N° 4153

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 12 mai 2021.

LETTRE RECTIFICATIVE

au projet de loi (n° 4104) relatif à la **prévention** *d'***actes** *de* **terrorisme** *et au* **renseignement**,

(Procédure accélérée)

(Renvoyée à la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement.)

PRÉSENTÉE

PAR M. Jean CASTEX,
Premier ministre

Le Premier Ministre

Paris, le 12 mai 2021

LETTRE RECTIFICATIVE AU PROJET DE LOI
relatif à la prévention d'actes de terrorisme et au renseignement

Monsieur le Président,

J'ai l'honneur de vous faire connaître que le Gouvernement a décidé de modifier le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, enregistré le 28 avril 2021 à la Présidence de l'Assemblée nationale, sous le numéro 4104.

Je vous communique, ci-joint, accompagné d'un exposé des motifs, d'une étude d'impact et de l'avis du Conseil d'Etat, l'ensemble de ces modifications qui sont les suivantes :

- au chapitre Ier, ajout d'un 6° dans un article (article 3) ;

- au chapitre II, insertion de six articles (articles 12 à 17) ;

- insertion d'un chapitre intitulé « Dispositions relatives aux archives intéressant la défense nationale » (chapitre IV) et d'un article (article 19) ;

- modification du chapitre IV devenant le chapitre V, les articles 13 à 17 devenant les articles 20 à 24, l'article 18 devenant l'article 26 et l'article 19 devenant l'article 29 ;

- au chapitre V, modification de deux articles (articles 20 et 26) et insertion de trois articles (articles 25, 27 et 28).

Je vous demande d'informer le Sénat de cette rectification.

Je vous prie d'agréer, Monsieur le Président, l'expression de ma haute considération.

Jean CASTEX

Monsieur Richard FERRAND
Président de l'Assemblée nationale
Assemblée nationale
126, rue de l'Université

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

La présente lettre rectificative au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement complète d'un 6° l'article 3 du projet de loi afin d'articuler la procédure de renouvellement des mesures individuelles de contrôle administratif et de surveillance en cours, qui expireront nécessairement le 31 juillet 2021, avec la date d'entrée en vigueur de la loi, cette procédure supposant nécessairement, à compter de cette date, un délai de cinq jours entre la notification du renouvellement de la mesure et exécution, ce délai pouvant être mis à profit par la personne concernée pour saisir le juge administratif.

Surtout, la présente lettre rectificative vise d'une part, à compléter le régime de certaines techniques de recueil de renseignement et d'autre part, à tirer les conséquences de l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2020 (n° C-511/18, C-512/18 et C-520/18) et de la décision French data Network et autres du Conseil d'Etat du 21 avril 2021 (n° 393099, 394922, 397844, 397851, 424717, 424718).

Ainsi, le chapitre II est complété par six articles numérotés 12 à 17 et après l'article 12, qui devient l'article 18, il est inséré un chapitre IV intitulé « Dispositions relatives aux archives intéressant la défense nationale » comprenant l'article 19.

Enfin, la présente lettre rectificative opère à des modifications de numérotation des chapitres et des articles du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement. Ainsi, le chapitre IV devient le chapitre V, les articles 13 à 17 deviennent les articles 20 à 24, l'article 18 devient l'article 26 et l'article 19 devient l'article 29.

LETTRE RECTIFICATIVE AU PROJET DE LOI RELATIF À LA PRÉVENTION D'ACTES DE TERRORISME ET AU RENSEIGNEMENT

Le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement est ainsi modifié :

1° L'article 3 est modifié selon la rédaction annexée ;

2° Le chapitre II est complété par six articles numérotés 12 à 17 ;

3° Après l'article 12, qui devient l'article 18, il est inséré un chapitre IV intitulé « Dispositions relatives aux archives intéressant la défense nationale » comprenant l'article 19 ;

4° Le chapitre IV devient le chapitre V, les articles 13 à 17 deviennent les articles 20 à 24, l'article 18 devient l'article 26 et l'article 19 devient l'article 29 ;

5° Le chapitre V est complété par trois articles numérotés 25, 27 et 28 ;

6° Les articles 20 et 26 sont modifiés selon la rédaction annexée.

