuvre ainsi que la nature des renseignements collectés et le matériel utilisé. Ce relevé est tenu à la disposition de la commission qui peut y accéder de manière permanente, complète et directe quel que soit son degré d'achèvement.

Ces fiches sont en principe rédigées dès la fin de la mise en œuvre d'une technique ou, en l'absence de mise en œuvre, dès l'arrivée à échéance de l'autorisation. Grâce aux applications mises à sa disposition par le GIC, la commission peut vérifier de façon immédiate l'existence et le contenu des relevés, qui contribuent à la préparation des contrôles sur pièces et sur place au sein des services de renseignement mais peuvent être aussi l'occasion d'échanges entre la commission et les services destinés à préciser l'état de mise en œuvre d'une technique. La refonte des interfaces dédiées à la transmission et à la mise à disposition des fiches de traçabilité lancée par le GIC en 2020 a progressé en 2021 et devrait être déployée au cours des deuxième et troisième trimestres de l'année 2022.

Grâce à la rigueur et de la diligence avec laquelle la plupart des services s'efforcent de renseigner ces fiches de traçabilité, seules quelques-unes d'entre-elles manquaient à la fin de l'année 2021.

La traçabilité de la mise en œuvre des techniques de renseignement se heurte néanmoins à une difficulté concernant les rares techniques de renseignement dont la validation n'est pas réalisée sur les applications informatiques du GIC mais par des canaux de transmission différents. Il s'agit notamment des interceptions de correspondances échangées au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs (article L. 852-2) et des autorisations de mise en œuvre des algorithmes (article L. 851-3).

En effet, l'absence d'outil assurant la centralisation des demandes d'autorisation de ces techniques impose à la CNCTR de solliciter directement les services demandeurs ou le GIC afin de connaître l'état de leur mise en œuvre, le volume des données éventuellement recueillies ou encore la date de délivrance et d'échéance de l'autorisation délivrée par le Premier ministre.

S'agissant de la traçabilité de l'exploitation des données recueillies, la situation a peu évolué depuis l'an passé et n'est pas satisfaisante.

Poursuivant sa démarche d'approfondissement et de perfectionnement du contrôle *a posteriori* dont la loi l'a chargée, la CNCTR s'efforce depuis 2018, de renforcer son contrôle sur la phase d'exploitation des données recueillies, en particulier sur la réalisation, la diffusion et la conservation des transcriptions et des extractions de ces données. Les renseignements bruts collectés par la mise en œuvre d'une technique de renseignement sont, en effet, exploités afin d'en tirer les informations pertinentes, qui seront ensuite intégrées dans les documents d'analyse produits par les services de renseignement. Cette exploitation, qui consiste à examiner et à trier les données brutes recueillies, peut prendre la forme d'extractions ou de transcriptions qui pourront être conservées tant qu'elles demeurent indispensables à la poursuite des finalités qui ont motivé leur réalisation.

Pour assurer son contrôle, la CNCTR dispose, en application du 2° de l'article L. 833-2 du code de la sécurité intérieure, d'un accès permanent, complet, direct et, pour certaines techniques, immédiat, aux relevés, registres, renseignements collectés, transcriptions et extractions. Cet accès est garanti par la loi, où que ces éléments se trouvent.

Dans l'hypothèse où un service de renseignement refuserait à la CNCTR l'accès à certains lieux, physiques ou logiciels, de conservation des transcriptions et des extractions, l'article L. 833-2 du code de la sécurité intérieure permet à celle-ci de demander ces éléments au Premier ministre, à l'exclusion de ceux communiqués par des services étrangers ou qui donneraient connaissance à la commission, directement ou indirectement, de l'identité des sources des services de renseignement. L'article L. 833-3 du même code punit d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'entraver l'action de la CNCTR en refusant de lui communiquer les documents qu'elle a sollicités en application de l'article L. 833-2, en dissimulant ces documents ou en les faisant disparaître.

En pratique, d'importants progrès restent à accomplir en matière de suivi de l'exploitation des données recueillies par les techniques de renseignement.

Comme la CNCTR l'indiquait dans ses précédents rapports d'activité, la majorité des services de renseignement lui refusent l'accès aux données contenues dans les fichiers intéressant la sûreté de l'État au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, communément dénommés « fichiers de souveraineté »[84].

Ces services justifient leur position par le fait qu'outre les données issues de techniques de renseignement, figureraient, dans ces fichiers, des données de provenances différentes, incluant des données communiquées par des services étrangers ou des éléments susceptibles de dévoiler, directement ou indirectement, l'identité des sources des services de renseignement, non soumis au contrôle de la CNCTR[85].

Faute de pouvoir accéder à ces fichiers, la commission ne peut, en l'état, s'assurer qu'ils ne contiennent pas d'éléments issus de renseignements collectés, transcrits, extraits voire transmis irrégulièrement et qu'il n'y subsiste aucune trace de données dont la destruction a été demandée puis réalisée à la suite d'un contrôle. Cette limite s'applique notamment aux vérifications ayant conduit à la détection des anomalies décrites au point 3.2.1.1 de ce rapport.

Au cours de l'année 2019, des solutions alternatives à l'accès aux fichiers de souveraineté ont été proposées à la CNCTR afin qu'elle puisse exercer son contrôle sur les données issues de techniques de renseignement susceptibles de venir alimenter les notes, bulletins de renseignement et fichiers de souveraineté.

Ces propositions, jugées constructives, avaient été accueillies favorablement par la commission dès lors que leur développement pouvait faire escompter des progrès en matière de centralisation des données et contribuer ainsi à améliorer l'efficacité des contrôles.

84 - Voir notamment l'article R. 841-2 du code de la sécurité intérieure.

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

Le constat de leur mise en œuvre est cependant décevant. Les résultats initialement annoncés par les services de renseignement n'ont pas été atteints au cours de l'année 2020 en raison des difficultés engendrées par la crise sanitaire. Au terme de l'année 2021, force est de constater que la situation n'a pas progressé.

Les rares solutions élaborées par les services consistant, pour l'essentiel, à synthétiser dans un tableur informatique les données issues de techniques de renseignement destinées à alimenter les documents d'analyse, les notes et les fichiers de souveraineté, n'ont, en pratique, pas été exécutées avec rigueur. Les informations renseignées se sont révélées très largement incomplètes, imprécises et parfois inexactes.

La commission forme le vœu qu'une solution soit trouvée à ce problème avec l'aide du Premier ministre, de manière à éviter l'existence d'une faille dans la garantie « de bout en bout » du contrôle qu'exige la jurisprudence de la Cour de Strasbourg. Elle rappelle que le Premier ministre a aussi la faculté de saisir le Conseil d'État d'une demande d'avis permettant d'éclairer l'exacte portée de l'article L. 833-2 s'agissant des fichiers de renseignement.

4. Un exercice limité des voies de recours ouvertes contre la mise en œuvre des techniques de renseignement

4.1 Une légère progression du nombre de réclamations adressées à la CNCTR

La CNCTR peut être saisie par toute personne qui souhaite vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Cette procédure de réclamation préalable est prévue par les dispositions de l'article L.833-4 du code de la sécurité intérieure, en ce qui concerne la surveillance nationale, et par celles de l'article L. 854-9 du même code, en ce qui concerne la surveillance des communications électroniques internationales.

Comme la CNCTR le précisait dans ses précédents rapports d'activité, le pouvoir de vérification que la loi lui a confié porte sur les seules techniques de renseignement prévues au livre VIII du code de la sécurité intérieure, à savoir des mesures de surveillance mises en œuvre par les services de renseignement au titre de leurs missions de police administrative. Cette compétence ne s'étend ni aux mesures de surveillance ordonnées par l'autorité judiciaire ni à celles, au demeurant illégales, que pratiqueraient des personnes privées.

La CNCTR souligne, par ailleurs, une nouvelle fois[86] que, pour des motifs de sécurité nationale, et en application des dispositions du décret n° 2015-1405 du 5 novembre 2015 relatif aux exceptions à l'application du droit des usagers de saisir l'administration par voie électronique, elle ne peut valablement être saisie que par lettre envoyée par voie postale.

86 - Cette obligation était précisée au point 5.1.1 du premier rapport d'activité pour la période 2015/2016 de la CNCTR.

La réclamation doit être présentée par la personne concernée, justifiant de son identité, et mentionner, le cas échéant, les éléments techniques à partir desquels elle souhaite que les vérifications soient conduites. Ces éléments techniques, notamment des numéros de téléphone ou des adresses de messagerie électronique, doivent être assortis de justificatifs, tels qu'un contrat d'abonnement ou une facture. Les vérifications ne peuvent avoir lieu que lorsque l'ensemble de ces informations et justificatifs a été communiqué à la commission.

La CNCTR instruit les réclamations qui lui sont adressées de la même manière et en utilisant les mêmes outils que lorsqu'elle effectue de sa propre initiative un contrôle *a posteriori* depuis ses locaux.

Le nombre de réclamations reçues par la CNCTR en 2021 est en hausse par rapport à 2020 et se rapproche des chiffres enregistrés en 2019. La commission souligne toutefois que le volume des réclamations dont elle est saisie relève du même ordre de grandeur depuis son installation, sans que les variations constatées d'une année sur l'autre puissent être regardées comme significatives.

	2016	2017	2018	2019	2020	2021
Nombre de réclamations	**49**	**54**	**30**	**47**	**33**	**48**

Aucune personne n'a présenté plus d'une réclamation au cours de l'année 2021. En revanche, six réclamations ont été présentées par des personnes ayant déjà saisi la CNCTR au cours des années antérieures et souhaitant que des vérifications soient à nouveau conduites à leur sujet.

Le délai de réponse aux réclamations contenant toutes les informations nécessaires à leur traitement a été inférieur à deux mois[87].

Aucune réclamation n'a conduit la CNCTR à envoyer de recommandation au chef du service de renseignement concerné, au ministre dont il relève ou au Premier ministre pour que la mise en œuvre d'une technique soit

87 - Ce délai court à compter de la date à laquelle la réclamation est en état d'être instruite. Lorsqu'une demande de pièces complémentaires (justificatifs d'identité, justificatifs d'abonnement…) a été adressée à l'auteur de la réclamation, ce délai ne commence à courir qu'à compter de la réception de ces pièces.

interrompue et les renseignements collectés détruits, conformément à l'article L. 833-6 du code de la sécurité intérieure. En conséquence, la CNCTR ne s'est pas non plus trouvée dans la situation de devoir saisir le Conseil d'État d'un recours contentieux sur le fondement de l'article L. 833-8 du code, cette voie de recours étant ouverte dans l'hypothèse où le Premier ministre ne donnerait pas suite aux recommandations de la commission.

Le dispositif propre aux « lanceurs d'alerte »

Pour garantir qu'il soit mis fin aux éventuelles violations manifestes du cadre juridique applicable aux techniques de renseignement, l'article L. 861-3 du code de la sécurité intérieure prévoit que les agents des services de renseignement ayant connaissance, dans l'exercice de leurs fonctions, d'une telle violation, peuvent porter ces faits à la connaissance de la seule CNCTR. Il appartient alors à la commission, au vu des éléments qui lui ont été transmis, de faire usage, le cas échéant, des pouvoirs de contrôle que lui attribue la loi.

En 2021, la CNCTR n'a pas été saisie sur le fondement de l'article L. 861-3 du code de la sécurité intérieure. Ces dispositions n'ont pas reçu d'application depuis l'entrée en vigueur du cadre légal en 2015.

4.2 Une stabilité du nombre de requêtes introduites devant le Conseil d'État

La procédure contentieuse spéciale prévue aux articles L. 773-1 et suivants du code de justice administrative permet de demander à une formation spécialisée du Conseil d'État de vérifier qu'une technique de renseignement n'est ou n'a pas été irrégulièrement mise en œuvre à l'encontre d'une personne. Les membres et le rapporteur public de la formation spécialisée sont habilités ès qualités à connaître d'informations couvertes par le secret de la défense nationale.

En ce qui concerne les techniques de renseignement relevant de la surveillance intérieure, la formation spécialisée du Conseil d'État peut être saisie, sur le fondement de l'article L. 841-1 du code de la sécurité intérieure, par toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR.

En ce qui concerne la surveillance des communications électroniques internationales, seul le président ou trois membres au moins de la commission peuvent présenter une requête au Conseil d'État, sauf s'il s'agit de vérifier la légalité de l'exploitation des communications de personnes utilisant des identifiants rattachables au territoire national et communiquant depuis la France. Dans ce dernier cas, toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR peut saisir le Conseil d'État, sur le fondement de l'article L. 854-9 du code de la sécurité intérieure.

Comme en 2020, huit nouvelles requêtes ont été enregistrées devant le Conseil d'État sur le fondement de l'article L. 841-1 du code de la sécurité intérieure en 2021. Celui-ci a statué sur seize requêtes au cours de l'année 2021 contre sept en 2020 et en 2019. Cette hausse est liée aux reports d'audiences décidés en 2020 en raison de la crise sanitaire.

Au 31 décembre 2021, trois affaires demeuraient en instance, enregistrées en 2021.

En application de l'article L. 773-3 du code de justice administrative, la CNCTR est informée de toute requête introduite sur le fondement de l'article L. 841-1 du code de la sécurité intérieure et est invitée à présenter, le cas échéant, des observations écrites ou orales. Elle a, ainsi, le statut d'observateur devant le Conseil d'État. En tant qu'autorité décisionnaire en matière d'autorisations de mise en œuvre des techniques de renseignement, le Premier ministre, représenté par le GIC, a la qualité de défendeur.

Comme les années précédentes, la CNCTR a produit des observations sur tous les recours qui lui ont été communiqués par le Conseil d'État.

Comme les années précédentes également, elle ne s'est pas trouvée dans la situation d'exercer elle-même un recours contentieux devant le Conseil d'État sur le fondement des articles L. 833-8 ou L. 854-9 du code de la sécurité intérieure. Cette voie de recours est ouverte au président de la commission ou à trois de ses membres, lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission. En 2021, les contrôles *a posteriori* effectués par la commission n'ont en effet pas révélé d'irrégularité justifiant l'envoi d'une recommandation au Premier ministre.

La commission n'a pas davantage été conduite à saisir le Conseil d'État d'une requête présentée dans les conditions prévues par les dispositions du deuxième alinéa de l'article L. 821-1 du code de la sécurité intérieure tel qu'il a été modifié par la loi du 30 juillet 2021. En application de ces dispositions, le président de la CNCTR ou l'un de ses membres ayant la qualité de magistrat, doit immédiatement saisir le Conseil d'État lorsque le Premier ministre délivre une autorisation de mise en œuvre d'une technique de renseignement après avis défavorable de la commission. La formation spécialisée mentionnée à l'article L. 773-2 du code de justice administrative, le président de la formation restreinte mentionnée au même article L. 773-2 ou le membre qu'il délègue statue alors dans un délai de vingt-quatre heures à compter de cette saisine. La décision d'autorisation du Premier ministre ne peut être exécutée avant que le Conseil d'État ait statué, sauf en cas d'urgence dûment justifiée et si le Premier ministre a ordonné sa mise en œuvre immédiate. En 2021, comme les années précédentes, le Premier ministre a suivi tous les avis défavorables émis par la CNCTR.

Le dialogue institutionnel avec le Parlement, l'information du public et les relations internationales

Au sein de la chaîne opérationnelle conduisant au recueil et à l'exploitation du renseignement, la CNCTR se voit confier par la loi une mission de contrôle qui ne peut, en application du principe de séparation des pouvoirs et eu égard aux exigences du secret de la défense nationale, être accomplie que par un organisme distinct non seulement du Gouvernement mais également du Parlement et du public. La commission se présente, dès lors, comme un « tiers de confiance », auquel le législateur a attribué une compétence spécialisée qu'il ne peut lui-même assurer directement. En retour, la CNCTR rend compte tout au long de l'année de ses activités au Parlement et au public, dans le respect du secret de la défense nationale qui couvre ses travaux en application de l'article L. 832-5 du code de la sécurité intérieure.

La commission conduit, par ailleurs, une action internationale destinée à faire connaître le cadre légal français applicable aux activités de renseignement et à recueillir les bonnes pratiques mises en œuvre par les institutions nationales de contrôle des pays partenaires de la France.

Le dialogue institutionnel que développe la CNCTR avec le Parlement avait pour contexte, cette année, le débat législatif sur le devenir de la technique de l'algorithme et la révision du cadre légal créé par la loi du 24 juillet 2015 relative au renseignement.

Invité par la délégation parlementaire au renseignement à en décrire les enjeux en matière de contrôle, le président de la commission a présenté, en avril 2021, un bilan de l'application de la loi du 24 juillet 2015 ainsi que ses perspectives d'évolution. En mai 2021, dans le cadre d'un cycle d'auditions dédié au renseignement et destiné à préparer ce débat, il a été entendu par la commission de la défense nationale et des forces armées de l'Assemblée nationale afin de présenter la mission et l'activité de la CNCTR. Le président a ensuite, en mai et juin de cette année, été auditionné à l'Assemblée nationale puis au Sénat par les rapporteurs des commissions compétentes au fond sur

les dispositions concernant le renseignement que contenait le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

En juin 2021, il a été reçu, aux côtés des deux membres de la CNCTR ayant la qualité de députés, par le président de l'Assemblée nationale, puis, en juillet de cette année, par le président du Sénat, pour une présentation du rapport d'activité de la commission pour 2020. Le président était alors accompagné des deux membres de la commission ayant la qualité de sénateurs.

Enfin, le président de la CNCTR a été auditionné, lors de l'examen au Sénat du projet de loi de finances pour l'année 2022, par le rapporteur de la commission des lois saisie pour avis concernant les moyens financiers et humains alloués à la commission pour remplir sa mission.

Outre la publication de son rapport annuel d'activité, la CNCTR entend faire connaître aux professionnels du droit, aux universitaires et à des associations de défense des libertés, notamment, le cadre juridique applicable aux activités de renseignement. En novembre 2021, le président a été invité pour la première fois par le Centre des hautes études militaires à intervenir devant les auditeurs de nationalité française de cette école de préparation à l'exercice de hautes responsabilités dans le domaine de la défense pour leur présenter le régime juridique relatif au renseignement et l'activité de contrôle de la commission.

S'agissant des relations internationales, la CNCTR entretient un dialogue avec ses homologues européens dans le cadre de réunions bilatérales mais également multilatérales depuis la première rencontre des autorités nationales de contrôle en Europe organisée à Paris en décembre 2018. Cette activité a connu un net ralentissement ces deux dernières années en raison de la situation créée par la pandémie de Covid-19. La troisième rencontre multilatérale de ce type, initialement prévue en 2020, a pu avoir lieu à Rome en octobre 2021. Cette conférence européenne avait notamment pour programme un échange sur les conséquences à tirer de la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne en matière de renseignement. La prochaine conférence est prévue fin 2022, à Londres.

Annexes

Annexe n° 1

Un résumé du cadre juridique en vigueur au 31 décembre 2021

Le livre VIII du code de la sécurité intérieure, créé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, prévoit que les services de renseignement peuvent être autorisés à mettre en œuvre, pour des finalités limitativement énumérées, des techniques destinées à recueillir des renseignements. Chaque autorisation est accordée par le Premier ministre.

La Commission nationale de contrôle des techniques de renseignement (CNCTR) s'assure que les techniques de renseignement sont mises en œuvre sur le territoire national conformément au cadre légal. Elle est consultée préalablement à la décision du Premier ministre sur toutes les demandes tendant à mettre en œuvre une technique ou, s'agissant de la surveillance des communications électroniques internationales, sur toutes les demandes tendant à exploiter des communications interceptées. La CNCTR vérifie également *a posteriori* que les prescriptions légales ont été respectées, en contrôlant l'exécution des autorisations accordées et en vérifiant qu'aucun recueil ou qu'aucune exploitation soumis à autorisation n'a été irrégulièrement mis en œuvre. Elle exerce un contrôle de légalité, qui inclut un contrôle de la proportionnalité des atteintes portées à la vie privée par rapport aux finalités poursuivies.

Les services de renseignement sont notamment des services spécialisés, dits du « premier cercle ». Il s'agit de :

- la direction générale de la sécurité extérieure (DGSE) ;
- la direction du renseignement et de la sécurité de la défense (DRSD) ;
- la direction du renseignement militaire (DRM) ;

- la direction générale de la sécurité intérieure (DGSI) ;
- le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) ;
- le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin).

D'autres services peuvent se voir confier des missions de renseignement. Ces services, dits du « second cercle », se trouvent notamment au sein de la direction générale de la police nationale, de la direction générale de la gendarmerie nationale, de la préfecture de police de Paris et de la direction de l'administration pénitentiaire.

En matière de surveillance intérieure, c'est-à-dire visant le territoire national, les techniques de renseignement qui peuvent être autorisées sont :

- les accès administratifs aux données de connexion[88], qui comprennent :
  - les accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure),
  - les accès aux données de connexion en temps réel, à la seule fin de prévention du terrorisme (article L. 851-2 du code de la sécurité intérieure),
  - la mise en œuvre, à la seule fin de prévention du terrorisme, de traitements automatisés sur les seules données de connexion acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de services en ligne (article L. 851-3 du code de la sécurité intérieure),

88 - Définies à l'article L. 851-1 du code de la sécurité intérieure, les données de connexion sont les « *informations ou documents traités ou conservés par* [les] *réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ». Cette définition a été précisée à l'article R. 851-5 du code de la sécurité intérieure.

- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure),
- le balisage (article L. 851-5 du code de la sécurité intérieure),
- le recueil de données de connexion par *IMSI catcher*[89] (article L. 851-6 du code de la sécurité intérieure) ;

- les interceptions de sécurité, qui comprennent :
  - l'interception, via le groupement interministériel de contrôle (GIC) ou par *IMSI catcher*, des communications acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de service en ligne (article L. 852-1 du code de la sécurité intérieure),
  - l'interception des communications échangées au sein d'un réseau privatif empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques (article L. 852-2 du code de la sécurité intérieure) ;
  - l'interception des correspondances émises ou reçues par la voie satellitaire (article L. 852-3 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé (article L. 853-1 du code de la sécurité intérieure) ;
- la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- le recueil ou la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé, y compris à usage d'habitation (article L. 853-3 du code de la sécurité intérieure), qui ne constitue pas à proprement parler une technique de renseignement mais peut être autorisée, par décision spécifique, à la seule fin de

89 - Il s'agit de dispositifs techniques permettant de capter des données de connexion d'équipements terminaux, notamment le numéro de leur carte *SIM* ou *IMSI* (*international mobile subscriber identity*).

mettre en place, utiliser ou retirer un dispositif de balisage, de captation de paroles, de captation d'images ainsi que de recueil ou de captation de données informatiques.

En matière de surveillance des communications électroniques internationales, l'interception de ces communications ainsi que différentes mesures d'exploitation portant sur des communications ou des seules données de connexion peuvent être autorisées (articles L. 854-1 et suivants du code de la sécurité intérieure).

Les finalités pouvant justifier la mise en œuvre des techniques de renseignement sont limitativement énumérées à l'article L. 811-3 du code de la sécurité intérieure. Il s'agit de :

1° l'indépendance nationale, l'intégrité du territoire et la défense nationale ;

2° 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 ;

3° les intérêts économiques, industriels et scientifiques majeurs de la France ;

4° la prévention du terrorisme ;

5° la prévention des atteintes à la forme républicaine des institutions, la prévention des actions tendant au maintien ou à la reconstitution de groupements dissous et la prévention des violences collectives de nature à porter gravement atteinte à la paix publique ;

6° la prévention de la criminalité et de la délinquance organisées ;

7° la prévention de la prolifération des armes de destruction massive.

Le service du « second cercle » chargé du renseignement pénitentiaire peut en outre être autorisé à recourir à un nombre limité de techniques pour une finalité propre, prévue à l'article L. 855-1 du code de la

sécurité intérieure, à savoir prévenir les évasions et assurer la sécurité au sein des établissements pénitentiaires.

Toute personne peut saisir la CNCTR d'une réclamation tendant à ce que la commission vérifie qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Une fois cette faculté de réclamation utilisée, la personne peut présenter une requête devant une formation spécialisée du Conseil d'État pour demander au juge administratif de mener des vérifications similaires.

Annexe n° 2

Délibération de la CNCTR n° 2/2021 du 7 avril 2021

Saisie pour avis par le Premier ministre[90] 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) ;

90 - Voir le courrier du directeur, adjoint à la secrétaire générale du Gouvernement du 8 mars 2021.

- 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[91] 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. 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[92]. 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[93], 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.

91 - Voir le courrier du directeur, adjoint à la secrétaire générale du Gouvernement du 7 avril 2021.

92 - Cette loi sera désormais désignée comme la loi du 24 juillet 2015.

93 - Cet avis est disponible sur le site internet de la CNCTR.

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.

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. À 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[94] 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[95]. 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*[96]*, être exploités aux fins d'accéder au contenu de correspondances échangées ou d'informations consultées* ».

94 - Cette délibération est disponible sur le site internet de la CNCTR.

95 - 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* ».

96 - L'article L. 852-1 a trait aux interceptions de sécurité.

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[97], 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 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.

97 - 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* ».

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.

À 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'État, 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[98]. 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[99] par la CNCTR.

98 - 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.

99 - Cette délibération est disponible sur le site internet de 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* 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'État 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'État 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'État* ». Ce décret en Conseil d'État 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[100].

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.

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.

100 - 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.

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[101].

101 - 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 (…)* ».

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.

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.

Annexe n° 3

Délibération de la CNCTR n° 3/2021 du 14 avril 2021

Par une saisine complémentaire du 7 avril 2021[102], 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.

102 - 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[103] 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

103 - L'orbite géostationnaire de la Terre se situe à une altitude d'environ 36 000 kilomètres.

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.

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. À 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 5^{e} 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[104].

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

104 - 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.

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[105], 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 locaux administrés par le GIC constitue une garantie. Elle constate cependant

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

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.

Annexe n° 4

Délibération de la CNCTR n° 4/2021 du 30 avril 2021

La Commission nationale de contrôle des techniques de renseignement (CNCTR) a été saisie pour avis par le Premier ministre le 26 avril 2021 d'une lettre rectificative au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement[106]. Cette lettre contient deux articles additionnels destinés à tirer les conséquences de la décision « French data network et autres » rendue par l'assemblée du contentieux du Conseil d'État le 21 avril 2021[107] après que la Cour de justice de l'Union européenne (CJUE) a répondu, dans un arrêt du 6 octobre 2020[108], aux questions préjudicielles que le Conseil d'État lui avait posées dans une décision avant dire droit du 26 juillet 2018[109].

L'article 11 *quinquies* du projet de loi est relatif au régime de conservation des données relatives aux communications électroniques par les opérateurs de communications électroniques.

L'article 11 sexies modifie le dispositif de contrôle préalable des demandes de mise en œuvre des techniques de renseignement.

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

106 - La saisine initiale du 8 mars 2021 a été complétée par une première saisine rectificative le 7 avril 2021. Les délibérations de la CNCTR n° 2/2021 du 7 avril 2021 et n° 3/2021 du 14 avril 2021 constituent les avis rendus par la commission sur les dispositions soumises à son examen. Elles sont disponibles sur le site internet de la commission.

107 - Il s'agit de la décision rendue sur les requêtes nos 393099, 39492, 397844, 397851, 424717 et 424718.

108 - Il s'agit de l'arrêt « La Quadrature du Net et autres » rendue sur les requêtes C-511/18, C-512/18 et C-520/18.

109 - Voir les requêtes nos 394922, 397844, 397851 et 399099.

1. Sur le régime de conservation des données de connexion (article 11 *quinquies* du projet de loi)

L'article L. 34-1 du code des postes et des télécommunications (CPCE) et l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique imposent aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenus de conserver, pour une durée d'un an, l'ensemble des données de trafic et de localisation de leurs utilisateurs, les données relatives à leur identité civile ainsi que certaines informations relatives à leurs comptes et, le cas échéant, aux paiements qu'ils effectuent en ligne, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

Dans sa décision du 21 avril 2021, le Conseil d'État a jugé que le Gouvernement ne pouvait, sans méconnaître le droit de l'Union européenne, imposer aux opérateurs de communications électroniques et aux fournisseurs d'accès à internet la conservation généralisée et indifférenciée des données de connexion, autres que les données relatives à l'identité civile, aux adresses IP et aux informations relatives aux comptes et aux paiements, aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public. Il a, en revanche, admis qu'une telle obligation de conservation généralisée et indifférenciée peut être fondée sur la sauvegarde de la sécurité nationale et il a estimé que toutes les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure doivent être regardées comme relevant de la sécurité nationale. Il a, cependant, jugé que cette obligation doit être subordonnée au constat, à échéance régulière qui ne saurait raisonnablement excéder un an, de la persistance d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

L'article 11 *quinquies* tire les conséquences de l'arrêt du 21 avril 2021 en modifiant l'article L. 34-1 du CPCE pour y préciser :

- que les opérateurs de communications électroniques sont tenus de conserver jusqu'à l'expiration d'un délai de cinq ans après la fin de validité de leur contrat les informations relatives à l'identité civile de l'utilisateur et, pour une durée d'un an, les autres informations

fournies par l'utilisateur lors de la souscription de son contrat, les informations de paiement et les données techniques permettant d'identifier l'utilisateur ou relatives aux « équipements terminaux de connexion » utilisés parmi lesquelles figurent notamment les adresses IP attribuées à la source d'une connexion ;

- qu'ils sont également tenus, aux seules fins de sauvegarde de la sécurité nationale, d'opérer une conservation généralisée et indifférenciée, pendant une durée d'un an, de certaines catégories de données de connexion, y compris les données de trafic et de localisation, sous réserve qu'une injonction du Premier ministre, qui prend la forme d'un décret dont la durée d'application ne peut excéder un an et peut être renouvelée, constate l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

L'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique est également modifié pour prévoir les mêmes obligations pour les fournisseurs d'accès à internet et les hébergeurs de contenus.

Les dispositions de l'article 11 *quinquies* du projet de loi ont donc pour objet de mettre les dispositions législatives qui viennent d'être évoquées en conformité avec le droit de l'Union européenne. Elles n'appellent pas d'observations de la part de la CNCTR.

2. Sur le contrôle préalable des demandes de techniques de renseignement (article 11 sexies du projet de loi)

2.1 Dans sa décision « French data network et autres » du 21 avril 2021, le Conseil d'État a jugé que la mise en œuvre des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure devait être soumise au contrôle préalable d'une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou d'une juridiction, en dehors des cas d'urgence dûment justifiée, et que les dispositions en vigueur du code de la sécurité intérieure ne répondaient pas à cette

exigence. Il tire ainsi les conséquences des arrêts du 21 décembre 2016[110] et du 6 octobre 2020 de la Cour de justice de l'Union européenne qui ont jugé que le droit de l'Union européenne imposait, sauf en cas d'urgence dûment justifiée, un contrôle préalable par une juridiction ou une autorité administrative indépendante dotée d'un pouvoir contraignant.

L'article 11 *sexies* du projet de loi propose, pour adapter le dispositif actuel aux exigences du droit de l'Union européenne, plusieurs modifications aux dispositions du livre huitième du code de la sécurité intérieure relatives au renseignement :

- il prévoit, à l'article L. 821-1 de ce code, que lorsque le Premier ministre délivre une autorisation de mise en œuvre d'une technique de renseignement après avis défavorable de la CNCTR, le Conseil d'État est immédiatement saisi et doit statuer sur la légalité de la décision du Premier ministre dans un délai de vingt-quatre heures. La décision du Premier ministre ne peut être exécutée avant que le Conseil d'État ait statué « sauf en cas d'urgence dûment justifiée et si le Premier ministre a ordonné sa mise en œuvre immédiate » ;
- il exclut la possibilité d'invoquer l'urgence pour autoriser la mise en œuvre initiale ou le renouvellement de la technique de l'« algorithme » prévue à l'article L. 851-3 de ce code ;
- il limite à certaines finalités la possibilité d'invoquer le caractère d'urgence pour autoriser la captation de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé et le recueil et la captation de données informatiques par des dispositifs techniques, ainsi que pour autoriser la pénétration dans un lieu privé afin d'y mettre en œuvre une technique de renseignement ;
- il abroge, enfin, l'article L. 821-5 de ce code qui permet au Premier ministre, en cas d'« urgence absolue » et pour un nombre limité de finalités, de délivrer une autorisation de mise en œuvre d'une technique de renseignement sans avis préalable de la CNCTR.

110 - Il s'agit de l'arrêt dit « Tele 2 Sverige AB » rendu par la CJUE réunie en grande chambre le 21 décembre 2016 sur les requêtes C-203/15 et C-698/15.

2.2 La CNCTR rappelle que, jusqu'à présent, le Premier ministre n'a jamais autorisé la mise en œuvre d'une technique de renseignement après qu'elle a émis un avis défavorable. Ce constat, qui témoigne de la solidité du dispositif légal de contrôle préalable issu de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, ne prive, cependant, pas de pertinence les modifications proposées par l'article 11 sexies du projet de loi.

Le mécanisme de contrôle proposé est déjà prévu au III de l'article L.853-3 du code de la sécurité intérieure dans le cas précis et limité de l'introduction dans un lieu privé à usage d'habitation. La CNCTR estime que son extension, par la modification proposée de l'article L. 821-1 du même code, à l'ensemble des techniques de renseignement répond à l'exigence, posée par le Conseil d'État statuant au contentieux, d'un contrôle préalable de la mise en œuvre des techniques de renseignement par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou par une juridiction. Elle permet de combiner le contrôle préalable de la CNCTR, autorité administrative indépendante, et le contrôle juridictionnel du Conseil d'État. En application de ce mécanisme, lorsque la CNCTR émet un avis défavorable à une demande de mise en œuvre d'une technique de renseignement, le Premier ministre ne peut passer outre à cet avis défavorable en délivrant une autorisation sans que le Conseil d'État statuant au contentieux soit saisi et, sauf en cas d'urgence dûment justifiée, sans qu'il ait préalablement statué sur la légalité de sa décision. Ce mécanisme de contrôle préalable laisse entier le pouvoir du Premier ministre de ne pas autoriser une technique de renseignement qui aurait pourtant recueilli l'assentiment de la CNCTR. Outre que cette décision ne porte pas atteinte au droit au respect de la vie privée, il appartient en effet au Premier ministre, en vertu de ses prérogatives constitutionnelles, d'apprécier, lorsqu'il se prononce sur une demande de surveillance, les risques liés à la réalisation de l'opération envisagée.

2.3 La commission approuve le choix opéré par l'article 11 *sexies* du projet de loi d'appliquer le mécanisme de contrôle préalable à l'ensemble des techniques de renseignement, sans le limiter à celles relatives aux accès aux données de connexion qui étaient l'objet du litige porté devant le Conseil d'État. Ce choix conforte la cohérence du cadre légal de contrôle des techniques de renseignement.

Le projet de loi omet, cependant, d'étendre l'application du mécanisme proposé à la surveillance des communications électroniques internationales. Depuis la loi n° 2018-17 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, la CNCTR exerce un contrôle préalable sur les demandes d'autorisation d'exploitation des communications électroniques internationales (III de l'article L. 854-2 du code de la sécurité intérieure) ainsi que sur les demandes d'autorisation d'exploitation de communications d'identifiants techniques rattachables au territoire national dont l'utilisateur communique depuis ce territoire (V du même article). La CNCTR estime, dès lors, que le mécanisme d'avis conforme ci-dessus décrit doit également s'appliquer, pour des raisons de cohérence, dans le domaine de la surveillance des communications électroniques internationales. Elle recommande en conséquence que des dispositions similaires à celles prévues par le 1° du I de l'article 11 sexies du projet de loi soient introduites dans l'article L. 854-2 du code de la sécurité intérieure.

2.4 La CNCTR approuve l'abrogation de l'article L. 821-5 du code de la sécurité intérieure. Bien que cet article n'ait été utilisé qu'une seule fois[111], quelques mois après l'entrée en vigueur de la loi du 24 juillet 2015, il n'en constitue pas moins une exception au principe du contrôle préalable exercé par la CNCTR sur toutes les demandes de techniques de renseignement. Or, la commission a démontré qu'elle était en mesure d'exercer son contrôle préalable à tout moment, dans des délais extrêmement courts lorsque cela est nécessaire pour répondre aux exigences opérationnelles propres à l'activité des services de renseignement. Le maintien d'une disposition dérogatoire au principe du contrôle préalable n'est donc pas justifié.

2.5 Le mécanisme d'avis conforme proposé doit cependant prendre en compte les cas d'urgence dûment justifiée dans lesquels la mise en œuvre de l'autorisation ne peut attendre la décision de la formation spécialisée du Conseil d'État, même si elle est rendue dans le délai de vingt-quatre heures prévu par l'article 11 *sexies* du projet de loi. Ce texte envisage quatre situations :

111 - Alors que la CNCTR était pourtant en mesure de rendre son avis dans un délai compatible avec l'urgence invoquée.

a) celle de l'autorisation de la mise en œuvre ou du renouvellement d'un algorithme (I et II de l'article L. 851-3 du code de la sécurité intérieure), dans laquelle le caractère d'urgence ne peut être invoqué. La CNCTR estime que cette disposition est justifiée par la nature particulière de la technique de l'algorithme qui nécessite un contrôle approfondi.

La commission recommande également d'exclure la possibilité d'invoquer le caractère d'urgence pour la mise en œuvre de techniques concernant un parlementaire, un magistrat, un avocat ou un journaliste. Elle rappelle que l'article L. 821-7 du code de la sécurité intérieure prohibe la surveillance de ces personnes à raison de l'exercice de leur mandat ou de leur profession et qu'il écarte la procédure d'urgence absolue de l'article L. 821-5 du code de la sécurité intérieure pour la délivrance d'une autorisation de mise en œuvre d'une technique de renseignement, quelle qu'elle soit. Elle estime, dès lors, qu'en cas de désaccord entre la Commission et le Premier ministre il est préférable qu'avant toute mise en œuvre d'une mesure de surveillance le Conseil d'État statuant au contentieux ait pu se prononcer.

b) celle de l'autorisation de pénétrer dans un lieu privé à usage d'habitation pour y mettre en œuvre certaines techniques de renseignement (article L. 853-3 du code de la sécurité intérieure), dans laquelle le caractère d'urgence ne peut être invoqué que si l'autorisation a été délivrée au titre de la prévention du terrorisme. Le projet de loi propose de conserver les dispositions déjà prévues dans un tel cas par l'article L. 853-3, comme cela a été dit plus haut. La CNCTR estime que ces dispositions sont justifiées par le caractère particulièrement attentatoire à la vie privée de la pénétration dans un lieu d'habitation.

c) celle, propre à plusieurs techniques, dont la mise en œuvre porte une atteinte substantielle au droit au respect de la vie privée, dans laquelle le caractère d'urgence ne peut être invoqué que pour un nombre limité de finalités. Les techniques sont celles de l'article L. 853-1 du code de la sécurité intérieure (recueil de paroles prononcées à titre privé ou confidentiel et d'images dans un lieu privé) et de l'article L. 853-2 du même code (recueil de données informatiques par un dispositif technique). Est également concernée l'autorisation de pénétrer dans un lieu privé qui n'est pas un lieu d'habitation (article L. 853-3 de ce code). Les finalités sont celles prévues aux 1°, 4° et a du 5° de l'article L. 811-3 de ce code,

qui concernent respectivement la défense de l'indépendance nationale, de l'intégrité du territoire et de la défense nationale, la prévention du terrorisme et la prévention des atteintes à la forme républicaine des institutions.

Ni la liste des finalités proposées, ni celle des techniques concernées n'appellent d'objections de la part de la CNCTR. La commission recommande, cependant, que pour d'autres techniques, qu'elle regarde comme portant également une atteinte substantielle au droit au respect de la vie privée le caractère d'urgence ne puisse être invoqué que pour ce nombre limité de finalités. Il s'agit des interceptions de sécurité réalisées avec le concours d'un opérateur (I de l'article L. 852-1 du code de la sécurité intérieure), par l'utilisation d'un *IMSI catcher*[112] (II du même article) et au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne (article L. 852-2 du même code) ainsi que du recueil de données de connexion au moyen d'un *IMSI catcher* (article L. 851-6 de ce code). Il est également souhaitable, à son avis, de faire de même pour la nouvelle technique d'interception de correspondances émises ou reçues par la voie satellitaire prévue, à titre expérimental, par l'article 13 bis du projet de loi.

d) celle, applicable aux autres techniques, dans laquelle le caractère d'urgence peut être invoqué sans limitation à certaines finalités.

Sous réserve des recommandations formulées ci-dessus aux points a et c, la CNCTR n'a pas d'objections sur ce point. Elle relève que, dans certains cas, les techniques de renseignement concernées ne sont autorisées que pour la finalité de prévention du terrorisme. Il s'agit du recueil de données de connexion en temps réel prévu par l'article L. 851-2 du code de la sécurité intérieure et de l'autorisation d'identification des personnes dont les données de connexion ont été détectées par un algorithme comme susceptibles de révéler une menace terroriste (IV de l'article L. 851-3 du même code).