ANNEXE

Texte du projet de loi n° 4104,
relatif à la prévention d'actes de terrorisme et au renseignement

(Rédaction résultant de la lettre rectificative n° 4153)

EXPOSÉ DES MOTIFS

Le présent projet de loi vise, en son chapitre Ier, à pérenniser et à compléter les instruments de prévention de la commission d'actes de terrorisme dont le législateur a doté l'autorité administrative à l'issue de l'état d'urgence, au terme de trois ans de mise en œuvre et alors que le niveau de la menace demeure toujours très élevé sur l'ensemble du territoire national.

Les articles 1er à 4 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (dite loi « SILT ») ont ainsi instauré de nouvelles mesures de police administrative inspirées de l'état d'urgence mais adaptées à des situations de droit commun : les périmètres de protection (article L. 226-1), la fermeture des lieux de cultes (article L. 227-1), les mesures individuelles de contrôle administratif et de surveillance (article L. 228-1) et les visites domiciliaires et saisies (article L. 229-1).

En raison du caractère novateur de ces mesures accroissant de manière significative les pouvoirs de l'autorité de police administrative, l'article 5 de la loi du 30 octobre 2017 a prévu une information permanente du Parlement ainsi qu'une évaluation annuelle de leur mise en œuvre et a limité au 31 décembre 2020 l'application des dispositions les instituant, renvoyant de ce fait la question de la pérennisation de ces mesures au-delà de cette date à l'évaluation de leur caractère nécessaire, adapté et proportionné. La crise sanitaire liée à la covid-19 et ses conséquences sur le fonctionnement normal des institutions n'ayant pas permis au Gouvernement de présenter en temps utile au Parlement le projet de loi pérennisant ces mesures, cette échéance a été reportée au 31 juillet 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.

L'examen de l'ensemble des décisions prises en application de ces dispositions, depuis plus de trois ans, démontre leur grande utilité opérationnelle pour l'autorité administrative et leur caractère complémentaire par rapport à l'intervention de l'autorité judiciaire, soit en amont de l'ouverture d'une procédure judiciaire pour assurer le suivi d'une personne manifestant des signes de radicalisation à caractère terroriste, soit à l'issue de la détention d'une personne condamnée pour une infraction à caractère terroriste ou ayant présenté des signes de radicalisation en détention.

Par ailleurs, leur nombre mesuré – de l'ordre d'une cinquantaine de mesures individuelles de contrôle administratif et de surveillance en vigueur simultanément –, ainsi que les faibles taux de contestation et de remise en cause par le juge des décisions prises confirment une bonne appropriation de ces instruments par l'autorité de police administrative. Ce bilan justifie donc la pérennisation de ces mesures, dont la nécessité est confirmée par la permanence de la menace terroriste.

L'**article 1er** abroge en conséquence le II de l'article 5 de la loi n° 2017-1510 du 30 octobre 2017 aux termes duquel les chapitres VI à X du titre II du code de la sécurité intérieure, issus des quatre premiers articles de cette loi, ne sont applicables que jusqu'au 31 juillet 2021. Cette abrogation permet ainsi de conférer un caractère permanent à ces dispositions.

L'application quotidienne de la loi ayant, par ailleurs, permis d'en révéler certaines insuffisances ou limites, les articles suivants visent à compléter ou à ajuster ces mesures sans toutefois modifier l'équilibre général du dispositif voté par le législateur en 2017 et dont le Conseil constitutionnel a estimé qu'il opérait une conciliation qui n'était pas manifestement déséquilibrée entre l'objectif de prévention d'actes de terrorisme et la protection des droits et libertés garantis par la Constitution.

Dans cette optique, l'**article 2** vise à élargir le champ d'application de la mesure de fermeture des lieux de culte en permettant de prononcer également la fermeture de lieux dépendant du lieu de culte visé par la mesure et dont il existe des raisons sérieuses de penser qu'ils seraient susceptibles d'être utilisés aux même fins pour faire échec à l'exécution de la mesure de fermeture. Selon les informations dont dispose l'autorité administrative, cette fermeture pourra être concomitante à celle du lieu de culte ou postérieure, une fois constatées les manœuvres pour y faire échec. Dans tous les cas, la mesure prendra fin en même temps que celle visant le lieu de culte lui-même.

L'**article 3** ajuste certaines dispositions applicables aux mesures individuelles de contrôle administratif et de surveillance pour rendre ce dispositif encore plus opérationnel.