112 - Dont la mise en œuvre ne peut d'ailleurs être autorisée que pour les mêmes finalités prévues au 1°, 4° et a du 5° de l'article L. 811-3 du code de la sécurité intérieure.

Annexe n° 5

Décision du Conseil d'État statuant au contentieux

N° 3930099

Publié au recueil Lebon

Assemblée du contentieux

M. Réda Wadjinny-Green, rapporteur

M. Alexandre Lallet, rapporteur public

Lecture du mercredi 21 avril 2021

AU NOM DU PEUPLE FRANCAIS

Vu les procédures suivantes :

1° Sous les nos 394922, 397844 et 397851, par une décision du 26 juillet 2018, le Conseil d'État, statuant au contentieux sur les requêtes de l'association La Quadrature du Net et autres et de l'association Igwan.net tendant à l'annulation pour excès de pouvoir des décrets n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 de ce code et n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement, a sursis à statuer jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur les questions suivantes :

1°) L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États-membres en vertu de l'article 4 du traité sur l'Union européenne ;

2°) La directive du 12 juillet 2002 lue à la lumière de la Charte des droits fondamentaux de l'Union européenne doit-elle être interprétée en ce sens qu'elle autorise des mesures législatives, telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données ;

3°) La directive du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, doit-elle être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou de telles procédures peuvent-elles être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours ;

2° Sous le n° 393099, par une décision du 26 juillet 2018, le Conseil d'État, statuant au contentieux sur la requête de l'association French Data Network et autres tendant à l'annulation pour excès de pouvoir de la décision implicite de rejet résultant du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques et du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données

permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, a sursis à statuer jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur les questions suivantes :

> 1°) L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États-membres en vertu de l'article 4 du traité sur l'Union européenne ;
>
> 2°) Les dispositions de la directive du 8 juin 2000, lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doivent-elles être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale ;

3° Sous le n° 424717, par une requête, deux mémoires en réplique et trois nouveaux mémoires, enregistrés au secrétariat du contentieux du Conseil d'État les 5 octobre 2018 et les 11 janvier, 19 février, 5 mars, 19 mars et 7 avril 2021, la société Free Mobile demande au Conseil d'État :

1°) d'annuler pour excès de pouvoir la décision implicite de rejet résultant du silence gardé par le Premier ministre sur sa demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques ;

2°) d'enjoindre au Premier ministre d'abroger ces dispositions ou, à défaut, de statuer à nouveau sur sa demande dans un délai de quinze jours ;

3°) de mettre à la charge de l'État la somme de 10 000 euros au titre de l'article L. 761-1 du code de justice administrative.

4° Sous le n° 424718, par une requête, deux mémoires en réplique et trois nouveaux mémoires, enregistrés au secrétariat du contentieux du Conseil d'État les 5 octobre 2018 et les 11 janvier, 19 février, 5 mars, 19 mars et 7 avril 2021, la société Free demande au Conseil d'État :

1°) d'annuler pour excès de pouvoir la décision implicite de rejet résultant du silence gardé par le Premier ministre sur sa demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques ;

2°) d'enjoindre au Premier ministre d'abroger ces dispositions ou, à défaut, de statuer à nouveau sur sa demande dans un délai de quinze jours ;

3°) de mettre à la charge de l'État la somme de 10 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Vu les autres pièces des dossiers, y compris celles visées par les décisions du Conseil d'État du 26 juillet 2018 ;

Vu :

- la Constitution ;
- le traité sur l'Union européenne ;
- le traité sur le fonctionnement de l'Union européenne ;
- la Charte des droits fondamentaux de l'Union européenne ;
- la convention de Budapest du 23 novembre 2001 sur la cybercriminalité ;
- le règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;

- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 ;
- le code des postes et des communications électroniques ;
- le code de procédure pénale ;
- le code de la sécurité intérieure, notamment son livre VIII ;
- la loi n° 2004-575 du 21 juin 2004 ;
- le décret n° 2011-219 du 25 février 2011 ;
- le décret n° 2015-1185 du 28 septembre 2015 ;
- le décret n° 2015-1639 du 11 décembre 2015 ;
- le décret n° 2016-67 du 29 janvier 2016 ;
- le décret n° 2020-1404 du 18 novembre 2020 ;
- l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014, Digital Rights Ireland Ltd (C-293/12 et C-594/12) ;
- l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016, Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson et autres (C-203/15 et C-698/15) ;
- l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2020, La Quadrature du net et autres (C-511/18, C-512/18, C520/18) ;
- l'arrêt de la Cour de justice de l'Union européenne du 2 mars 2021, H.K. / Prokuratuur (C-746/18) ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Réda Wadjinny-Green, auditeur,
- les conclusions de M. Alexandre Lallet, rapporteur public ;

Vu la note en délibéré, enregistrée le 16 avril 2021, présentée sous les nos 393099, 394922, 397844 et 397851 par les associations French Data Network, La Quadrature du Net, la Fédération des fournisseurs d'accès à internet associatifs et Igwan.net.

Vu la note en délibéré, enregistrée le 16 avril 2021, présentée sous les nos 393099, 394922, 397844, 397851, 424717 et 424718 par le Premier ministre.

Considérant ce qui suit :

1. Les associations et sociétés requérantes contestent les dispositions réglementaires imposant aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenus de conserver de façon généralisée et indifférenciée, pour une durée d'un an, les données de trafic et de localisation de l'ensemble de leurs utilisateurs ainsi que leurs données d'identité civile et certaines données relatives à leurs comptes et aux paiements qu'ils effectuent en ligne. Elles contestent également les dispositions réglementaires permettant aux services de renseignement de recueillir et d'opérer des traitements sur ces données. Sous le n° 393099, les associations French Data Network, La Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs demandent l'annulation de la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques et du décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. La Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs demandent l'annulation pour excès de pouvoir, sous le n° 394922, du décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement et, sous le n° 397851, du décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement. Sous le n° 397844, l'association Igwan.net demande l'annulation pour excès de pouvoir du décret du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du même code. Sous les n^{os} 424717 et 424718, les sociétés Free Mobile et Free demandent l'annulation de la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques. Par ses décisions n° 393099 et n^{os} 394922, 394925, 397844, 397851 du 26 juillet 2018, le Conseil d'État, statuant au contentieux, a écarté les moyens invoqués devant lui autres que ceux tirés de la méconnaissance du droit de l'Union européenne et a sursis à statuer jusqu'à ce que la Cour de justice de l'Union européenne se soit

prononcée sur les questions préjudicielles dont il l'a saisie. Par un arrêt en date du 6 octobre 2020, rendu dans les affaires jointes C-511/18, C-512/18 et C-520/18, la Cour de justice s'est prononcée sur ces questions.

2. Les requêtes présentent à juger des questions communes. Il y a lieu de les joindre pour statuer par une seule décision.

I. Sur le cadre juridique des litiges :

En ce qui concerne les exigences inhérentes à la hiérarchie des normes :

3. En vertu de l'article 88-1 de la Constitution : « *La République participe à l'Union européenne constituée d'États qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007* ». Selon le paragraphe 3 de l'article 4 du traité sur l'Union européenne : « *En vertu du principe de coopération loyale, l'Union et les États membres se respectent et s'assistent mutuellement dans l'accomplissement des missions découlant des traités. / Les États membres prennent toute mesure générale ou particulière propre à assurer l'exécution des obligations découlant des traités ou résultant des actes des institutions de l'Union. / Les États membres facilitent l'accomplissement par l'Union de sa mission et s'abstiennent de toute mesure susceptible de mettre en péril la réalisation des objectifs de l'Union* ». La seconde phrase du paragraphe 1 de l'article 19 du même traité assigne à la Cour de justice de l'Union européenne la mission d'assurer « *le respect du droit dans l'interprétation et l'application des traités* ».

4. Le respect du droit de l'Union constitue une obligation tant en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne qu'en application de l'article 88-1 de la Constitution. Il emporte l'obligation de transposer les directives et d'adapter le droit interne aux règlements européens. En vertu des principes de primauté, d'unité et d'effectivité issus des traités, tels qu'ils ont été interprétés par la Cour de justice de l'Union européenne, le juge national, chargé

d'appliquer les dispositions et principes généraux du droit de l'Union, a l'obligation d'en assurer le plein effet en laissant au besoin inappliquée toute disposition contraire, qu'elle résulte d'un engagement international de la France, d'une loi ou d'un acte administratif.

5. Toutefois, tout en consacrant l'existence d'un ordre juridique de l'Union européenne intégré à l'ordre juridique interne, dans les conditions mentionnées au point précédent, l'article 88-1 confirme la place de la Constitution au sommet de ce dernier. Il appartient au juge administratif, s'il y a lieu, de retenir de l'interprétation que la Cour de justice de l'Union européenne a donnée des obligations résultant du droit de l'Union la lecture la plus conforme aux exigences constitutionnelles autres que celles qui découlent de l'article 88-1, dans la mesure où les énonciations des arrêts de la Cour le permettent. Dans le cas où l'application d'une directive ou d'un règlement européen, tel qu'interprété par la Cour de justice de l'Union européenne, aurait pour effet de priver de garanties effectives l'une de ces exigences constitutionnelles, qui ne bénéficierait pas, en droit de l'Union, d'une protection équivalente, le juge administratif, saisi d'un moyen en ce sens, doit l'écarter dans la stricte mesure où le respect de la Constitution l'exige.

6. Il en résulte, d'une part, que, dans le cadre du contrôle de la légalité et de la constitutionnalité des actes réglementaires assurant directement la transposition d'une directive européenne ou l'adaptation du droit interne à un règlement et dont le contenu découle nécessairement des obligations prévues par la directive ou le règlement, il appartient au juge administratif, saisi d'un moyen tiré de la méconnaissance d'une disposition ou d'un principe de valeur constitutionnelle, de rechercher s'il existe une règle ou un principe général du droit de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité du respect de la disposition ou du principe constitutionnel invoqué. Dans l'affirmative, il y a lieu pour le juge administratif, afin de s'assurer de la constitutionnalité de l'acte réglementaire contesté, de rechercher si la directive que cet acte transpose ou le règlement auquel cet acte adapte le droit interne est conforme à cette règle ou à ce principe général du droit de l'Union.

Il lui revient, en l'absence de difficulté sérieuse, d'écarter le moyen invoqué, ou, dans le cas contraire, de saisir la Cour de justice de l'Union européenne d'une question préjudicielle, dans les conditions prévues par l'article 167 du traité sur le fonctionnement de l'Union européenne. En revanche, s'il n'existe pas de règle ou de principe général du droit de l'Union garantissant l'effectivité du respect de la disposition ou du principe constitutionnel invoqué, il revient au juge administratif d'examiner directement la constitutionnalité des dispositions réglementaires contestées.

7. D'autre part, lorsqu'il est saisi d'un recours contre un acte administratif relevant du champ d'application du droit de l'Union et qu'est invoqué devant lui le moyen tiré de ce que cet acte, ou les dispositions législatives qui en constituent la base légale ou pour l'application desquelles il a été pris, sont contraires à une directive ou un règlement européen, il appartient au juge administratif, après avoir saisi le cas échéant la Cour de justice d'une question préjudicielle portant sur l'interprétation ou la validité de la disposition du droit de l'Union invoquée, d'écarter ce moyen ou d'annuler l'acte attaqué, selon le cas. Toutefois, s'il est saisi par le défendeur d'un moyen, assorti des précisions nécessaires pour en apprécier le bien-fondé, tiré de ce qu'une règle de droit national, alors même qu'elle est contraire à la disposition du droit de l'Union européenne invoquée dans le litige, ne saurait être écartée sans priver de garanties effectives une exigence constitutionnelle, il appartient au juge administratif de rechercher s'il existe une règle ou un principe général du droit de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité de l'exigence constitutionnelle invoquée. Dans l'affirmative, il lui revient, en l'absence de difficulté sérieuse justifiant une question préjudicielle à la Cour de justice, d'écarter cette argumentation avant de faire droit au moyen du requérant, le cas échéant. Si, à l'inverse, une telle disposition ou un tel principe général du droit de l'Union n'existe pas ou que la portée qui lui est reconnue dans l'ordre juridique européen n'est pas équivalente à celle que la Constitution garantit, il revient au juge administratif d'examiner si, en écartant la règle de droit national au motif de sa contrariété avec le droit de l'Union européenne, il priverait de garanties

effectives l'exigence constitutionnelle dont le défendeur se prévaut et, le cas échéant, d'écarter le moyen dont le requérant l'a saisi.

8. En revanche, et contrairement à ce que soutient le Premier ministre, il n'appartient pas au juge administratif de s'assurer du respect, par le droit dérivé de l'Union européenne ou par la Cour de justice elle-même, de la répartition des compétences entre l'Union européenne et les États membres. Il ne saurait ainsi exercer un contrôle sur la conformité au droit de l'Union des décisions de la Cour de justice et, notamment, priver de telles décisions de la force obligatoire dont elles sont revêtues, rappelée par l'article 91 de son règlement de procédure, au motif que celle-ci aurait excédé sa compétence en conférant à un principe ou à un acte du droit de l'Union une portée excédant le champ d'application prévu par les traités.

En ce qui concerne les exigences constitutionnelles invoquées en défense par l'État :

9. Il est soutenu en défense que les dispositions du droit national contestées au motif qu'elles seraient contraires au droit de l'Union européenne ne sauraient être écartées sans priver de garanties effectives les objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme. Il ressort en effet de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789 que la garantie des droits de l'homme et du citoyen, sans laquelle une société n'a point de constitution selon l'article 16 de la même Déclaration, nécessite une force publique. La sauvegarde des intérêts fondamentaux de la Nation, la prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, la lutte contre le terrorisme, ainsi que la recherche des auteurs d'infractions pénales constituent des objectifs de valeur constitutionnelle, nécessaires à la sauvegarde de droits et de principes de même valeur, qui doivent être conciliés avec l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté individuelle, la liberté d'aller et venir et le respect de la vie privée.

10. Selon le paragraphe 2 de l'article 4 du traité sur l'Union européenne, il appartient à l'Union, y compris à la Cour de justice de l'Union européenne, de respecter l'identité nationale des États membres, « *inhérente à leurs structures fondamentales politiques et constitutionnelles »,* ainsi que *« les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale* », cette dernière restant « *de la seule responsabilité des États membres* ». Aux termes du paragraphe 1 de l'article 52 de la Charte des droits fondamentaux de l'Union européenne : « *Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui* ». Il ressort de la jurisprudence de la Cour de justice de l'Union européenne, d'une part, que les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave, qui contribuent à la protection des droits et des libertés d'autrui, sont au nombre des objectifs d'intérêt général reconnus par l'Union, comme tels susceptibles de justifier des limitations aux droits garantis par la Charte en vertu de son article 52, et, d'autre part, que si l'article 6 de la Charte, qui garantit le droit à la sûreté, ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer des infractions pénales, il découle de ses articles 3, 4 et 7, qui garantissent le droit au respect de l'intégrité de la personne, l'interdiction de la torture et des peines et traitements inhumains ou dégradants et le respect de la vie privée et familiale, des obligations positives à la charge de l'État, incluant la mise en place de règles permettant une lutte effective contre certaines infractions pénales. Toutefois, les exigences constitutionnelles mentionnées au point 9, qui s'appliquent à des domaines relevant exclusivement ou essentiellement de la compétence des États membres en vertu des traités constitutifs de l'Union, ne sauraient être regardées comme bénéficiant, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution.

En ce qui concerne l'office du juge dans le contentieux du refus d'abroger un acte réglementaire:

11. L'autorité compétente, saisie d'une demande tendant à l'abrogation d'un règlement illégal, est tenue d'y déférer, soit que, réserve faite des vices de forme et de procédure dont il serait entaché, ce règlement ait été illégal dès la date de sa signature, soit que l'illégalité résulte de circonstances de droit ou de fait postérieures à cette date.

12. L'effet utile de l'annulation pour excès de pouvoir du refus d'abroger un acte réglementaire illégal réside dans l'obligation, que le juge peut prescrire d'office en vertu des dispositions de l'article L. 911-1 du code de justice administrative, pour l'autorité compétente, de procéder à l'abrogation de cet acte afin que cessent les atteintes illégales que son maintien en vigueur porte à l'ordre juridique. Il s'ensuit que lorsqu'il est saisi de conclusions aux fins d'annulation du refus d'abroger un acte réglementaire, le juge de l'excès de pouvoir est conduit à apprécier la légalité de l'acte réglementaire dont l'abrogation a été demandée au regard des règles applicables à la date de sa décision.

En ce qui concerne les questions soulevées par les requêtes :

13. Les associations et sociétés requérantes contestent la conformité au droit de l'Union européenne de deux séries de dispositions. La première d'entre elles concerne l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011, pris respectivement pour l'application de l'article L. 34-1 du même code et de l'article 6 de la loi du 21 juin 2004. Ces dispositions imposent aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de conserver, pour une durée d'un an, l'ensemble des données de trafic et de localisation de leurs utilisateurs, lesquelles ne couvrent pas le contenu des communications, les données relatives à leur identité civile, ainsi que certaines informations relatives à leurs comptes et, le cas échéant, aux paiements qu'ils effectuent en ligne pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et la sauvegarde de la sécurité nationale. La seconde série de dispositions concerne les décrets du 28 septembre 2015, du 11 décembre 2015 et du 29 janvier 2016, pris pour

l'application du livre VIII de la partie législative du code de la sécurité intérieure relatif au renseignement. Sont en particulier en cause les techniques de renseignement mentionnées aux articles L. 851-1 à L. 851-4 de ce code. Il y a lieu d'analyser successivement aux II et III de la présente décision la compatibilité au droit de l'Union européenne de chacune de ces séries de dispositions.

II. Sur la conservation générale et indifférenciée des données de connexion :

En ce qui concerne le cadre juridique national :

14. Le II de l'article L. 34-1 du code des postes et des communications électroniques fait obligation aux opérateurs de services de communications électroniques, notamment aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, d'effacer ou de rendre anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI du même article. Les données relatives au trafic au sens de ces dispositions sont définies par le 18° de l'article L. 32 du même code comme « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* ». Elles incluent les données d'identification des utilisateurs des réseaux de communications électroniques, les données relatives aux caractéristiques techniques des communications qu'ils ont effectuées à l'aide de tels réseaux et, enfin, les données de localisation, définies par le c) de l'article 2 de la directive 2002/58/CE du 12 juillet 2002 comme « *toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ».

15. Par exception à la règle fixée au II de l'article L. 34-1 du code des postes et des communications électroniques, les opérateurs sont autorisés par le IV du même article à conserver, d'une part, les catégories

de données énumérées aux I à III de l'article R. 10-14 de ce code, pour les besoins de la facturation et du paiement des prestations de communications électroniques qu'ils fournissent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, soit un an à compter du jour du paiement en vertu de l'article L. 34-2 et, d'autre part, les données énumérées au IV de cet article R. 10-14, pour les besoins de la sécurité des réseaux et des installations, pour une durée n'excédant pas trois mois.

16. Par dérogation au principe d'anonymisation des données de connexion, le III du même article L. 34-1 prévoit la possibilité d'imposer aux opérateurs de communications électroniques la conservation des données relatives au trafic et à la localisation, pour une durée maximale d'un an, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales. Il dispose ainsi que : « *III. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs* ». Le VI du même article précise que : « *VI. - Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur*

l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. / Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. / La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. / Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article ».

17. Le 2° de l'article L. 39-3 du code des postes et des communications électroniques punit d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents de ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

18. Le premier alinéa du II de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoit par ailleurs que les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services « *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ».

19. Pour les besoins du renseignement, l'article L. 851-1 du code de la sécurité intérieure, relatif aux accès administratifs aux données de connexion par les services de renseignement, prévoit que, dans les conditions prévues au chapitre I^{er} du titre II du livre VIII de ce code, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques et à l'article 6 de la loi du 21 juin 2004, des informations ou documents traités ou conservés

par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. Selon l'article L. 811-3 du code de la sécurité intérieure, « *pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants : / 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; / 2° 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 ; / 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; / 4° La prévention du terrorisme ; / 5° La prévention : / a) Des atteintes à la forme républicaine des institutions ; / b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L.212-1 ; / c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; / 6° La prévention de la criminalité et de la délinquance organisées ; / 7° La prévention de la prolifération des armes de destruction massive* ». L'article L. 811-4 renvoie à un décret en Conseil d'État le soin de désigner les services, autres que les services spécialisés de renseignement, qui peuvent être autorisés à recourir aux techniques mentionnées au titre V du même livre VIII.