Le *a* du 1° et le 2° visent à renforcer la surveillance des personnes faisant l'objet d'une telle mesure en permettant à l'autorité administrative d'exiger un justificatif de domicile de la personne concernée afin de vérifier son lieu d'habitation pour définir son périmètre de résidence (article L. 228-2 du code de la sécurité intérieure), pour aménager la mesure afin de permettre à la personne concernée de poursuivre sa vie privée ou familiale (article L. 228-2), ou encore dans le cadre d'une obligation de déclaration des déplacements de la personne en dehors d'un périmètre déterminé (article L. 228-4). Cette nouvelle exigence vise à renforcer le caractère proportionné de la définition de ce périmètre tout en limitant les risques de déclarations de domicile ou de changement de domicile visant à faire échec à la surveillance.

Le *b* du 1° vise à permettre à l'autorité administrative de prononcer une mesure ponctuelle d'interdiction de paraître à l'encontre des personnes faisant l'objet d'une mesure individuelle de contrôle administratif et de surveillance au titre de l'article L. 228-1 du code de la sécurité intérieure. Actuellement, les personnes faisant l'objet d'une telle mesure peuvent être soumises à deux régimes distincts mais alternatifs, au-delà des obligations communes de déclaration de domicile ou de changement de domicile : au titre de l'article L. 228-2, le ministre de l'intérieur peut leur faire interdiction de se déplacer au-delà d'un périmètre géographique déterminé et leur prescrire de se présenter périodiquement aux services de police ou aux unités de gendarmerie ; au titre de l'article L. 228-4, ils sont seulement astreints à signaler leurs déplacements au-delà d'un périmètre déterminé et peuvent, ponctuellement ou pendant la durée de la mesure, faire l'objet d'une interdiction de paraître en un lieu déterminé. Par suite, une personne faisant l'objet d'une interdiction de déplacement en dehors d'un périmètre de résidence ne peut simultanément faire l'objet d'une interdiction de paraître dans un lieu particulier, alors que les besoins de surveillance et de contrôle peuvent parfois commander de cumuler ces interdictions, en particulier lorsque se tient, au sein même du périmètre prescrit pour la résidence, un événement qui, par son ampleur ou ses circonstances particulières, est exposé à un risque de menace terroriste. Cette interdiction de paraître pourra donc désormais être prononcée en complément des obligations prévues à l'article L. 228-2 du code de la sécurité intérieure afin d'écarter temporairement la personne du lieu où se tient un tel événement. Pour tenir compte de la rigueur de cette mesure, prononcée en complément de l'interdiction de quitter un périmètre déterminé, celle-ci devra être expressément motivée au regard des

critères définis par la loi, ne pourra excéder la durée de celle de l'événement, dans la limite d'une durée de trente jours, et devra, sauf urgence dûment justifiée, être notifiée à l'intéressé au moins quarante-huit heures avant son entrée en vigueur.

Le 3° instaure une dérogation à la durée maximale des mesures individuelles de contrôle administratif et de surveillance, en principe prononcées pour une durée de trois mois renouvelable sans pouvoir toutefois excéder une durée cumulée de douze mois, leur renouvellement au-delà de six mois étant, par ailleurs, subordonné à l'existence d'éléments nouveaux ou complémentaires. La disposition nouvelle vise à porter cette durée maximale cumulée à vingt-quatre mois lorsque ces obligations sont prononcées dans un délai de six mois à compter de la libération d'une personne ayant fait l'objet d'une condamnation à une peine d'emprisonnement supérieure ou égale à cinq ans pour des faits de terrorisme, ou d'une durée supérieure ou égale à trois ans lorsque l'infraction aura été commise en état de récidive légale. Chaque renouvellement au-delà d'une durée cumulée de douze mois sera prononcé pour une durée de trois mois et subordonné à l'existence d'éléments nouveaux ou complémentaires. Comme tel est actuellement le cas, ces renouvellements au-delà de douze mois seront effectués sous le contrôle rapide du juge, chaque renouvellement étant notifié au moins cinq jours avant l'expiration de la mesure précédente afin de permettre à la personne concernée de saisir le juge de l'excès de pouvoir, sous 48 heures, de la légalité de cette mesure qui ne peut alors entrer en vigueur avant que le juge ait statué, dans un délai maximal de 72 heures.

Le 4° prévoit également, s'agissant précisément de cette procédure spécifique de contestation de la mesure de renouvellement, que lorsque la personne concernée a saisi un tribunal territorialement incompétent, imposant ainsi un renvoi à la juridiction compétente, l'arrêté initial est prorogé jusqu'à ce que la juridiction compétente ait statué. Cette disposition vise ainsi à éviter que la saisine d'un tribunal incompétent ne soit utilisée de manière dilatoire, risquant alors d'aboutir au prononcé d'une décision juridictionnelle après l'expiration de la précédente mesure et provoquant ainsi une discontinuité dans l'application de la mesure.