20. Il résulte de l'ensemble des dispositions mentionnées aux points précédents que le législateur a entendu imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs l'obligation de conserver de manière générale et indifférenciée les données de connexion pour les besoins, d'une part, de la recherche, de la constatation et de la poursuite des infractions, notamment pénales, et, d'autre part, des missions de défense et

de promotion des intérêts fondamentaux de la Nation confiées aux services de renseignement, dans les conditions et limites fixées par la loi et les dispositions réglementaires prises pour son application.

En ce qui concerne les dispositions réglementaires dont il est demandé l'abrogation :

21. L'article R. 10-13 du code des postes et des communications électroniques, dont le refus d'abrogation est contesté sous les n[os] 393099, 424717 et 424718, énumère les données qui doivent être conservées, pour une durée d'un an à compter du jour de leur enregistrement, par les opérateurs de communications électroniques aux fins mentionnées au point précédent. Sont concernées par cette obligation : « *a) Les informations permettant d'identifier l'utilisateur ; / b) Les données relatives aux équipements terminaux de communication utilisés ; / c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; / d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; / e) Les données permettant d'identifier le ou les destinataires de la communication* ». Il prévoit également que, pour les activités de téléphonie, l'opérateur doit conserver les données relatives au trafic « *et, en outre, celles permettant d'identifier l'origine et la localisation de la communication* ».

22. Pour l'application des dispositions de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, l'article 1[er] du décret du 25 février 2011, dont le refus d'abrogation est contesté sous le n° 393099, prévoit que : « *Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes : / 1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés : / a) L'identifiant de la connexion ; / b) L'identifiant attribué par ces personnes à l'abonné ; / c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ; / d) Les dates et heure de début et de fin de la connexion ; / e) Les caractéristiques de la ligne de l'abonné ; / 2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création : / a) L'identifiant*

de la connexion à l'origine de la communication ; / b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ; / c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ; / d) La nature de l'opération ; / e) Les date et heure de l'opération ; / f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ; / 3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte : / a) Au moment de la création du compte, l'identifiant de cette connexion ; / b) Les nom et prénom ou la raison sociale ; / c) Les adresses postales associées ; / d) Les pseudonymes utilisés ; / e) Les adresses de courrier électronique ou de compte associées ; / f) Les numéros de téléphone ; / g) Les données permettant de vérifier le mot de passe ou de le modifier, dans leur dernière version mise à jour ; / 4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement : / a) Le type de paiement utilisé ; / b) La référence du paiement ; / c) Le montant ; / d) La date et l'heure de la transaction ».

En ce qui concerne les exigences qui découlent du droit de l'Union européenne :

S'agissant des textes de droit dérivé applicables :

23. La directive du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, qui a été prise sur le fondement de l'article 95 du traité instituant la Communauté européenne, désormais repris à l'article 114 du traité sur le fonctionnement de l'Union européenne, procède de la volonté de rapprocher les législations des États membres afin de permettre l'établissement et le fonctionnement du marché intérieur. Elle a pour objet, ainsi que l'énonce le paragraphe 1 de son article 3, le « *traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communication dans la Communauté* ». Aux termes de son article 5 : « *1. Les États membres garantissent, par la législation*

nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité », tandis qu'en vertu de son article 6 : « 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1 ». Toutefois, l'article 15 de la même directive prévoit que « *Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne* ».

24. Il résulte des articles 1er et 2 de cette directive, tels qu'interprétés par la Cour de justice de l'Union européenne, que les dispositions

précitées s'appliquent aux opérateurs de services de communications électroniques, c'est-à-dire aux services qui consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, tels que les services d'accès à internet. Les opérateurs mentionnés à l'article L. 34-1 du code des postes et des communications électroniques, notamment les fournisseurs d'accès à internet et les opérateurs de téléphonie, ainsi que les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne au sens du paragraphe 1 du I de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, ce qui vise en particulier les fournisseurs d'accès à internet, relèvent du champ d'application de cette directive. Tel n'est pas le cas, en revanche, des « hébergeurs », c'est-à-dire des personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, mentionnées au paragraphe 2 du I du même article 6, dès lors que leurs services ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques.

25. L'article 23 du règlement du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (RGPD) prévoit que : « *1. Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir : / a) la sécurité nationale ; / b) la défense nationale ; / c) la sécurité publique ; / d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité*

publique et la prévention de telles menaces (...) ». Les hébergeurs mentionnés au point précédent constituent, au titre de cette activité, des responsables de traitement de données à caractère personnel, comme tels soumis aux dispositions de ce règlement.

26. Il ressort des dispositions citées aux points précédents que les États membres sont autorisés, pour des motifs tenant à la sauvegarde de la sécurité nationale, à la sûreté de l'État ou à la lutte contre les infractions pénales, à prévoir une dérogation, d'une part, à l'obligation de confidentialité des données à caractère personnel et, d'autre part, à celle de confidentialité des données relatives au trafic y afférentes, qui découlent toutes deux de l'article 5, paragraphe 1, de la directive, ainsi qu'aux droits et obligations prévues aux articles 12 à 22 du RGPD.

S'agissant de la réponse apportée par la Cour de justice de l'Union européenne aux questions préjudicielles posées par le Conseil d'État :

27. Par son arrêt du 6 octobre 2020 La Quadrature du Net et autres (C-511/18, C-512/18, C-520/18), la Cour de justice de l'Union européenne a, en réponse aux questions que lui avait posées le Conseil d'État dans sa décision avant-dire droit du 26 juillet 2018, dit pour droit que : « *1) L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, ne s'oppose pas à des mesures législatives /*

- permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ; / - prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ; / - prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ; / - prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et / - permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent

ces fournisseurs de services / dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

28. Si la Cour a également dit pour droit que « *l'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services* », elle a relevé, au point 211 de sa décision, qui constitue le soutien nécessaire de cette partie du dispositif, que : « *les constatations et les appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C511/18 et C512/18 ainsi qu'aux première et deuxième questions dans l'affaire C520/18 s'appliquent mutatis mutandis à l'article 23 du règlement 2016/679* ». Il en ressort clairement que les conditions permettant de déroger aux droits et obligations prévus aux articles 12 à 22 du RGPD sur le fondement de l'article 23 du règlement et celles permettant de déroger à l'interdiction de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation sur le fondement de l'article 15, paragraphe 1 de la directive du 12 juillet 2002 sont identiques.

29. Il résulte de ce qui a été dit aux points 27 et 28 que l'article 15, paragraphe 1, de la directive du 12 juillet 2002 et l'article 23 du RGPD, tels qu'interprétés par la Cour de justice dans son arrêt du 6 octobre 2020, limitent la possibilité d'imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation des données de connexion de leurs utilisateurs. L'encadrement précisé par la Cour de justice diffère selon la nature des données en cause, les finalités poursuivies et le type de conservation.

30. En premier lieu, le droit de l'Union européenne s'oppose à ce que soit imposée aux opérateurs la conservation généralisée et indifférenciée

des données de trafic et de localisation autres que les adresses IP, y compris aux fins de lutte contre la criminalité grave. Toutefois, il est possible d'imposer aux opérateurs une conservation ciblée de ces données, en fonction de catégories de personnes, dont des éléments objectifs permettent d'établir que leurs données sont susceptibles de révéler un lien au moins indirect avec des actes de criminalité grave, de contribuer, d'une manière ou d'une autre, à la lutte contre cette criminalité ou de prévenir un risque grave pour la sécurité publique, d'une part, ou en fonction de zones géographiques caractérisées par un risque élevé de préparation ou de commission d'actes de criminalité grave, d'autre part.

31. En revanche et en deuxième lieu, le droit de l'Union européenne permet d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de trafic et de localisation autres que les adresses IP aux seules fins de sauvegarde de la sécurité nationale lorsqu'un État est confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, sur injonction d'une autorité publique, soumise à un contrôle effectif d'une juridiction ou d'une autorité administrative indépendante, chargée notamment de vérifier la réalité de la menace, pour une période limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace.

32. En troisième lieu, le droit de l'Union européenne permet d'imposer aux opérateurs une « conservation rapide » des données de trafic et de localisation, c'est-à-dire une obligation à effet immédiat de conserver en l'état et pour une durée limitée au strict nécessaire certaines des données dont ils disposent, sous le contrôle d'un juge, lorsque ces données sont susceptibles de contribuer à l'élucidation d'une infraction grave ou à la prévention de menaces graves contre la sécurité publique. Ces données ne sont pas limitées aux personnes soupçonnées d'être les auteurs de l'infraction, mais peuvent être étendues à d'autres personnes pour les besoins de l'enquête, sur le fondement de critères objectifs.

33. En quatrième lieu, la conversation généralisée et indifférenciée des adresses IP peut être imposée aux fournisseurs d'accès à internet et aux hébergeurs, pour une période limitée au strict nécessaire, dès

lors qu'elle peut constituer, comme le relève la Cour au point 154 de sa décision, le seul moyen d'investigation permettant l'identification d'une personne ayant commis une infraction en ligne. Toutefois, dès lors qu'une telle conservation emporte une ingérence grave dans les droits fondamentaux des personnes concernées, elle ne saurait être justifiée qu'aux fins de lutte contre la criminalité grave, pour la prévention des menaces graves contre la sécurité publique et pour la sauvegarde de la sécurité nationale.

34. En dernier lieu, la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs est possible, sans délai particulier, aux fins de prévention des menaces à la sécurité publique, de recherche, de détection et de poursuite des infractions pénales en général et de sauvegarde de la sécurité nationale. Ainsi que la Cour le relève au point 157 de sa décision, l'ingérence qu'emporte la conservation de telles données ne saurait, en principe, être qualifiée de grave dès lors que ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes.

En ce qui concerne la compatibilité avec le droit de l'Union européenne des dispositions en litige :

S'agissant de la conservation générale et indifférenciée des données relatives à l'identité civile, aux paiements, aux contrats et aux comptes de l'abonné :

35. Ainsi qu'il a été dit au point 34, les données relatives à l'identité civile des utilisateurs de moyens de communications électroniques peuvent faire l'objet, sans limitation de durée, d'une conservation généralisée et indifférenciée pour les besoins de toute procédure pénale, de la prévention de toute menace contre la sécurité publique et de la sauvegarde de la sécurité nationale. Il suit de là que l'article R. 10-13 du code des postes et des communications électroniques et l'article 1er du décret du 25 février 2011, en tant qu'ils prévoient l'obligation pour les opérateurs de conserver de telles données, ne sont pas contraires au droit de l'Union européenne.

36. En outre, il résulte clairement de la directive du 12 juillet 2002 et du RGPD qu'ils ne s'opposent pas à une obligation de conservation généralisée et indifférenciée, pour une durée d'un an, des informations autres que celles relatives à l'identité civile fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, d'une part, et des données relatives aux paiements, d'autre part, mentionnées respectivement aux 3° et 4° de l'article 1er du décret du 25 février 2011.

S'agissant de la conservation générale et indifférenciée des adresses IP :

37. Il résulte de l'arrêt de la Cour de justice précité que, dans la mesure où elles ne révèlent aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication, et où elles peuvent constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction, les adresses IP attribuées à la source d'une connexion peuvent faire l'objet d'une obligation de conservation généralisée et indifférenciée à des fins de lutte contre la criminalité grave ou de prévention des menaces graves contre la sécurité publique, pour une période temporellement limitée au strict nécessaire.

38. Si la conservation généralisée et indifférenciée des adresses IP ne saurait être justifiée par les besoins de la lutte contre l'ensemble des infractions pénales, il ne résulte pas des énonciations de l'arrêt de la Cour de justice de l'Union européenne que le législateur serait tenu d'énumérer les infractions relevant du champ de la criminalité grave en se référant à des catégories strictement prédéfinies en droit interne. Le rattachement d'une infraction pénale à la criminalité grave a donc vocation à s'apprécier de façon concrète, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce. Une obligation de conservation généralisée et indifférenciée des adresses IP peut ainsi être imposée aux opérateurs, dès lors que les conditions d'accès à ces données par les services d'enquête sont fixées en fonction de la gravité des infractions susceptibles de le justifier, dans le respect du principe de proportionnalité, lequel fait partie des principes généraux du droit de l'Union européenne.

39. Les associations requérantes soutiennent que les dispositions attaquées relatives à la conservation des adresses IP méconnaissent le droit de l'Union européenne dès lors qu'elles ne circonscrivent pas cette conservation aux seules fins de lutte contre la criminalité grave. Or, aux termes de l'article préliminaire du code de procédure pénale : « *Au cours de la procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction* ». Conformément au principe de proportionnalité consacré par cet article, l'obligation de conservation résultant du III de l'article L. 34-1 du code des postes et des communications électroniques et du II de l'article 6 de la loi du 21 juin 2004 n'est donc imposée aux opérateurs, sous le contrôle des juridictions compétentes, que pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales susceptibles de présenter un degré de gravité suffisant pour justifier l'ingérence dans les droits protégés par les articles 4, 7 et 11 de la Charte des droits fondamentaux de l'Union européenne. Seules de telles infractions pouvant légalement justifier l'accès des services d'enquêtes aux données conservées par les opérateurs, il s'ensuit que la conservation des adresses IP imposée de façon généralisée et indifférenciée aux opérateurs ne saurait être regardée comme méconnaissant les exigences de la directive du 12 juillet 2002.

40. En outre, il résulte du III de l'article R. 10-13 du code des postes et des communications électroniques et de l'article 3 du décret du 25 février 2011 que les adresses IP ne peuvent être conservées qu'un an. Il ne ressort pas des pièces du dossier que cette durée de conservation ne serait pas strictement nécessaire aux besoins de la lutte contre la criminalité grave et de la prévention des menaces graves pour la sécurité publique.

41. Il résulte de ce qui précède que l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011, en tant qu'ils prévoient une obligation de conservation généralisée et indifférenciée des adresses IP, ne sont pas contraires au droit de l'Union européenne.

S'agissant de la conservation générale et indifférenciée des données de trafic et de localisation autres que les adresses IP :

42. Ainsi qu'il a été dit au point 31, la Cour a dit pour droit que la directive ne s'opposait pas à ce que des mesures législatives permettent, aux fins de sauvegarde de la sécurité nationale, d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de trafic et des données de localisation, sous réserve qu'une décision soumise à un contrôle effectif constate l'existence d'une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, pour une durée limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. Il ressort en outre du point 135 de son arrêt du 6 octobre 2020 que la responsabilité des États membres en matière de sécurité nationale, au sens du droit de l'Union, correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société, et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme.

Quant à la conservation générale et indifférenciée de ces données de connexion aux fins de sauvegarde de la sécurité nationale :

43. En premier lieu, les dispositions citées aux points 16, 18 et 19 imposent la conservation généralisée et indifférenciée, pour une durée d'un an, des données énumérées à l'article R. 10-13 du code des postes et des communications électroniques et à l'article 1er du décret du 25 février 2011 en vue de défendre et de promouvoir les intérêts fondamentaux de la Nation énumérés à l'article L. 811-3 du code de la sécurité intérieure, de même que pour les besoins de la recherche, de la constatation et de la poursuite d'infractions qui mettent en cause la sécurité nationale, notamment les atteintes aux intérêts fondamentaux de la Nation figurant au titre Ier du livre IV du code pénal et le terrorisme réprimé par les dispositions de son titre II. Dans cette mesure, cette obligation de conservation imposée aux opérateurs, mise en œuvre par des dispositions à caractère réglementaire susceptibles de faire

l'objet d'un recours pour excès de pouvoir devant le juge administratif, assorti, le cas échéant, d'une demande de suspension de leurs effets sur le fondement de l'article L. 521-1 du code de justice administrative, ou d'un référé fondé sur l'article L. 521-2 du même code, est justifiée, dans son principe, par l'objectif de sauvegarde de la sécurité nationale.

44. En deuxième lieu, il ressort des pièces du dossier, notamment des mesures d'instruction diligentées par la dixième chambre de la section du contentieux, que la France est confrontée à une menace pour sa sécurité nationale, appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure cité au point 19 qui, par son intensité, revêt un caractère grave et réel. Cette menace est, à la date de la présente décision, non seulement prévisible mais aussi actuelle. Cette menace procède d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés. Deux nouveaux attentats ont déjà été déjoués en 2021. Le plan Vigipirate a été mis en œuvre au niveau « Urgence attentat » entre le 29 octobre 2020 et le 4 mars 2021 puis au niveau « Sécurité renforcée - risque attentat » depuis le 5 mars 2021, attestant d'un niveau de menace terroriste durablement élevé sur le territoire. Par ailleurs, la France est particulièrement exposée au risque d'espionnage et d'ingérence étrangère, en raison notamment de ses capacités et de ses engagements militaires et de son potentiel technologique et économique. De nombreuses entreprises françaises, tant des grands groupes que des petites et moyennes entreprises, font ainsi l'objet d'actions malveillantes, visant leur savoir-faire et leur potentiel d'innovation, à travers des opérations d'espionnage industriel ou scientifique, de sabotage, d'atteintes à la réputation ou de débauchage d'experts. La France est également confrontée à des menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes. Ces menaces sont de nature à justifier l'obligation de conservation généralisée et indifférenciée des données de connexion listées à l'article R. 10-13 du code des postes et des communications électroniques autres que les données relatives à l'identité civile et aux adresses IP. En outre, il ne ressort pas des pièces du dossier que la durée de conservation de ces données, fixée à un an,

ne serait pas strictement nécessaire aux besoins de la sauvegarde de la sécurité nationale.

45. En troisième lieu, toutefois, ni l'article L. 34-1 du code des postes et des communications électroniques, ni l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique ne prévoient un réexamen périodique, au regard des risques pour la sécurité nationale, de la nécessité de maintenir l'obligation faite aux personnes concernées de conserver les données de connexion. Les dispositions de ces articles, ainsi, par suite, que celles de l'article R. 10-13 du code des postes et des communications électroniques et du décret du 25 février 2011, en tant qu'elles ne subordonnent pas le maintien en vigueur de cette obligation au constat, à échéance régulière, qui ne saurait raisonnablement excéder un an, de la persistance d'une menace grave, réelle et actuelle ou prévisible, pour la sécurité nationale sont, dans cette mesure, contraires au droit de l'Union européenne. Par ailleurs, le fait d'imposer aux pouvoirs publics un tel réexamen n'affecte pas, par lui-même, les exigences constitutionnelles mentionnées au point 9.

46. Il résulte de ce qui précède que, s'agissant de l'objectif de sauvegarde de la sécurité nationale, le refus d'abroger l'article R. 10-13 du code des postes et des communications électroniques et l'article 1er du décret du 25 février 2011 doit être annulé en tant seulement que leurs dispositions ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, s'agissant des données qu'elles mentionnent autres que celles afférentes à l'identité civile, aux comptes et aux paiements des utilisateurs et aux adresses IP. Il y a lieu d'enjoindre au Gouvernement de compléter ces dispositions dans un délai de six mois à compter de la présente décision. Dans la mesure où il résulte de la présente décision, ainsi qu'il a été dit au point 44, que la réalité et la gravité de la menace pesant sur la sécurité nationale justifient l'obligation de conservation généralisée et indifférenciée de l'ensemble des données de connexion à cette fin, les opérateurs ne sauraient, avant l'expiration de ce délai, se soustraire à cette obligation et aux sanctions dont sa méconnaissance est assortie au motif que la durée de l'injonction qui leur est faite n'a pas été limitée dans le temps par le pouvoir réglementaire.

Quant à la conservation générale et indifférenciée de ces données de connexion aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public :

47. Les dispositions mentionnées aux points 16 et 18 organisent également la conservation généralisée et indifférenciée des données de connexion pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales, ou de manquements à certaines législations particulières, ne mettant pas en jeu la sécurité nationale.

48. Ainsi qu'il a été rappelé aux points 30 à 34, le droit de l'Union européenne, tel qu'interprété par la Cour de justice, s'oppose à une obligation de conservation généralisée et indifférenciée des données de connexion, autres que celles d'identification des utilisateurs et les adresses IP, aux fins de lutte contre la criminalité et la prévention des menaces pour la sécurité publique, quel que soit le degré de gravité de cette criminalité ou de ces menaces.

49. Le Premier ministre soutient en défense que l'obligation pour le juge d'écarter les dispositions du droit national imposant une conservation généralisée et indifférenciée des données de connexion pour des finalités autres que de sauvegarde de la sécurité nationale priverait de garanties effectives les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment des atteintes à la sécurité des personnes et des biens, et de recherche des auteurs d'infractions pénales.

50. En premier lieu, il ressort des pièces du dossier, notamment des mesures d'instruction diligentées par la dixième chambre de la section du contentieux, ainsi que des échanges intervenus au cours de la séance orale d'instruction qui s'est tenue le 22 mars 2021, que l'obligation de conservation généralisée et indifférenciée des données de connexion pour une période d'un an, imposée aux opérateurs sur le fondement des dispositions mentionnées aux points 16, 18, 21 et 22, est une condition déterminante de succès des enquêtes conduites en vue de la recherche, de la constatation et de la poursuite des auteurs d'infractions à caractère criminel et délictuel. L'exploitation ultérieure de ces données, en particulier des données de localisation

du détenteur d'un équipement terminal, est en effet, dans de très nombreuses hypothèses, l'unique moyen de retrouver leurs auteurs. Il ne ressort en outre pas des pièces du dossier que des méthodes alternatives puissent utilement s'y substituer. Par construction, les méthodes d'investigation traditionnelles, telles que les filatures et les surveillances, outre les aléas auxquelles elles sont confrontées, ne permettent pas d'apporter d'éléments sur des événements passés et sont inefficaces pour les infractions dématérialisées. Les méthodes d'investigation scientifique, telles que la recherche d'empreintes digitales et de traces génétiques, ne peuvent être efficaces que si des éléments matériels sont laissés par les auteurs d'infraction. À l'inverse, s'il existe des méthodes d'investigation complexes présentant une réelle efficacité pour l'élucidation des crimes et délits, comme la captation de données en temps réel, elles sont plus intrusives et plus attentatoires aux libertés. L'accès différé aux données de connexion revêt une importance d'autant plus cruciale que l'utilisation des moyens de communications électroniques, notamment cryptées, constitue un instrument qui facilite la commission de ces crimes et délits et rend plus difficile la recherche de leurs auteurs. Il permet, à l'inverse, de lever les soupçons pesant sur des personnes suspectées, à tort, d'y être impliquées.

51. En deuxième lieu, les articles 5, 6 et 9 de la directive 2002/58 ménagent, il est vrai, aux opérateurs la faculté de conserver certaines données pour les besoins de l'acheminement des communications et des opérations de facturation et de paiement des services rendus. Ces dispositions sont transposées au IV de l'article L. 34-1 et à l'article R. 10-14 du code des postes et des communications électroniques. Il résulte de ces dispositions, combinées avec l'article L. 34-2 du même code, que les données nécessaires aux opérations relatives à la facturation et au paiement des factures sont susceptibles d'être conservées jusqu'à l'expiration du délai de prescription des demandes en restitution du prix des prestations formées par les utilisateurs, fixé à un an à compter du jour du paiement, ou des demandes de paiement des prestations formulées par les opérateurs, également fixé à un an à compter de la date d'exigibilité des sommes. Toutefois, il ressort des pièces du dossier que seule une partie des données couvertes par l'article R. 10-13

est volontairement conservée par les opérateurs pour leurs besoins propres ou pour la sécurité des réseaux et installations au titre du seul article R. 10-14, et pour des durées moindres. En particulier, les données de connexion relatives aux appels entrants et celles relatives à la géolocalisation ne font que très rarement l'objet d'une conservation à ce titre de la part des opérateurs. De même, les données relatives aux appels sortants dans le cadre de forfaits illimités ne sont pas conservées dès lors qu'elles ne sont pas utiles à la facturation. Or le recueil de ces données contribue de façon déterminante à l'efficacité des enquêtes pénales.

52. En troisième lieu, il résulte de la jurisprudence de la Cour de justice que la directive ne s'oppose pas à une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable, en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique.

53. Il ressort cependant des pièces du dossier, notamment des éléments recueillis auprès de la Fédération française des télécoms, qu'une telle conservation ciblée se heurte à des obstacles techniques qui en compromettent manifestement la mise en œuvre. En ce qui concerne une conservation ciblée selon des critères géographiques, il apparaît que l'implantation des relais de téléphonie mobile et de leurs cellules est propre à chaque opérateur, que le mode de propagation des ondes radio émises par les relais de téléphonie mobile n'est pas compatible avec des limites géographiques prédéfinies et que l'information de localisation n'est pas systématiquement présente dans les données collectées. Les sociétés Free Mobile et Free indiquent, quant à elles, que les données de connexion stockées dans leur système d'information ne sont pas associées à une zone géographique particulière, qu'au surplus cette localisation est changeante dans le temps et qu'elles ne sont en mesure d'établir une corrélation entre la « cellule » radio à laquelle sont associées des données de connexion et la localisation géographique de cette cellule qu'au cas par cas, en réponse à une

réquisition judiciaire. Quant à une conservation ciblée sur des personnes, la Fédération française des télécoms fait valoir qu'elle se heurterait au fait que les informations contenues dans les données de trafic ne permettent pas d'effectuer un tri selon des catégories de personnes. Les sociétés Free et Free Mobile précisent, pour leur part, que les personnes sont identifiées par des données - le numéro de téléphone, le numéro IMSI et le numéro IMEI - qui peuvent varier dans le temps et que ces données sont gérées de façon étanche pour répondre aux exigences du RGPD.

54. En outre, une conservation ciblée, à la supposer techniquement possible, présenterait un intérêt opérationnel particulièrement incertain, dès lors qu'elle ne permettrait pas, y compris en cas de faits particulièrement graves, d'accéder aux données de connexion d'une personne suspectée d'une infraction qui n'aurait pas été préalablement identifiée comme étant susceptible de commettre un tel acte. Ainsi, notamment pour les cas de primo-délinquants, mais également lorsque les auteurs d'infractions pénales ont recours à des téléphones dotés de cartes prépayées qu'ils n'utilisent que pour une durée limitée et qui, par construction, n'auraient pu être préalablement identifiés, les services d'enquête judiciaire ne pourraient pas accéder aux données de connexion indispensables à l'élucidation des affaires dont ils sont saisis. Par ailleurs, il est impossible de définir par avance des zones géographiques où, par nature, aucun acte de criminalité grave susceptible de justifier la conservation des données de connexion ne pourrait survenir. Une obligation de conservation des données de connexion limitée à certaines zones géographiques, à supposer même qu'elle soit techniquement envisageable, ferait ainsi obstacle à l'action des services d'enquête dans les autres parties du territoire national lorsque de telles infractions y seraient commises. Enfin, aucune présomption de dangerosité ne saurait être légalement retenue à l'encontre de personnes en fonction de leur lieu de résidence ou d'activité professionnelle pour justifier la conservation de leurs données de trafic et de localisation. Une différence de traitement instaurée sur ces fondements serait contraire au principe constitutionnel d'égalité devant la loi.

55. En quatrième lieu, la Cour de justice a admis, au regard de la directive 2002/58 et du RGPD, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données de trafic et des données de localisation dont disposent ces fournisseurs de services, au sens de l'article 16 de la convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001. Les stipulations de cette convention, à laquelle la France est partie, lui font obligation d'adopter les mesures nécessaires pour permettre à ses autorités, aux fins d'enquêtes et de procédures pénales et en vue d'assurer la collecte des preuves électroniques de toute infraction pénale, d'ordonner ou d'imposer d'une autre manière la conservation rapide de données de trafic, stockées au moyen d'un système informatique, et, en particulier pour obliger la personne qui les détient ou les contrôle à conserver et protéger l'intégrité de ces données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, le cas échéant renouvelable, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Selon la Cour de justice, une telle conservation rapide peut non seulement porter sur les données des personnes concrètement soupçonnées d'avoir projeté ou commis une infraction pénale ou une atteinte à la sécurité nationale, mais aussi sur les données d'autres personnes, pour autant qu'elles peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation de cette infraction ou de cette atteinte à la sécurité nationale, telles que les données de la victime de celle-ci et de son entourage social ou professionnel, ou encore des données relatives à des zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction. Au point 164 de sa décision, la Cour précise ainsi que : « *Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et*

8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence. En outre, afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient ». Il s'ensuit que, lorsqu'est en cause une infraction suffisamment grave pour justifier l'ingérence dans la vie privée induite par la conservation des données de connexion, dans le respect du principe de proportionnalité rappelé aux points 38 et 39, l'autorité judiciaire peut, sans méconnaître ni la directive du 12 juillet 2002, ni le RGPD, enjoindre aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de sites internet de procéder à la conservation rapide des données de trafic et de localisation qu'ils détiennent, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale.

56. La conservation rapide des données de connexion est ainsi de nature à faire obstacle à la disparition des informations nécessaires à la recherche, à la constatation et à la poursuite des auteurs d'infractions pénales à compter de la date et de l'heure à laquelle il est enjoint à un opérateur d'y procéder, à la suite de la commission d'une infraction ou du recueil d'éléments donnant à penser qu'une telle infraction est projetée, ainsi qu'à l'effacement ou à l'anonymisation des données relatives à des communications antérieures lorsqu'elles ont été conservées par les opérateurs. Cependant, sur ce dernier point, l'efficacité du dispositif est subordonnée à la condition que les données aient été effectivement conservées. À défaut, la conservation rapide ne permet pas aux services d'enquête et à l'autorité judiciaire d'exploiter des données relatives aux communications effectuées avant qu'elle soit ordonnée.

57. Il résulte de ce qui précède que ni l'accès aux données de connexion conservées volontairement par les opérateurs, ni la possibilité de leur imposer une obligation de conservation ciblée, ni le recours à la technique de la conservation rapide ne permettent, par eux-mêmes, de garantir le respect des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, ainsi que de recherche des auteurs d'infractions, notamment pénales. Toutefois, d'une part, à la date de la présente décision, l'état des menaces pesant sur la sécurité nationale rappelées au point 44 justifie légalement que soit imposée aux opérateurs la conservation générale et indifférenciée des données de connexion. D'autre part, la conservation rapide des données susceptibles de contribuer à la recherche, la constatation et la poursuite des infractions pénales, dans le respect du principe de proportionnalité prévu par le code de procédure pénale conformément à ce qui a été rappelé au point 39, est possible dans les conditions prévues par la directive du 12 juillet 2002 et le RGPD, y compris, comme l'a jugé la Cour ainsi qu'il a été rappelé au point 55, lorsque cette conservation rapide porte sur des données initialement conservées aux fins de sauvegarde de la sécurité nationale. L'autorité judiciaire est donc en mesure d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie. Le même principe s'applique nécessairement aux autorités administratives indépendantes disposant d'un droit d'accès aux données de connexion en vertu de la loi en vue de lutter contre les manquements graves aux règles dont elles ont la charge d'assurer le respect. Dans ces conditions, le Premier ministre n'est pas fondé à soutenir qu'en l'état, la mise à l'écart des dispositions contestées du droit national, au motif qu'elles seraient contraires au droit de l'Union européenne, priverait de garanties effectives les objectifs de valeur constitutionnelle invoqués.

58. Il résulte de tout ce qui précède que le Gouvernement ne pouvait pas imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation généralisée et indifférenciée des données de connexion, autres que les données mentionnées aux points 33, 34 et 36, relatives à

l'identité civile, aux adresses IP et aux informations relatives aux comptes et aux paiements, aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public sans méconnaître le droit de l'Union européenne. Il ressort du point précédent qu'à la date de la présente décision, et aussi longtemps que l'existence d'une menace grave sur la sécurité nationale justifie la conservation généralisée et indifférenciée des données de connexion, l'application du droit de l'Union européenne, en conduisant à écarter le droit national, ne prive pas de garanties effectives les objectifs de valeur constitutionnelle invoqués par le Premier ministre en défense. Il y a dès lors lieu d'écarter les articles L. 34-1 du code des postes et des communications électroniques et 6 de la loi du 21 juin 2004 en tant qu'ils poursuivent une finalité autre que celle de la sauvegarde de la sécurité nationale. Par suite, les associations requérantes sont fondées à soutenir que les dispositions du I et du II de l'article R. 10-13 du code des postes et des communications électroniques d'une part, et du 1° et du 2° de l'article 1er du décret du 25 février 2011 sont entachées d'illégalité dans cette mesure. C'est donc à tort que le Premier ministre a refusé d'en prononcer l'abrogation dans cette même mesure.

59. Il y a lieu de décider que le Premier ministre disposera d'un délai d'au plus six mois à compter de la notification de la présente décision pour limiter les finalités poursuivies par ces articles et adapter le cadre réglementaire relatif à la conservation des données de connexion. Il n'y a pas lieu, dans les circonstances de l'espèce, d'assortir cette injonction d'une astreinte.

III. Sur les traitements mis en œuvre par les services de renseignement sur les données de connexion :

60. Les associations requérantes contestent la conformité au droit de l'Union européenne de quatre techniques de renseignement. La première, définie par l'article L. 851-1 du code de la sécurité intérieure, permet aux services de renseignement d'accéder aux données de trafic et de localisation conservées par les opérateurs de communications électroniques, les fournisseurs d'accès à internet et les hébergeurs de contenu. La deuxième,

définie à l'article L. 851-2 du code leur permet, pour les seuls besoins de prévention du terrorisme, de recueillir en temps réel ces données pour les personnes préalablement identifiées comme présentant une menace. La troisième, prévue par l'article L. 851-3 du code, permet la mise en place de traitements automatisés sur les données de connexion conservées par les opérateurs afin de détecter des connexions susceptibles de révéler une menace terroriste. Enfin, l'article L. 851-4 permet aux services de renseignement de recueillir en temps réel les données techniques relatives à la localisation des équipements terminaux de communications électroniques. Les associations requérantes soutiennent que ces dispositions méconnaissent le droit de l'Union européenne tel qu'interprété par l'arrêt de la Cour de justice du 6 octobre 2020. Il y a lieu d'apprécier, en premier lieu, l'opérance des moyens invoqués, en deuxième lieu, la conformité au droit de l'Union de chacune de ces méthodes de renseignement et, en troisième lieu, d'examiner les autres moyens invoqués tirés de ce que les garanties procédurales encadrant les dispositions législatives du livre VIII du code de la sécurité intérieure seraient insuffisantes au regard du droit de l'Union.

En ce qui concerne l'opérance du moyen tiré de ce que les dispositions législatives du code de la sécurité intérieure seraient incompatibles avec le droit de l'Union européenne :

61. Sous les nos 394922, 397844 et 397851, les associations requérantes soutiennent, par la voie de l'exception, que les articles L. 851-1 à L. 851-4 du code de la sécurité intérieure seraient incompatibles avec le droit de l'Union européenne.

62. La contrariété d'une disposition législative aux stipulations d'un traité international ou au droit de l'Union européenne ne peut être utilement invoquée à l'appui de conclusions dirigées contre un acte réglementaire que si ce dernier a été pris pour son application ou si en elle constitue la base légale.

63. Le décret du 28 septembre 2015 désigne, en application de l'article L. 811-2 du code de la sécurité intérieure, les services spécialisés de renseignement et prévoit les modalités d'application des articles L. 853-1 à L. 853-3 du code. Il suit de là que les associations requérantes

ne sauraient utilement contester, par la voie de l'exception, l'incompatibilité avec le droit de l'Union européenne des articles L. 851-1 à L. 851-4 à l'appui de leurs conclusions dirigées contre ce décret, qui n'a pas été pris pour l'application de ces articles et dont ceux-ci ne constituent pas la base légale. La requête présentée sous le n° 394922 doit, par suite, être rejetée.

64. L'article 3 du décret du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure, insère dans le code des articles R. 851-1 et R. 851-2 qui désignent les services autres que les services spécialisés de renseignement qui peuvent, pour des finalités qu'ils précisent, recourir aux techniques définies par les articles L. 851-1 et L. 851-4 du code. Les autres dispositions du décret ne sont pas prises pour l'application des articles L. 851-1 à L. 851-4 et ces articles n'en constituent pas la base légale. Il suit de là que l'association Igwan.net ne saurait utilement contester, par la voie de l'exception, l'incompatibilité avec le droit de l'Union européenne des articles L. 851-1 et L. 851-4 du code de la sécurité intérieure qu'à l'appui de ses conclusions dirigées contre les dispositions de l'article 3 du décret contesté en tant qu'il insère les articles R. 851-1 et R. 851-2 dans ce code. Ses conclusions dirigées contre les autres dispositions de ce décret ne peuvent, dès lors, qu'être rejetées.

65. L'article 1er du décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement insère au code de la sécurité intérieure un article R. 823-1 qui précise le rôle du groupement interministériel de contrôle. Aux termes du 3° de cet article, ce service est chargé de : « *Recueillir et conserver les informations ou documents mentionnés à l'article L. 851-1 dans les conditions fixées au chapitre Ier du titre V du présent livre* ». Par ailleurs, l'article 2 du décret insère au même code un article R. 851-1-1, qui désigne les services autres que les services spécialisés de renseignement pouvant être autorisés à utiliser la technique mentionnée à l'article L. 851-2 du code de la sécurité intérieure au titre de la prévention du terrorisme, et des articles R. 851-5 à R. 851-10 qui précisent notamment les conditions d'application

des articles L. 851-1 à L. 851-4. Les autres dispositions du décret ne sont pas prises pour l'application des articles L. 851-1 à L. 851-4 et ces articles n'en constituent pas la base légale. Il suit de là que les associations requérantes ne peuvent utilement contester, par la voie de l'exception, l'incompatibilité avec le droit de l'Union européenne des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure qu'à l'appui de leurs conclusions dirigées contre l'article 1er du décret attaqué en tant qu'il insère au code le 3° de l'article R. 823-1 et contre l'article 2 en tant qu'il insère au même code les articles R. 851-1-1 et R. 851-5 à R. 851-10. Leurs conclusions dirigées contre les autres dispositions de ce décret ne peuvent, dès lors, qu'être rejetées.

En ce qui concerne la conformité au droit de l'Union des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure :

S'agissant de l'accès administratif par les services de renseignement aux données de trafic et de localisation prévu par l'article L. 851-1 du code de la sécurité intérieure :

Quant au moyen tiré de ce que les dispositions attaquées organisent l'accès à des données conservées en méconnaissance du droit de l'Union :

66. Il ressort clairement des pièces du dossier qu'en 2015 et 2016, date à laquelle les décrets attaqués ont été adoptés, la France était confrontée à une menace grave, réelle et actuelle pour sa sécurité nationale, ainsi qu'en témoignent notamment l'attentat ayant visé « Charlie Hebdo » survenu le 7 janvier 2015 et la série d'attentats du 13 novembre 2015. Il s'ensuit que le livre VIII du code de la sécurité intérieure pouvait, ainsi qu'il a été dit précédemment, imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation généralisée et indifférenciée des données de trafic et de localisation aux fins de sauvegarde de la sécurité nationale.

Quant aux finalités poursuivies par les services de renseignement :

67. Dans sa rédaction applicable au litige, l'article L. 851-1 du code de la sécurité intérieure dispose que : « *Dans les conditions prévues au chapitre I^er^ du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications (...)* ». En application de l'article L. 811-3 du même code : « *Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants : / 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; / 2° 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 ; / 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; / 4° La prévention du terrorisme ; / 5° La prévention : / a) Des atteintes à la forme républicaine des institutions ; / b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; / c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; / 6° La prévention de la criminalité et de la délinquance organisées ; / 7° La prévention de la prolifération des armes de destruction massive* ». Dès lors que ces finalités concourent à la défense des intérêts fondamentaux de la Nation, elles doivent être regardées comme relevant de la sauvegarde de la sécurité nationale au sens de l'article 15 de la directive du 12 juillet 2002.

Quant à l'existence d'un contrôle préalable :

68. Par son arrêt du 21 décembre 2016 Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson et autres (C-203/15 et C 698/15), la Cour de justice de l'Union européenne a dit pour droit que l'article 15 de la directive du 12 juillet 2002 devait : « *être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante* ». Le point 120 de cet arrêt précise que « *Aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales* ». Si la Cour de justice n'a rappelé cette règle dans son arrêt du 6 octobre 2020 qu'à propos du recueil en temps réel des données de connexion par les services de renseignement, elle a réitéré le principe du contrôle préalable de l'accès des autorités nationales aux données de connexion par une juridiction ou une autorité administrative indépendante dans son arrêt du 2 mars 2021, H.K. / Prokuratuur (C-746/18).

69. Il résulte de ce qui a été dit au point précédent que l'accès des services de renseignement aux données de trafic et de localisation conservées par les opérateurs de communications électroniques sur le fondement des articles L. 34-1 du code des postes et des communications électroniques et 6 de la loi du 21 juin 2004, pour les finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure, qui toutes relèvent de la sauvegarde de la sécurité nationale, est possible

sans méconnaître les dispositions de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 et de l'article 23 du RGPD, à condition que cet accès soit soumis, sauf en cas d'urgence dûment justifiée, à un contrôle préalable par une juridiction ou une autorité administrative indépendante dotée d'un pouvoir contraignant et s'opère sur le fondement de critères objectifs et non discriminatoires.