Enfin, le 5° modifie l'article L. 228-6 du code de la sécurité intérieure pour préciser que les obligations imposées dans le cadre d'une mesure individuelle de contrôle administratif et de surveillance prennent en compte les obligations déjà prescrites par l'autorité judiciaire lorsqu'elles sont de même nature ou poursuivent le même objectif, afin de respecter le principe

de proportionnalité, conformément à la jurisprudence du Conseil d'Etat en la matière.

L'**article 4** ouvre la possibilité de procéder à la saisie des supports informatiques contenant des données lorsque, au cours d'une visite et alors que celle-ci a révélé des éléments en lien avec la menace, la personne concernée par la mesure fait obstacle à l'accès à ces données informatiques ou à leur copie.

L'**article 5** crée, au sein du code de procédure pénale, une mesure judiciaire de réinsertion sociale antiterroriste destinée à renforcer le suivi des personnes condamnées pour des infractions à caractère terroriste qui ne font l'objet, à leur sortie de détention, d'aucune autre mesure de suivi judiciaire. Cette mesure ne peut être prononcée qu'à l'encontre des individus condamnés, pour des infractions de nature terroriste, à des peines graves, supérieure ou égale à cinq ans d'emprisonnement, ou trois ans en cas de récidive, et qui présentent, à leur sortie de détention, un niveau de dangerosité particulièrement élevée. Elle permet d'assujettir la personne à un certain nombre d'obligations destinées à faciliter sa réinsertion et à prévenir sa récidive. Au regard de la sensibilité de la mesure, et afin de tenir compte des exigences posées par le Conseil constitutionnel dans sa décision n° 2020-895 DC du 7 août 2020, le prononcé de la mesure est entouré de plusieurs garanties : elle est prononcée par le tribunal de l'application des peines, après débat contradictoire ; sa durée maximale est fixée à un an, renouvelable dans la limite de cinq ans ; elle ne peut être prononcée qu'à l'encontre de personnes ayant été placés en mesure de recevoir un accompagnement à la réinsertion en détention.

L'**article 6** étend la possibilité de communication des informations relatives à l'admission d'une personne en soins psychiatriques, aujourd'hui limitée au seul représentant de l'État dans le département du lieu d'hospitalisation, à celui qui est chargé du suivi de cette personne lorsqu'elle représente par ailleurs une menace grave pour la sécurité et l'ordre publics à raison de sa radicalisation à caractère terroriste. En effet, certains individus suivis pour ce motif peuvent faire l'objet d'une admission en soins psychiatriques dans un département différent de celui dans lequel ils résident, dès lors que les troubles conduisant à cette admission ont été constatés dans ce département. Il en résulte une déperdition de l'information pour l'autorité administrative, départementale ou nationale, en charge du suivi de la radicalisation à caractère terroriste de la personne concernée.

Le chapitre II a trait à la modification de certaines dispositions relatives au renseignement. Près de cinq ans après l'adoption de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, il vise à apporter au livre VIII du code de sécurité intérieure les ajustements nécessaires pour que les services de renseignement continuent de disposer de moyens d'action adéquats et proportionnés face aux menaces persistantes qui pèsent sur les intérêts fondamentaux de la Nation.

L'**article 7** complète l'article L. 822-3 du code de sécurité intérieure pour encadrer les conditions dans lesquelles les services de renseignement peuvent, d'une part, exploiter les renseignements qu'ils ont obtenus pour une finalité différente de celle qui en a justifié le recueil et, d'autre part, se transmettre les renseignements qu'ils ont collectés par la mise en œuvre des techniques autorisées par le livre VIII du code de la sécurité intérieure.

Le partage des renseignements nécessaires à l'exercice des missions de chacun des services de la communauté du renseignement est en effet une condition essentielle de l'efficacité de l'action qu'ils mènent pour la défense et la promotion des intérêts fondamentaux de la Nation. Dans cette perspective, l'article en précise le cadre opérationnel, dans le respect du principe, posé par le législateur en 2015, suivant lequel les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles prévues à l'article L. 811-3.

Ainsi, en premier lieu, lorsqu'un service de renseignement obtient, après la mise en œuvre régulière d'une technique de renseignement pour une finalité donnée, des renseignements utiles à la poursuite d'une finalité différente de celle qui en a justifié le recueil, il peut les transcrire ou les extraire pour le seul exercice de ses missions.