70. D'une part, en vertu des articles L. 821-1 à L. 821-8 du code de la sécurité intérieure, la mise en œuvre des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 du code est soumise à l'autorisation préalable du Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement, laquelle contrôle notamment le respect du principe de proportionnalité de l'atteinte à la vie privée qu'entrainent ces techniques, en vertu de l'article L. 801-1 du code. Cette autorisation est délivrée sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes. L'autorisation de mise en œuvre de ces techniques est délivrée pour une durée maximale de quatre mois. Si, en cas d'urgence absolue et pour les seules finalités mentionnées aux points 1°, 4° et a) du 5° de l'article L. 811-3, le recours à ces techniques de renseignement peut être autorisé sans avis préalable de la Commission nationale de contrôle des techniques de renseignement, le Premier ministre lui fait parvenir, dans un délai maximal de vingt-quatre heures, tous les éléments de motivation de la demande et ceux justifiant le caractère d'urgence absolue. Enfin, l'article L. 822-2 du code précise les délais dans lesquels les renseignements collectés doivent être détruits.

71. D'autre part, aux termes de l'article L. 833-4 du code de la sécurité intérieure : « *De sa propre initiative ou lorsqu'elle est saisie d'une réclamation de toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard, la commission procède au contrôle de la ou des techniques invoquées en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect du présent livre. Elle notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer leur mise en œuvre* ». Le Conseil d'État peut en outre être saisi, conformément à

l'article L. 841-1 par : « *1° Toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard et justifiant de la mise en œuvre préalable de la procédure prévue à l'article L. 833-4 ; / 2° La Commission nationale de contrôle des techniques de renseignement, dans les conditions prévues à l'article L. 833-8 ». Enfin, l'article L. 833-8 du code prévoit que : « Le Conseil d'État peut être saisi d'un recours prévu au 2° de l'article L. 841-1 soit par le président de la commission lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission ou que les suites qui y sont données sont estimées insuffisantes, soit par au moins trois membres de la commission* ».

72. Il résulte de l'article L. 801-1 du code de la sécurité intérieure que l'autorité publique ne peut porter atteinte au respect de la vie privée, dans toutes ses composantes, notamment la protection des données à caractère personnel, que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité. À ce titre, l'autorisation et la mise en œuvre sur le territoire national de la technique de renseignement prévue à l'article L. 851-1 de ce code ne peuvent être décidées que si elles procèdent d'une autorité ayant légalement compétence pour le faire, s'inscrivent dans les missions confiées aux services de renseignement, respectent la procédure d'autorisation et les règles de conservation par les services de renseignement définies au titre II du livre VIII de ce code, sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, et si les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués.

73. La mise en œuvre de la technique de renseignement prévue à l'article L. 851-1 du code de la sécurité intérieure ne donne pas lieu au contrôle préalable par une juridiction ou par une autorité administrative indépendante dotée d'un pouvoir contraignant, dès lors que la Commission nationale de contrôle des techniques de renseignement n'émet qu'un avis simple ou des recommandations non contraignantes et que la saisine du Conseil d'État ne lui est ouverte, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, qu'après la délivrance de l'autorisation par le Premier

ministre et, le cas échéant, sa mise en œuvre. En revanche, les exigences rappelées au point 68 sont respectées en cas d'urgence dûment justifiée, dans la mesure où, d'une part, le président de la commission ou trois de ses membres peuvent saisir le Conseil d'État à bref délai lorsque l'avis de cette commission ou, dans les cas d'urgence absolue mentionnés à l'article L. 821-5 du code de la sécurité intérieure, la recommandation de la commission tendant à l'interruption de la mise en œuvre de la technique de renseignement litigieuse, n'a pas été suivi et où, d'autre part, il appartient à la formation spécialisée dans le contentieux des techniques de renseignement de se prononcer dans les plus brefs délais.

74. La directive du 12 juillet 2002 et le RGPD, tels qu'interprétés par la Cour de justice, imposent la mise en place d'un contrôle juridictionnel ou assuré par une autorité administrative indépendante dotée d'un pouvoir contraignant préalablement à l'accès différé aux données de connexion par les services de renseignement, en-dehors des cas d'urgence dûment justifiée. Cette obligation impose d'écarter les dispositions législatives contestées dans la seule mesure où elles ne prévoient pas un tel contrôle préalable, ce qui n'est pas susceptible de priver de garanties effectives les exigences constitutionnelles mentionnées au point 9. Il suit de là que le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement doit être annulé en tant qu'il permet l'accès en temps différé aux données de connexion par les services de renseignement, sans donner un caractère contraignant à l'avis de la Commission nationale de contrôle des techniques de renseignement, en-dehors des cas d'urgence dûment justifiée.

S'agissant de l'analyse automatisée des données de trafic et de localisation prévue à l'article L. 851-3 du code de la sécurité intérieure :

75. Aux termes de l'article L. 851-3 du code de la sécurité intérieure, dans sa rédaction applicable au litige : « *I.- Dans les conditions prévues au chapitre I^er^ du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste. / Ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans*

recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent. (...) II.- La Commission nationale de contrôle des techniques de renseignement émet un avis sur la demande d'autorisation relative aux traitements automatisés et les paramètres de détection retenus. Elle dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies. Elle est informée de toute modification apportée aux traitements et paramètres et peut émettre des recommandations (...) IV.- Lorsque les traitements mentionnés au I du présent article détectent des données susceptibles de caractériser l'existence d'une menace à caractère terroriste, le Premier ministre ou l'une des personnes déléguées par lui peut autoriser, après avis de la Commission nationale de contrôle des techniques de renseignement donné dans les conditions prévues au chapitre Ier du titre II du présent livre, l'identification de la ou des personnes concernées et le recueil des données y afférentes. Ces données sont exploitées dans un délai de soixante jours à compter de ce 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 ».

76. Dans son arrêt du 6 octobre 2020 précité, la Cour a dit pour droit que : « *L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée (...) des données relatives au trafic et des données de localisation (...) lorsque / le recours à l'analyse automatisée est limité à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours à cette analyse pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues* ».

77. Il ne peut être recouru à l'analyse automatisée des données de trafic et de localisation prévue à l'article L. 851-3 du code de la sécurité intérieure que pour les seuls besoins de la prévention du terrorisme. La mise en œuvre de cette méthode n'est possible qu'après avis de la Commission nationale de contrôle des techniques de renseignement, laquelle est chargée, notamment, de vérifier qu'elle est mise en œuvre pour cette seule finalité et qu'elle repose sur des critères objectifs et non discriminatoires. À cette occasion, la Commission vérifie l'existence et l'actualité de la menace grave pour la sécurité nationale susceptible de justifier une telle mesure. Si l'avis de la Commission n'est pas doté d'un effet contraignant, le Conseil d'État peut être saisi d'un recours dans les conditions prévues à l'article L. 833-8 précité. Cette procédure respecte l'exigence qu'une telle méthode de renseignement puisse faire l'objet d'un contrôle effectif par une juridiction ou une autorité administrative indépendante. En revanche, si, en vertu du IV de l'article L. 851-3, lorsqu'une menace est détectée par un traitement automatisé, le Premier ministre peut autoriser l'identification des personnes concernées et le recueil des données y afférentes après un réexamen individuel, cette identification n'est pas subordonnée à un contrôle préalable exercé par une juridiction ou par une autorité administrative indépendante dotée d'un pouvoir contraignant. Il s'ensuit que le IV de l'article L. 851-3 du code de la sécurité intérieure méconnaît l'article 15, paragraphe 1, de la directive du 12 juillet 2002 et l'article 23 du RGPD dans cette mesure. Il doit donc être écarté dans cette mesure seule, ce qui n'est pas susceptible de priver de garanties effectives les exigences constitutionnelles mentionnées au point 9, et les décrets attaqués doivent être annulés en tant seulement qu'ils permettent la mise en œuvre de traitements automatisés sans prévoir un tel contrôle avant l'identification des personnes dont les données sont susceptibles de révéler une menace à caractère terroriste.

S'agissant du recueil en temps réel des données de trafic et de localisation prévu aux articles L. 851-2 et L. 851-4 du code de la sécurité intérieure :

78. Par son arrêt du 6 octobre 2020 précité, la Cour de justice de l'Union européenne a dit pour droit que : « *L'article 15, paragraphe 1, de la*

directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir (...) au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque (...) - le recours à un recueil en temps réel des données relatives au trafic et des données de localisation est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme et est soumis à un contrôle préalable, effectué, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais ».

Quant à l'article L. 851-2 du code de la sécurité intérieure :

79. Dans sa rédaction applicable au litige, l'article L. 851-2 du code de la sécurité intérieure dispose que : « *I.- Dans les conditions prévues au chapitre I^er^ du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée comme présentant une menace. / II.- Par dérogation à l'article L.821-4, l'autorisation est délivrée pour une durée de deux mois, renouvelable dans les mêmes conditions de durée* ».

80. Il résulte de ce que la Cour a dit pour droit, et qui a été rappelé au point 78 de la présente décision, que le droit de l'Union européenne autorise le recueil en temps réel des données de trafic et de localisation lorsque celui-ci est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une

autre dans des activités de terrorisme. Il s'ensuit que la technique définie à l'article L. 851-2 du code de la sécurité intérieure, dans sa rédaction applicable à la date des décrets contestés, n'est pas contraire, dans son principe, aux dispositions de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 et de l'article 23 du RGPD telles qu'interprétées par la Cour de justice de l'Union européenne. En revanche, le recueil en temps réel des données de trafic et de localisation doit être soumis au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante dont la décision est dotée d'un effet contraignant. Or, d'une part, les avis que rend la Commission nationale de contrôle des techniques de renseignement ne sont pas contraignants et, d'autre part, l'article L. 833-8 du code de la sécurité intérieure ne prévoit pas de saisine systématique du Conseil d'État lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission. Il s'ensuit que l'article L. 851-2 du code de la sécurité intérieure méconnaît les dispositions de la directive en tant qu'il ne prévoit pas de contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction. Il doit donc être écarté dans cette mesure seule et les décrets attaqués doivent être annulés en tant seulement qu'ils permettent la mise en œuvre du recueil en temps réel des données de trafic et de localisation sans prévoir un tel contrôle. La mise à l'écart du droit national par le juge dans cette mesure n'est pas de nature à priver de garanties effectives les objectifs de valeur constitutionnelle cités au point 9.

Quant à l'article L. 851-4 du code de la sécurité intérieure :

81. Dans sa rédaction applicable au litige, l'article L. 851-4 du code de la sécurité intérieure dispose que : « *Dans les conditions prévues au chapitre Ier du titre II du présent livre, les données techniques relatives à la localisation des équipements terminaux utilisés mentionnées à l'article L. 851-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs à un service du Premier ministre* ».

82. Il résulte de ce que la Cour a dit pour droit et qui a été rappelé au point 78 que l'article 15 de la directive du 12 juillet 2002 autorise le recueil en temps réel des données de localisation pour la prévention du terrorisme. Toutefois, il ne ressort pas de l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2020 que la directive interdirait

le recours à cette méthode de renseignement pour la défense et la promotion des autres intérêts fondamentaux de la Nation définis à l'article L. 811-3 du code de la sécurité intérieure, dans le respect du principe de proportionnalité des atteintes à la vie privée rappelé à l'article L. 801-1 du code. Il s'ensuit que les associations requérantes ne sont pas fondées à soutenir que l'article L. 851-4 du code de la sécurité intérieure méconnaîtrait le droit de l'Union européenne en tant qu'il poursuivrait des finalités trop larges.

83. En revanche, et pour les mêmes motifs que ceux précisés au point 80 de la présente décision, l'article L. 851-4 du code de la sécurité intérieure méconnaît les dispositions de la directive en tant qu'il ne prévoit pas de contrôle préalable du recueil en temps réel des données de localisation par une autorité administrative indépendante dotée d'un pouvoir contraignant ou une juridiction. Il doit donc être écarté dans cette seule mesure, ce qui n'est pas susceptible de priver de garanties effectives les exigences constitutionnelles mentionnées au point 9, et les décrets attaqués doivent être annulés en tant seulement qu'ils permettent sa mise en œuvre sans prévoir un tel contrôle.

En ce qui concerne les moyens tirés de ce que les techniques du livre VIII du code de la sécurité intérieure seraient entourées de garanties procédurales insuffisantes :

S'agissant du moyen tiré de ce que les dispositions attaquées organisent l'accès aux données des personnes dont les communications sont soumises au secret professionnel, conservées en méconnaissance du droit de l'Union :

84. D'une part, il découle clairement de l'article 15 de la directive du 12 juillet 2002 que le droit de l'Union européenne ne s'oppose pas à ce que les données de connexion des personnes dont les communications sont soumises au secret professionnel fassent l'objet d'une obligation de conservation en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale. Il résulte de l'état de la menace rappelé aux points 44 et 66 que le pouvoir réglementaire pouvait légalement imposer aux opérateurs cités aux articles L. 34-1 du code des postes et des communications et 6 de la loi du 21 juin 2004 de conserver les données de trafic et de localisation de ces personnes.

85. D'autre part, les requérants soutiennent que les articles L. 851-1 à L. 851-4 du code de la sécurité intérieure méconnaissent le droit de l'Union européenne faute de prévoir des garanties légales pour le traitement des données de connexion des personnes dont les communications sont soumises au secret professionnel. Or, l'article L. 821-7 du code de la sécurité intérieure dispose, dans sa rédaction applicable au litige, que : « *Un parlementaire, un magistrat, un avocat ou un journaliste ne peut être l'objet d'une demande de mise en œuvre, sur le territoire national, d'une technique de recueil de renseignement mentionnée au titre V du présent livre à raison de l'exercice de son mandat ou de sa profession. Lorsqu'une telle demande concerne l'une de ces personnes ou ses véhicules, ses bureaux ou ses domiciles, l'avis de la Commission nationale de contrôle des techniques de renseignement est examiné en formation plénière. L'article L. 821-5 n'est pas applicable. (...) Les transcriptions des renseignements collectés en application du présent article sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats* ». Il s'ensuit que le moyen invoqué à ce titre manque en fait.

S'agissant des personnes susceptibles d'accéder aux données de trafic et de localisation :

86. Aux termes de l'article L. 811-4 du code de la sécurité intérieure : « *Un décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement, désigne les services, autres que les services spécialisés de renseignement, relevant des ministres de la défense, de l'intérieur et de la justice ainsi que des ministres chargés de l'économie, du budget ou des douanes, qui peuvent être autorisés à recourir aux techniques mentionnées au titre V du présent livre dans les conditions prévues au même livre. Il précise, pour chaque service, les finalités mentionnées à l'article L. 811-3 et les techniques qui peuvent donner lieu à autorisation* ». Les associations requérantes soutiennent qu'en ne limitant pas le nombre de personnes pouvant accéder aux données de connexion et les exploiter, ces dispositions méconnaissent les droits au respect de la vie privée et familiale et à la protection des données à caractère

personnel respectivement protégés par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

87. Dans son arrêt du 8 avril 2014, Digital Rights Ireland Ltd (C-293/12 et C-594/12), la Cour de justice de l'Union européenne a dit pour droit que la directive 2006/24/CE du Parlement et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE était invalide, au motif notamment qu'elle ne prévoyait « *aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi* ».

88. En premier lieu, le décret du 11 décembre 2015 attaqué énumère limitativement, par technique de renseignement et par finalité poursuivie, les services autorisés à recourir aux techniques du titre V du livre VIII de la partie législative du code de la sécurité intérieure. Le décret du 29 janvier 2016 également attaqué insère quant à lui au code de la sécurité intérieure un article R.821-1 qui dispose que : « *Seuls peuvent mettre en œuvre les techniques de recueil de renseignement mentionnées au titre V du présent livre les agents individuellement désignés et habilités par le ministre ou, par délégation, par le directeur dont ils relèvent* ». De même, s'agissant plus précisément des méthodes de renseignement prévues par les articles L. 851-1, L. 851-2 et L. 851-4 du code, les articles R. 851-1, R. 851-1-1 et R. 851-2 du code issus des décrets attaqués prévoient également que seuls les agents individuellement désignés et habilités peuvent y recourir. Il résulte enfin du principe de proportionnalité, rappelé à l'article L. 801-1 du code, que le nombre des agents habilités ne saurait excéder celui nécessaire à l'exercice de ces activités.

89. En second lieu, il appartient au juge administratif, lorsqu'il est saisi d'un moyen en ce sens, de vérifier que l'accès aux données de connexion des personnes énumérées par les décrets pris pour l'application de l'article L. 811-4 et des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure est limité au strict nécessaire au regard des finalités poursuivies. Il s'ensuit que le moyen tiré de ce que ce décret méconnaîtrait les articles

7 et 8 de la Charte des droits fondamentaux de l'Union européenne au motif qu'il ne limiterait pas le nombre de personnes pouvant accéder aux données de connexion et les exploiter doit être écarté.

S'agissant de l'information des personnes ayant fait l'objet d'une technique de renseignement :

90. Au point 190 de son arrêt du 6 octobre 2020 précité, la Cour de justice de l'Union européenne précise qu'il « *importe que les autorités nationales compétentes procédant au recueil en temps réel des données relatives au trafic et des données de localisation en informent les personnes concernées, dans le cadre des procédures nationales applicables, pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent à ces autorités* ».

91. L'article 32 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose, dans sa version applicable au litige que : « *I. - La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant : 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ; / 2° De la finalité poursuivie par le traitement auquel les données sont destinées (...) V. - Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement* ». Il résulte de ces dispositions que l'obligation d'information des personnes prévue par le I de cet article ne s'applique pas aux traitements mentionnés au V lorsqu'une telle limitation est nécessaire au respect des finalités poursuivies par ces traitements. En revanche, cette information est garantie dès lors qu'elle n'est plus susceptible de compromettre le respect des fins poursuivies par ces mêmes traitements. Ces dispositions doivent être regardées comme prévoyant, le cas échéant, l'information des personnes ayant fait l'objet d'un traitement de leurs données

personnelles dans le cadre d'une des techniques de renseignement mentionnées aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent aux services de renseignement, ainsi que l'exige la Cour de justice de l'Union européenne dans les motifs de son arrêt rappelés au point précédent. Il s'ensuit que les associations requérantes ne sont pas fondées à soutenir que les décrets attaqués méconnaîtraient le droit de l'Union, faute de prévoir une telle communication.

S'agissant des moyens dirigés contre des dispositions du code de la sécurité intérieure qui ne relèvent pas du champ de la directive du 12 juillet 2002 :

Quant à la durée de conservation des données recueillies sur le fondement de l'article L. 851-1 par les services de renseignement :

92. Les associations requérantes soutiennent que l'article L. 822-2 du code de la sécurité intérieure méconnaît la directive du 12 juillet 2002 en tant que la durée de conservation des données collectées par les services de renseignement sur le fondement de l'article L. 851-1 qu'il prévoit est excessive. L'article R. 851-6 inséré au code de la sécurité intérieure par le décret du 29 janvier 2016 attaqué dispose que : « *II. - Le groupement interministériel de contrôle enregistre et conserve dans les mêmes conditions de durée que celles prévues à l'article L. 822-2 pour les renseignements collectés, dans un traitement automatisé qu'il met en œuvre, les demandes tendant au recueil mentionné à l'article L. 851-1 ainsi que les décisions du Premier ministre ou de ses délégués relatives à ces demandes* ». Aux termes de l'article L. 822-2 du code de la sécurité intérieure dans sa rédaction applicable au litige : « *I. - Les renseignements collectés par la mise en œuvre d'une technique de recueil de renseignement autorisée en application du chapitre I^er du présent titre sont détruits à l'issue d'une durée de : (...) 3° Quatre ans à compter de leur recueil pour les informations ou documents mentionnés à l'article L. 851-1. / Pour ceux des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement. Ils ne peuvent être conservés plus de six ans à compter de leur recueil. / Dans une mesure strictement nécessaire aux besoins de l'analyse technique et à l'exclusion de toute utilisation pour la surveillance des personnes*

concernées, les renseignements collectés qui contiennent des éléments de cyberattaque ou qui sont chiffrés, ainsi que les renseignements déchiffrés associés à ces derniers, peuvent être conservés au-delà des durées mentionnées au présent I ».

93. En vertu de son article 1er, paragraphe 3, la directive du 12 juillet 2002 « *ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne (...) et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal* ». Il en résulte clairement que les dispositions de l'article L. 822-2 du code de la sécurité intérieure ne relèvent pas du champ d'application de cette directive dès lors qu'elles fixent la durée pendant laquelle les services de renseignement peuvent conserver les données collectées sur le fondement de l'article L. 851-1 du même code, sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Ces dispositions ne sauraient donc être regardées comme mettant en œuvre le droit de l'Union européenne et, par suite, les moyens tirés de la méconnaissance de la directive du 12 juillet 2002 interprétée à la lumière de la Charte des droits fondamentaux de l'Union européenne ne peuvent être utilement invoqués à leur encontre.

Quant au moyen tiré de l'insuffisance du contrôle de l'exploitation des données collectées par les services de renseignement et de celui de la collecte et de l'exploitation des données transmises par des services étrangers :

94. Les associations requérantes soutiennent qu'en ne prévoyant pas de contrôle de l'exploitation des données collectées par les services de renseignement sur le fondement du livre VIII du code de la sécurité intérieure, d'une part, ni de contrôle de la conservation et de l'exploitation des données qui leur sont transmises par des services étrangers, d'autre part, les dispositions contestées méconnaissent le droit de l'Union européenne. Toutefois, il résulte clairement de l'article 1er, paragraphe 3 de la directive cité au point précédent que ni les règles relatives à l'exploitation par les services de renseignement

des données collectées auprès des opérateurs ni celles relatives à la collecte et à l'exploitation par eux de données transmises par des services de renseignement étrangers ne régissent l'activité des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Il s'ensuit que ces règles ne sauraient être regardées comme mettant en œuvre le droit de l'Union européenne et que le moyen soulevé ne peut être utilement invoqué à l'encontre des dispositions attaquées.

Quant aux moyens tirés de l'inconventionnalité de l'article L. 854-1 du code de la sécurité intérieure :

95. Les associations requérantes soutiennent à nouveau que l'article L.854-1 du code de la sécurité intérieure méconnaît le droit de l'Union européenne. Toutefois, ainsi que l'a jugé le Conseil d'État, statuant au contentieux, au point 21 de sa décision n° 394922 et autres du 26 juillet 2018, ces dispositions ne sauraient être regardées comme mettant en œuvre le droit de l'Union européenne et, par suite, les moyens tirés de la méconnaissance de la directive du 12 juillet 2002 interprétée à la lumière de la Charte des droits fondamentaux de l'Union européenne ne peuvent être utilement invoqués à leur encontre.

En ce qui concerne les conséquences des illégalités affectant les décrets du 11 décembre 2015 et du 29 janvier 2016 :

96. Ainsi qu'il a été rappelé au point 66, la France était confrontée, à la date de publication des décrets attaqués, à une menace grave, réelle et actuelle pour sa sécurité nationale. Il ressort en outre des pièces du dossier que cette menace, dont les contours sont rappelés aux points 44 et 66, s'est maintenue à un niveau élevé entre cette date et celle de la présente décision. Il s'ensuit que, tout au long de cette période, le Gouvernement pouvait légalement imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenu, la conservation généralisée et indifférenciée des données de trafic et de localisation aux fins de sauvegarde de la sécurité nationale.

97. Comme précisé aux points 74, 77, 80 et 83 de la présente décision, les articles L. 851-1, L. 851-2, L. 851-4 et le IV de l'article L. 851-3 méconnaissent le droit de l'Union européenne, faute pour la Commission nationale de contrôle des techniques de renseignement de disposer d'un pouvoir d'avis conforme. L'annulation des décrets attaqués en tant qu'ils permettent l'application de ces dispositions sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiée, ne saurait toutefois avoir pour conséquence d'entacher d'illégalité, pour le passé, l'usage par les services de renseignement des techniques prévues par ces articles que dans les hypothèses où le Premier ministre les aurait mises en œuvre, en dehors des cas d'urgence dûment justifiée, malgré un avis défavorable de la commission. Or, il ressort des rapports publics de la commission que l'avis rendu par celle-ci préalablement à la mise en œuvre de ces techniques de renseignement, bien qu'étant dépourvu d'effet contraignant, a été, dans les faits, systématiquement suivi par le Premier ministre. Il suit de là que l'annulation rétroactive des décrets attaqués, qui n'impliquerait par elle-même la suppression d'aucune donnée recueillie par les services de renseignement sur leur fondement, n'emporterait pas de conséquences manifestement excessives pas plus qu'elle ne priverait de garanties effectives les exigences constitutionnelles mentionnées au point 9.

98. Par ailleurs, l'annulation des décrets attaqués, compte tenu de sa portée, implique seulement, dans l'attente de l'intervention des textes nécessaires à la mise en conformité des dispositions du droit national avec le droit de l'Union européenne, qu'en cas d'avis défavorable de la Commission nationale de contrôle des techniques de renseignement, le Premier ministre ne pourra légalement autoriser la mise en œuvre des techniques de renseignement mentionnées aux articles L. 851-1, L. 851-2, L. 851-4 et au IV de l'article L. 851-3 avant l'intervention de la décision du Conseil d'État, qu'il appartiendra alors à la commission de saisir en application de l'article L. 833-8 du même code. Dans ces conditions, il n'y a pas lieu de différer dans le temps les effets de l'annulation ainsi prononcée.

IV. Sur les conclusions tendant à l'application des dispositions de l'article L.761-1 du code de justice administrative :

99. Il y a lieu de mettre à la charge de l'État la somme de 3 000 euros à verser à chacune des associations requérantes ainsi que la somme de 1 500 euros à verser aux sociétés Free Mobile et Free au titre de l'article L. 761-1 du code de justice administrative.

D E C I D E :

Article 1er : Sont annulées les décisions du Premier ministre refusant d'abroger l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, en tant que ces dispositions réglementaires, d'une part, ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation autres que les données d'identité civile, les coordonnées de contact et de paiement, les données relatives aux contrats et aux comptes et les adresses IP à la sauvegarde de la sécurité nationale et, d'autre part, ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

Article 2 : Il est enjoint au Premier ministre de procéder à cette abrogation dans un délai de six mois à compter de la présente décision.

Article 3 : Les décrets du 11 décembre 2015 et du 29 janvier 2016 sont annulés en tant seulement qu'ils permettent la mise en œuvre des dispositions des articles L. 851-1, L. 851-2, L. 851-4 et du IV de l'article L. 851-3 du code de la sécurité intérieure sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiée.

Article 4 : La requête n° 394922 est rejetée.

Article 5 : L'État versera la somme de 3 000 euros à l'association La Quadrature du Net, 3 000 euros à l'association French Data Network, 3 000 euros à la Fédération des fournisseurs d'accès à internet associatifs, 3 000 euros à l'association Igwan.net, 1 500 euros à la société Free Mobile et 1 500 euros à la société Free au titre de l'article L. 761-1 du code de justice administrative.

Article 6 : Le surplus des conclusions des requêtes est rejeté.

Article 7 : La présente décision sera notifiée aux associations La Quadrature du Net, French Data Network, Igwan.net, à la Fédération des fournisseurs d'accès à internet associatifs, à la société Free Mobile, à la société Free, au Premier ministre, au ministre de l'économie, des finances et de la relance, à la ministre des armées, au ministre de l'intérieur, au garde des sceaux, ministre de la justice, à Privacy International et au Center for Democracy and Technology.

Copie en sera adressée à la Fédération française des télécoms.

Annexe n° 6

Délibération de la CNCTR n° 4/2021 du 4 février 2021

Saisie pour avis le 11 janvier 2021, puis le 19 janvier 2021, par le ministre de l'intérieur[113] d'un projet de décret en Conseil d'État modifiant diverses dispositions du code de la sécurité intérieure, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

I. Remarques de portée générale

Le projet de décret est pris pour l'application de l'article L. 811-4 du code de la sécurité intérieure, qui prévoit que les services dits du « second cercle », c'est-à-dire autres que les services spécialisés de renseignement, peuvent être autorisés à recourir aux techniques mentionnées au titre V du livre VIII du même code lorsqu'ils sont désignés à cet effet par décret en Conseil d'État pris après avis de la CNCTR. Ce décret doit préciser les techniques auxquelles les services peuvent recourir ainsi que les finalités qui peuvent donner lieu à autorisations.

La CNCTR a déjà rendu six avis[114] sur des projets de décret en Conseil d'État pris pour l'application de l'article L. 811-4 du code de la sécurité intérieure. Elle rappelle, à titre liminaire, certaines observations et recommandations de portée générale formulées dans ces avis.

a) L'article L.801-1 du code de la sécurité intérieure prévoit qu'il ne peut être porté atteinte au respect de la vie privée, dans toutes ses composantes,

113 - Voir le courrier du 8 janvier 2021, reçu le 11 janvier suivant, adressé au président de la CNCTR par le directeur des libertés publiques et des affaires juridiques du ministère de l'intérieur, complété par le courrier n° 2076 du 18 janvier 2021, reçu le 19 janvier suivant.

114 - Il s'agit des délibérations n° 2/2015 du 12 novembre 2015, n° 3/2016 du 8 décembre 2016, n° 5/2017 du 7 décembre 2017, n°2/2018 du 17 mai 2018, n° 1/2019 du 2 mai 2019 et n° 5/2019 du 7 novembre 2019. Ces délibérations sont publiées sur le site internet de la commission.

que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité. Il impose ainsi que la capacité de mettre en œuvre des techniques de renseignement soit strictement et précisément limitée aux services qui ont légalement pour mission de mener des actions de prévention relevant de la police administrative et justifient d'un besoin avéré d'y recourir.

La CNCTR en déduit que la nature des techniques auxquelles peuvent avoir accès les services du « second cercle » dépend de la part qu'occupe le renseignement au sein de leurs missions ainsi que de l'expertise technique requise pour mettre en œuvre les techniques de manière sûre.

b) La CNCTR estime, par ailleurs, que les termes de l'article L. 811-4 du code de la sécurité intérieure permettent au service du « second cercle » demandeur soit de mettre en œuvre lui même la technique, s'il en a la capacité, soit de faire réaliser l'opération par un opérateur technique, qui ne pourra pas, en revanche, participer à l'exploitation des renseignements collectés.

c) La CNCTR rappelle, enfin, que l'exercice effectif de la mission de contrôle qui lui a été confiée par la loi nécessite qu'elle puisse, outre le contrôle *a priori* sur les demandes tendant à mettre en œuvre une technique, mener à bien un contrôle *a posteriori* sur cette mise en œuvre et notamment sur les données recueillies. Ceci impose une centralisation de ces données, auxquelles la CNCTR doit avoir un accès permanent, complet et direct, conformément à l'article L. 833-2 du code de la sécurité intérieure. Pour les services du « second cercle », cette centralisation doit, du point de vue de la commission, être réalisée de préférence par le groupement interministériel de contrôle (GIC).

II. Observations détaillées

Le ministre de l'intérieur indique que le projet de décret tend, d'une part, à adapter les dispositions réglementaires du code de la sécurité intérieure aux évolutions de certaines formes de criminalité et, d'autre part, à prendre en considération la réforme des services territoriaux de la direction centrale de la police judiciaire ainsi que plusieurs réorganisations internes intervenues dans d'autres services de la préfecture de police.

Dans un souci de clarté de son avis, la CNCTR livrera ses commentaires pour chaque service concerné, en distinguant ceux qui relèvent de la direction centrale de la police judiciaire (DCPJ) et ceux qui relèvent de la préfecture de police de Paris (PP).

1. Les modifications affectant les services de la direction centrale de la police judiciaire (DCPJ)

1.1 La prise en considération de la réforme des services territoriaux de la DCPJ

Le ministre de l'intérieur indique que le projet de décret a pour but de tirer les conséquences de la nouvelle organisation territoriale de la DCPJ résultant du décret n° 2020 1776 du 30 décembre 2020 portant organisation des services territoriaux de police judiciaire de la police nationale.

La réforme de l'organisation territoriale de la DCPJ conduit à remplacer :

- les directions interrégionales ou régionales de police judiciaire (DIPJ et DRPJ) par des directions zonales de police judiciaire (DZPJ)[115] ;
- les services régionaux de police judiciaire (SRPJ) par des directions territoriales de police judiciaire (DTPJ) ;
- les antennes de police judiciaire (APJ) par des services de police judiciaire (SPJ) ;

La CNCTR relève, d'une part, que les nouvelles structures territoriales poursuivent les mêmes missions que celles qu'elles ont remplacées. D'autre part, plus de cinq ans après l'entrée en vigueur du décret du 12 décembre 2015[116] permettant aux services territoriaux de la DCPJ de mettre en œuvre des techniques de renseignement, aucun élément ne conduit la commission à recommander de restreindre leurs compétences en la matière.

115 - A l'exception de la DRPJ Versailles qui conserve sa dénomination actuelle.

116 - Il s'agit du décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 dudit code. Les dispositions de ce décret sont codifiées dans la partie réglementaire du livre VIII du code de la sécurité intérieure.

La CNCTR émet donc un avis favorable à ce que les nouveaux échelons territoriaux de la DCPJ aient accès aux mêmes techniques de renseignement et pour les mêmes finalités que les services qu'ils ont remplacés.

1.2 L'attribution de nouvelles techniques de renseignement à certains échelons territoriaux de la DCPJ

a) L'autorisation de recourir à la technique de recueil de données de connexion par *IMSI catcher* (L. 851-6 du code de la sécurité intérieure) au bénéfice des SPJ

En l'état du droit, seuls les DIPJ/DRPJ et les SRPJ, respectivement remplacés par les DZPJ et DTPJ, peuvent être autorisés à mettre en œuvre la technique de recueil de données de connexion par *IMSI catcher* prévue par l'article L. 851-6 du code de la sécurité intérieure, au titre des finalités de prévention du terrorisme et de prévention de la criminalité et de la délinquance organisées.

L'article 7 du projet de décret prévoit d'ouvrir le recours à cette technique aux nouveaux SPJ (qui remplacent les APJ), au titre de ces deux finalités.

La CNCTR relève, en premier lieu, que les SPJ ont les mêmes attributions que les DZPJ et les DTPJ en matière de prévention du terrorisme et de lutte contre la criminalité et la délinquance organisées. Ils traitent d'affaires de même importance et assurent le suivi de cibles présentant le même degré de sensibilité. Ainsi, leurs besoins opérationnels sont identiques à ceux des autres échelons territoriaux.

La CNCTR constate, en deuxième lieu, que les services territoriaux de la DCPJ font un usage modéré de la technique de recueil de données de connexion par *IMSI catcher*, dont la mise en œuvre est systématiquement réalisée avec le concours du service interministériel d'assistance technique (SIAT). En tout état de cause, cette technique est soumise à un contingentement en application duquel le nombre total d'appareils ou de dispositifs techniques pouvant être utilisés simultanément est limité.

La CNCTR rappelle, en troisième lieu, qu'elle n'avait établi aucune distinction entre les échelons territoriaux de la DPCJ dans sa délibération

n° 2/2015 du 12 novembre 2015[117] et avait émis un avis favorable à ce qu'ils puissent, dans leur ensemble, être autorisés à recourir à la technique de recueil de données de connexion par *IMSI catcher*, sous réserve que la mise en œuvre soit réalisée avec le concours du SIAT.

La CNCTR estime, enfin, au vu des contrôles qu'elle effectue depuis plus de cinq ans, que l'ensemble des services relevant de la DCPJ justifient d'une bonne maîtrise du cadre légal et utilisent les techniques de renseignement avec rigueur et modération. En outre, les procédures internes à la DCPJ fiabilisent la mise en œuvre des techniques de renseignement.

La CNCTR émet, en conséquence, un avis favorable à ce que les SPJ puissent être autorisés à recourir à la technique de recueil de données de connexion par *IMSI catcher*, sous réserve que sa mise en œuvre soit réalisée avec le concours du SIAT.

b) L'autorisation de recourir à la technique d'introduction dans un lieu privé (ILP) ne constituant pas un lieu d'habitation au bénéfice des DTPJ et des SPJ, pour mettre en œuvre les techniques de captation de paroles ou d'images

Tous les échelons territoriaux de la DCPJ sont autorisés à recourir aux techniques de captation de paroles prononcées à titre privé et de captation d'images dans un lieu privé prévues par l'article L. 853-1 du code de la sécurité intérieure, au titre des finalités de prévention du terrorisme et de lutte contre la criminalité et la délinquance organisées. Mais seules les DIPJ/DRPJ sont autorisées à solliciter l'autorisation de s'introduire dans un lieu privé ne constituant pas un lieu d'habitation, prévue par l'article L. 853-3 du code de la sécurité intérieure, pour y mettre en œuvre ces deux techniques.

L'article 14 du projet de décret prévoit d'étendre la possibilité d'introduction dans des lieux privés ne constituant pas des lieux d'habitation aux DTPJ et SPJ. Le ministre de l'intérieur précise que ces services bénéficieraient du concours du SIAT pour mettre en œuvre les techniques.

117 - Cette délibération a été rendue sur le projet de décret du 11 décembre 2015 cité ci-dessus.

La CNCTR constate que l'autorisation d'introduction dans un lieu privé ne constitue pas en elle-même une technique de renseignement autonome. Elle n'est que l'accessoire d'autres techniques expressément énumérées par l'article L. 853-3 du code de la sécurité intérieure et ne peut être utilisée qu'à des fins précises, dans le respect du principe de subsidiarité. Ainsi, elle ne peut servir qu'à mettre en place, utiliser ou retirer les dispositifs techniques mentionnés aux articles L. 851-5, L. 853-1 et L. 853-2 du code de la sécurité intérieure, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé.

Puisque les DTPJ et les SPJ sont, comme les DZPJ/DRPJ, autorisés à utiliser des dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans des lieux privés ne constituant pas des lieux d'habitation, ils doivent également être autorisés à les mettre en place et les retirer dans de tels lieux.

La CNCTR émet un avis favorable à ce que les DTPJ et les SPJ puissent être autorisés à recourir à la technique d'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en œuvre les techniques de captation de paroles ou d'images, sous réserve que la mise en œuvre soit réalisée avec le concours du SIAT.

c) L'autorisation de recourir à la technique d'interception de correspondances échangées par voie hertzienne (article L. 852-2 du code de la sécurité intérieure) au bénéfice de l'Office antistupéfiants (OFAST)

Créé par le décret n° 2019-1457 du 26 décembre 2019, l'OFAST a succédé, au 1er janvier 2020, à l'office central pour la répression du trafic illicite des stupéfiants (OCRTIS).

En application du décret n° 2019-1496 du 28 décembre 2019, pris selon les recommandations émises par la CNCTR dans sa délibération n° 5/2019 du 7 novembre 2019, l'OFAST a été autorisé à recourir, au seul titre de la prévention de la criminalité et de la délinquance organisées, aux techniques de renseignement suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- le recueil de données de connexion par IMSI catcher (article L. 851-6 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le groupement interministériel de contrôle (I de l'article L. 852-1 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou un dispositif de captation d'images.

L'article 10 du projet de décret prévoit d'ouvrir à l'OFAST le recours à la technique d'interception de sécurité effectuée sur des réseaux exclusivement hertziens, prévue par l'article L. 852-2 du code de la sécurité intérieure, au seul titre de la finalité de prévention de la criminalité et de la délinquance organisées.

Comme le souligne le ministre de l'intérieur, l'OCRTIS était autorisé à recourir à cette technique au titre de la même finalité. L'OFAST, qui l'a remplacé, devrait également y avoir accès.

La CNCTR émet donc un avis favorable à ce que l'OFAST puisse être autorisé à recourir à la technique prévue par l'article L. 852-2 du code de la sécurité intérieure, au seul titre de la finalité de prévention de la criminalité et de la délinquance organisées.

2. Les modifications affectant les services relevant de la préfecture de police de Paris (PP)

2.1 La prise en compte d'adaptations intervenues au sein de plusieurs directions de la préfecture de police

a) La suppression de la référence au centre opérationnel des ressources techniques (CORT), consécutive à la transformation de la direction opérationnelle des services techniques et logistiques (DOSTL)

L'article L. 811-4 du code de la sécurité intérieure permet à un service du « second cercle » soit de mettre en œuvre lui même la technique, s'il en a la capacité, soit de faire réaliser l'opération par un opérateur technique qui ne pourra pas, en revanche, participer à l'exploitation des renseignements collectés.

Au sein de la préfecture de police, la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP) peut actuellement bénéficier, selon les techniques de renseignement concernées, soit de l'appui technique du centre opérationnel des ressources techniques (CORT) de la direction opérationnelle des services techniques et logistiques (DOSTL), soit de l'appui technique de la cellule d'assistance technique (CAT) de l'état-major de la direction régionale de la police judiciaire (DRPJ) de Paris.

Dans le cadre de la démarche de modernisation entreprise à la préfecture de police, la direction de l'innovation, de la logistique et des technologies (DILT) a succédé à la DOSTL à compter du 1er octobre 2020. Cette transformation a entraîné le rattachement du CORT de la DOSTL à la DRPJ de Paris et son intégration à la cellule d'assistance technique (CAT) de cette direction.

La CAT devient ainsi le seul service susceptible d'apporter son concours à la mise en œuvre de techniques de renseignement au bénéfice de la DRPJ comme de la DSPAP. En conséquence, la mention des agents du CORT dans les articles réglementaires du code de la sécurité intérieure concernés doit être remplacée par celle des agents de la CAT.

La CNCTR prend acte de cette adaptation qui procède, à droit constant, à une simplification du régime applicable en matière d'assistance technique pour la mise en œuvre des techniques de renseignement au sein de la préfecture de police.

b) La suppression de la référence aux deux sous-directions de la sécurité intérieure et du renseignement territorial de la direction du renseignement de la préfecture de police (DRPP), consécutive à la classification de l'organigramme de cette direction

Le ministre de l'intérieur indique que la classification, au niveau « confidentiel défense », de l'arrêté d'organisation de la DRPP implique de ne plus faire apparaître la mention des sous directions de cette direction dans la partie réglementaire du code de la sécurité intérieure.

Les services autorisés à recourir aux techniques de renseignement sont désormais désignés comme ceux « *chargés des missions de sécurité intérieure* » et/ou ceux *« chargés des missions de renseignement territorial* ».

Ces modifications, opérées à droit constant, n'appellent aucune observation de la part de la CNCTR.

2.2 L'accès à de nouvelles techniques de renseignement ou à de nouvelles finalités pour plusieurs services de la direction régionale de la police judiciaire (DRPJ) de Paris

a) L'autorisation de recourir à la technique d'interception de correspondances échangées par voie hertzienne (article L. 852-2 du code de la sécurité intérieure) au bénéfice de plusieurs brigades de la DRPJ

La direction de la police judiciaire de la préfecture de police (PPPJ), qui constitue la direction régionale de la police judiciaire (DRPJ) de Paris, comporte quatre sous-directions parmi lesquelles la sous-direction des brigades centrales (SDBC) et la sous-direction des affaires économiques et financières (SDAEF). Ces deux sous-directions sont elles-mêmes organisées en sept brigades chacune.

Toutes les brigades de la SDBC[118] sont autorisées à recourir, au titre des finalités de prévention du terrorisme et de prévention de la criminalité et de la délinquance organisées, aux techniques de renseignement suivantes :

118 - Les sept brigades composant la SDBC sont les suivantes : brigade criminelle, brigade de répression du banditisme, brigade des stupéfiants, brigade de répression du proxénétisme, brigade de recherche et d'intervention, brigade de protection des mineurs et brigade de l'exécution des décisions de justice.

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le groupement interministériel de contrôle (I de l'article L. 852-1 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou un dispositif de captation d'images[119].

Les sept brigades de la SDAEF[120] sont autorisées à recourir aux mêmes techniques de renseignement, au titre de la finalité de prévention de la criminalité et de la délinquance organisées[121].

L'article 10 du projet de décret prévoit d'ouvrir le recours à la technique d'interception de correspondances échangées par voie hertzienne à

119 - En outre, la brigade criminelle (BC) est autorisée à mettre en œuvre, au seul titre de la finalité de prévention du terrorisme mentionnée, le recueil de données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure) et l'introduction dans un lieu à usage d'habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou d'images ou un dispositif de recueil ou de captation de données informatiques (article L. 853-2 du code de la sécurité intérieure). La brigade de recherche et d'intervention (BRI) est autorisée à mettre en œuvre, au seul titre de la finalité de prévention du terrorisme, le recueil de données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure) l'interception de sécurité par IMSI catcher (II de l'article L. 852-1 du code de la sécurité intérieure) et l'introduction dans un lieu à usage d'habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou d'images. La brigade de protection des mineurs (BPM) est quant à elle autorisée à mettre en œuvre, au seul titre de la finalité de prévention de la criminalité et de la délinquance organisées, les techniques d'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer un dispositif de recueil ou de captation de données informatiques.

120 - Les sept brigades composant la SDAEF sont les suivantes : brigade financière, brigade de répression de la délinquance astucieuse, brigade des fraudes aux moyens de paiement, brigade de répression de la délinquance économique, brigade de répression de la délinquance contre la personne, brigade d'enquêtes sur les fraudes aux technologies de l'information désormais dénommée « brigade de lutte contre la cybercriminalité » et brigade de recherches et d'investigations financières.

121 - La brigade de lutte contre la cybercriminalité (BLC) a, en outre, accès aux techniques d'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer un dispositif de recueil ou de captation de données informatiques (article L. 853-2 du code de la sécurité intérieure).

cinq brigades de la SDBC[122] et deux brigades de la SDAEF[123], au titre des finalités de prévention du terrorisme et de prévention de la criminalité et de la délinquance organisées.

Comme la CNCTR le soulignait dans sa délibération n° 2/2018 du 17 mai 2018 relative au projet de décret modifiant la partie réglementaire du code de la sécurité intérieure et relatif à la désignation des services autres que les services spécialisés de renseignement pouvant être autorisés à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure, les interceptions de sécurité prévues par cet article visent des correspondances échangées au sein de réseaux et au moyen de matériels spécifiques. Ces interceptions sont réalisées de manière décentralisée et nécessitent l'acquisition par les services de renseignement de dispositifs lourds et onéreux dont l'usage suppose des compétences techniques particulières, notamment pour positionner les dispositifs de manière adéquate et pour déterminer la fréquence à intercepter. En outre, le traitement des données recueillies se heurte à des contraintes techniques fortes. L'accès à la technique prévue par l'article L. 852-2 du code de la sécurité intérieure doit, en conséquence, être réservé aux services du « second cercle » ayant un besoin avéré d'y recourir et disposant de capacités opérationnelles adaptées.

À la lumière des constatations qu'elle a établies depuis plus de cinq ans, la CNCTR relève que seules la brigade de répression du banditisme (BRB), la brigade des stupéfiants (BSP) et la brigade de recherche et d'intervention (BRI) de la sous-direction des brigades centrales (SDBC) utilisent régulièrement les techniques de renseignement et justifient du besoin de recourir aux interceptions de sécurité hertziennes.

La CNCTR émet un avis favorable à ce que la brigade de répression du banditisme (BRB), la brigade des stupéfiants (BSP) et la brigade de recherche et d'intervention (BRI) de la sous-direction des brigades centrales (SDBC) puissent être autorisées à recourir, au seul titre de la finalité de prévention de la criminalité et de la

122 - Il s'agit des cinq brigades suivantes : brigade criminelle (BC), brigade de répression du banditisme (BRB), brigade des stupéfiants (BSP), brigade de répression du proxénétisme (BRP) et brigade de recherche et d'intervention (BRI).

123 - Il s'agit des deux brigades suivantes : brigade de recherches et d'investigations financières (BRIF) et brigade de lutte contre la cybercriminalité (BLC).

délinquance organisées, aux interceptions de correspondances échangées par voie hertzienne, sous réserve que leur mise en œuvre soit réalisée avec le concours du SIAT.

La commission émet, en revanche, en l'état des éléments dont elle dispose sur la réalité du besoin de recourir aux interceptions hertziennes, un avis défavorable concernant la brigade criminelle (BC) et la brigade de répression du proxénétisme (BRP) de cette même sous-direction ainsi que la brigade de recherches et d'investigations financières (BRIF) et la brigade de lutte contre la cybercriminalité (BLC) de la sous-direction des affaires économiques et financières (SDAEF). Au demeurant, le concours d'autres entités de la préfecture de police autorisées à mettre en œuvre cette technique pourrait être sollicité si un besoin opérationnel exceptionnel apparaissait.

b) L'accès à la finalité de prévention du terrorisme pour l'ensemble des brigades de la sous-direction des affaires économiques et financières (SDAEF)

Toutes les brigades de la SDAEF sont autorisées à recourir aux techniques de renseignement énumérées au point précédent, au titre de la finalité de prévention de la criminalité et de la délinquance organisées. Le projet de décret prévoit de les autoriser, en outre, à mettre en œuvre ces mêmes techniques au titre de la finalité de prévention du terrorisme.

Le ministre de l'intérieur fait valoir que l'arrêté d'organisation de la DRPJ en date du 2 juin 2020 a confié aux services de la SDAEF la mission supplémentaire de lutte contre « *les actes terroristes* » et que ces services apportent désormais, de manière presque systématique, leur concours actif aux enquêteurs antiterroristes et traitent de délinquances spécialisées susceptibles de contribuer au financement du terrorisme.

La CNCTR n'émet pas d'objection à ce que l'ensemble des brigades de la SDAEF aient accès à la finalité de prévention du terrorisme pour mettre en œuvre les techniques de renseignement auxquelles elles sont déjà autorisées à recourir au titre de la prévention de la criminalité et de la délinquance organisées.

c) L'accès à de nouvelles techniques de renseignement au bénéfice de la brigade de lutte contre la cybercriminalité (BLC) de la sous-direction des affaires économiques et financières (SDAEF)

La BLC, anciennement dénommée « brigade d'enquêtes sur les fraudes aux technologies de l'information », est l'une des sept brigades que compte la SDAEF.

Elle est, jusqu'à présent, autorisée à recourir, au seul titre de la finalité de prévention de la criminalité et de la délinquance organisées, aux techniques de renseignement suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
- le balisage (article L. 851-5 du code de la sécurité intérieure) ;
- le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le groupement interministériel de contrôle (I de l'article L. 852-1 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- le recueil ou la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure) ;
- l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise, un dispositif de captation de paroles ou d'images ainsi qu'un dispositif de recueil ou de captation de données informatiques.

Les articles 4 et 18 du projet prévoient d'ouvrir à cette brigade l'accès :

- au recueil de données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure) ;

- et à l'introduction dans un lieu à usage d'habitation pour y mettre en place ou retirer un dispositif de recueil de données informatiques (1° du I de l'article L. 853-2 du code de la sécurité intérieure).

Le ministre de l'intérieur fait valoir que les particularités de la cybercriminalité nécessitent de recourir à des techniques de renseignement plus intrusives et plus sophistiquées.

La CNCTR constate, en premier lieu, que la demande d'accès à la technique de recueil de données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure), réservée à la prévention du terrorisme, n'est assortie d'aucun élément de motivation permettant d'en apprécier le bien-fondé. Au demeurant, la commission tire de l'expérience des contrôles qu'elle mène depuis plus de cinq ans que la mise en œuvre de cette technique requiert des capacités d'analyse technique poussées dont peu de services de renseignement disposent actuellement.

La CNCTR relève, en second lieu, que la BLC n'a, jusqu'ici, sollicité aucune autorisation de mise en œuvre des techniques de captation ou de recueil de données informatiques dans un lieu privé ne constituant pas un lieu d'habitation alors que celles-ci lui sont ouvertes, au titre de la prévention de la criminalité et de la délinquance organisées, depuis 2015. Le besoin d'extension des compétences de la BLC pour mettre en œuvre ces techniques dans un lieu d'habitation n'est en rien démontré.

Comme cela a été rappelé dans les remarques de portée générale de la présente délibération, l'article L.801-1 du code de la sécurité intérieure prévoit qu'il ne peut être porté atteinte au respect de la vie privée, dans toutes ses composantes, que dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans le respect du principe de proportionnalité. La capacité de mettre en œuvre des techniques de renseignement doit ainsi être strictement et précisément limitée aux services qui justifient d'un besoin avéré d'y recourir. En l'état des éléments portés à la connaissance de la commission, cette exigence n'apparaît pas satisfaite.

La CNCTR émet, en conséquence, en l'état des éléments dont elle dispose sur la réalité du besoin de recourir aux techniques en cause, un avis défavorable à ce que la brigade de lutte contre

la cybercriminalité (BLC) puisse y avoir accès. Cette brigade pourrait, au demeurant, solliciter le concours d'autres entités de la préfecture de police autorisées à mettre en œuvre les techniques de recueil de données de connexion en temps réel et d'introduction dans un lieu à usage d'habitation pour y mettre en place ou retirer un dispositif de recueil de données informatiques, si un besoin opérationnel exceptionnel apparaissait.

2.3 La désignation de la sûreté régionale des transports comme nouveau service de renseignement du « second cercle » autorisé à recourir aux techniques de renseignement

La sûreté régionale des transports (SRT) est un service de la sous-direction régionale de police des transports (SDRPT), laquelle fait partie de la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP) de la préfecture de police. Elle est chargée de lutter contre la délinquance dans les transports en commun d'Ile-de-France.

Seul le département criminalité organisée de la sous-direction spécialisée dans la lutte contre l'immigration irrégulière (SDLII) et les quatre sûretés territoriales (Paris, Hauts-de-Seine, Seine-Saint-Denis et Val-de-Marne) de la DSPAP sont autorisés à recourir, au titre de la finalité de prévention de la criminalité et de la délinquance organisées, à certaines techniques de renseignement[124].

Le projet de décret prévoit d'autoriser la sûreté territoriale des transports (SRT) à recourir à des techniques de renseignement[125], au titre de la même finalité de prévention de la criminalité et de la délinquance organisées.

124 - Il s'agit de l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ; de la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ; du balisage (article L. 851-5 du code de la sécurité intérieure) ; de l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le groupement interministériel de contrôle (I de l'article L. 852-1 du code de la sécurité intérieure) et de l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise. En outre, le département de criminalité organisée de la SDLII est autorisé à recourir aux dispositifs de captation de paroles prononcées à titre privé et de captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ainsi qu'à l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer ces dispositifs.

125 - Il s'agit de l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ; de la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ; du balisage (article L. 851-5 du code de la sécurité intérieure) ; de l'interception de sécurité exécutée auprès des opérateurs de communications électroniques par le groupement interministériel de contrôle (I de l'article L. 852-1 du code de la sécurité intérieure) et de l'introduction dans un lieu privé ne constituant pas un lieu d'habitation pour y mettre en place, utiliser ou retirer une balise.

La CNCTR rappelle, à titre liminaire, que la capacité de mettre en œuvre les techniques de renseignement prévues au titre V du livre VIII du code de la sécurité intérieure doit être strictement et précisément limitée aux services qui ont légalement pour mission de mener des actions de prévention relevant de la police administrative et qui justifient d'un besoin avéré d'y recourir.

La commission constate que la SRT est l'entité judiciaire de la brigade des réseaux franciliens (BRF). Au regard des éléments communiqués par le ministre de l'intérieur, il apparait que celle-ci intervient essentiellement sur saisine de l'autorité judiciaire ou à la suite de plaintes et assure le traitement des délits commis en flagrance. En revanche, elle ne semble pas mener de travail d'initiative. Elle a, en conséquence, une vocation essentiellement judiciaire. L'exercice d'une mission de prévention relevant de la police administrative n'est, en l'état des informations portées à la connaissance de la commission, pas démontré.

Dans ces conditions, et en l'état des éléments dont elle dispose sur la réalité du besoin, pour la sûreté régionale des transports, d'accéder à des techniques de renseignement, la CNCTR émet un avis défavorable à la désignation de cette entité comme nouveau service de renseignement du « second cercle » autorisé à mettre en œuvre de telles techniques. Si un besoin opérationnel exceptionnel apparaissait, d'autres services de la préfecture de police, habilités à recourir à certaines techniques de renseignement, seraient à même d'y répondre.

Annexe n° 7

Les modifications législatives du cadre juridique applicable aux techniques de renseignement en 2021

Le tableau ci-dessous résume les modifications de nature législative apportées au livre VIII du code de la sécurité intérieure et au livre II du code des postes et des communications électroniques par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

	Dispositions créées ou modifiées	Objet	Texte d'application
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 9 (Entrée en vigueur le 31 juillet 2021)	Article L. 822-3 du code de la sécurité intérieure	**Encadrement de l'exploitation et du partage de renseignements issus de la mise en œuvre de techniques de renseignement**	
	Article L. 822-4 du même code	**Traçabilité des transcriptions, extractions et transmissions de renseignements**	
	Article L. 833-2 du même code	**Accès permanent, complet et direct de la CNCTR aux extractions, transcriptions et transmissions**	
	Article L. 833-6 du même code	**Pouvoir de recommandation de la CNCTR en cas de transcription, d'extraction ou de transmission irrégulière de renseignements**	
	Article L. 854-6 du même code	**Règles de procédures applicables aux transcriptions, extractions et transmissions de renseignements issus de la surveillance des communications électroniques internationales**	
	Article L. 854-9 du même code	**Accès permanent, complet et direct de la CNCTR aux transcriptions, extractions et transmissions de renseignements issus de la surveillance des communications électroniques internationales**	

Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 10 (Entrée en vigueur le 31 juillet 2021)	Article L. 822-2 du code de la sécurité intérieure (2e alinéa) (III)	**Alignement des délais de conservation des captations de paroles et d'images** **Faculté de conserver des renseignements jusqu'à 5 ans après leur recueil à des fins de recherche et développement**	
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 11 (Entrée en vigueur le 31 juillet 2021)	Article L. 853-2 du code de la sécurité intérieure	**Fusion des techniques de recueil et de captation de données informatiques**	
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 12 (Entrée en vigueur le 31 juillet 2021)	Article L. 871-6 du code de la sécurité intérieure	**Faculté de requérir la coopération des opérateurs de communications électroniques pour la mise en œuvre des techniques de recueil de données de connexion par IMSI-catcher et de recueil de données informatiques**	
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 13 (Entrée en vigueur le 31 juillet 2021)	Article L. 852-3 (nouveau) du code de la sécurité intérieure Article L. 822-2 du même code	**Mise en œuvre, à titre expérimental, d'un dispositif permettant l'interception de correspondances émises ou reçues par la voie satellitaire** **Destruction des renseignements collectés par la mise en œuvre de ce dispositif à l'issue d'un délai de 30 jours**	
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 14 (Entrée en vigueur le 31 juillet 2021)	Articles 24 et 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement	**Pérennisation de la technique, dite de l' « algorithme », permettant jusqu'alors à titre expérimental la détection de connexions susceptibles de révéler une menace terroriste**	

Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 15 (Entrée en vigueur le 31 juillet 2021)	Article L. 851-3 du code de la sécurité intérieure	**Extension du champ des données pouvant être recueillies pour la mise en œuvre de la technique dite de l'« algorithme », et encadrement de ses conditions d'exécution**	
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 16 (Entrée en vigueur le 31 juillet 2021)	Article L. 851-2 du code de la sécurité intérieure	**Extension du champ des données pouvant faire l'objet d'un recueil en temps réel**	
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 17 (Entrée en vigueur le 31 juillet 2021)	Article L. 34-1 du code des postes et des communications électroniques	**Encadrement des pouvoirs d'injonction du Premier ministre à l'égard des opérateurs de communications électroniques**	Décret n° 2021-1363 du 20 octobre 2021 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion Décret n° 2021-1361 du 20 octobre 2021 relatif aux catégories de données conservées par les opérateurs de communications électroniques, pris en application de l'article L. 34-1 du code des postes et des communications électroniques

Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 18 (Entrée en vigueur le 31 juillet 2021)	Articles L. 821-1, L. 851-3, L. 853-1, L. 853-2 et L. 853-3 du code de la sécurité intérieure	**Obligation pour la CNCTR de saisir immédiatement le Conseil d'État d'un recours, avec effet suspensif, en cas d'autorisation du Premier ministre de mettre en œuvre une technique de renseignement malgré un avis défavorable de la commission** **Faculté du Premier ministre d'ordonner la mise en œuvre immédiate d'une autorisation malgré un avis défavorable de la CNCTR, en cas d'urgence dûment justifiée et pour un nombre limité de techniques et de finalités**	
	Articles L. 821-5, L. 833-9 et L. 851-2 du même code	**Abrogation de la procédure d'« urgence absolue » qui, jusqu'alors et dans des cas exceptionnels, dispensait le Premier ministre de consulter la CNCTR avant d'autoriser la mise en œuvre de certaines techniques**	
	Article L. 821-7 du même code	**Interdiction pour le Premier ministre d'ordonner la mise en œuvre immédiate d'une technique de renseignement concernant un parlementaire, un magistrat, un avocat ou un journaliste, après un avis défavorable de la CNCTR**	
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 19 (Entrée en vigueur le 31 juillet 2021)	Articles L. 853-3 du code de la sécurité intérieure Article L. 832-3 du même code	**Procédure d'examen simplifiée des demandes de retrait ou de maintenance de dispositifs de surveillance installés à l'intérieur d'un lieu d'habitation** **Information de la formation plénière des avis rendus sur ces demandes selon cette procédure**	
Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement Voir l'article 23 (Entrée en vigueur le 31 juillet 2021)	Article L. 854-9 du code la sécurité intérieure	**Obligation pour la CNCTR de saisir immédiatement le Conseil d'État d'un recours suspensif en cas d'autorisation du Premier ministre d'exploiter, malgré un avis défavorable de la commission, des communications internationales, ou des données de connexion correspondantes, de personnes utilisant un identifiant technique rattachable au territoire national**	

COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

Hôtel de Cassini - 32 rue de Babylone - 75007 Paris

Maquette et impression : DSAF / DPSG / BAEC / Section Édition – Mai 2022.