En deuxième lieu, les renseignements collectés, extraits ou transcrits peuvent être transmis à d'autres services de renseignement si cette transmission est strictement nécessaire à l'exercice des missions du service destinataire. Une telle transmission devra néanmoins être subordonnée à l'autorisation du Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), dans deux hypothèses, afin de respecter les principes établis en 2015 et qui gouvernent l'activité de services de renseignement français :

– lorsque cette transmission concerne des renseignements à l'état brut – c'est-à-dire ni extraits, ni transcrits – et poursuit une finalité différente de celle ayant justifié leur recueil ;

– lorsque cette transmission concerne des renseignements, qu'ils soient à l'état brut, extraits ou transcrits, recueillis par la mise en œuvre d'une technique à laquelle le service de renseignement destinataire n'aurait pu recourir au titre de la finalité motivant la transmission.

Ces deux verrous permettent ainsi de s'assurer de la pertinence de la transmission entre services, en particulier lorsqu'elle procède d'une technique limitée à une finalité donnée ou réservée à un nombre restreint de services de renseignement.

L'article 7 organise également deux types de contrôle :

– d'une part, un dispositif de contrôle interne, le responsable de chaque service de renseignement désignant un agent chargé de veiller, sous sa responsabilité, au respect des conditions précitées ainsi qu'à la destruction des renseignements transmis dans les délais de conservation applicables à chacun. Pour mener à bien cette mission, il sera informé par ses homologues des autres services de la destruction, dans les conditions fixées au cinquième alinéa du II de l'article L. 822-3 du code de la sécurité intérieure, des renseignements que le service auprès duquel il a été placé a été autorisé à recueillir ;

– d'autre part, les opérations de transmission sont placées sous le contrôle de la CNCTR, qui disposera d'un accès permanent aux relevés assurant la traçabilité des transmissions et précisant la date, la nature, la finalité et les destinataires de chacune d'elles, ce qui permettra à la commission d'exercer utilement son contrôle et de faire usage, le cas échéant, de son pouvoir de recommandation au Premier ministre en cas de manquement constaté voire, si elle estime qu'un manquement persiste, d'en saisir la formation spécialisée du Conseil d'Etat compétente en matière de renseignement.

Le VI de cet article modifie les dispositions de l'article L. 863-2 en encadrant davantage les modalités de transmission d'informations par les différentes autorités administratives aux services de renseignement, d'initiative ou sur la demande de ces derniers. Le champ de ces transmissions, qui concernent également les informations couvertes par un secret protégé par la loi, est limité aux informations strictement nécessaires à l'accomplissement des missions de ces services et susceptibles de concourir à la défense et à la promotion des intérêts fondamentaux de la Nation. Lorsque les informations ainsi transmises font l'objet, de la part des services destinataires de ces informations, d'un traitement de données à caractère personnel, elles doivent être conservées dans les conditions

applicables à ce traitement et détruites lorsqu'elles ne sont plus nécessaires à l'accomplissement des missions ayant motivées leur transmission. La nouvelle rédaction de l'article L. 863-2 rappelle que les agents destinataires de ces informations sont tenus au respect du secret professionnel. Enfin, un contrôle interne du respect de ces dispositions est mis en place.

Eu égard à la création de ce régime général de transmission d'informations par les autorités administratives aux services de renseignement, le VI de l'article 7 abroge l'article L. 135 S du livre des procédures fiscales qui organise, au profit des services de renseignement, un droit de communication des informations détenues par les services fiscaux, droit de communication spécifique désormais superflu.

Enfin, dans les conditions prévues par le règlement général sur la protection des données, le VIII de l'article 7 modifie les articles 48 et 49 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui organisent le droit d'accès des personnes aux traitements dont leurs données à caractère personnel font l'objet, pour en exclure l'information suivant laquelle des données à caractère personnel ont fait l'objet d'une transmission aux services de renseignement, eu égard au risque opérationnel que ferait courir un tel accès.

L'**article 8** instaure un régime autonome de conservation de renseignements pour les seuls besoins de la recherche et du développement en matière de capacités techniques de recueil et d'exploitation des renseignements. Il est en effet indispensable pour les services de renseignement de disposer d'un stock important de données, captées par telle ou telle technique de renseignement, leur permettant d'acquérir des connaissances suffisantes pour développer, améliorer et valider ces capacités. Le nouveau III de l'article L. 822-2 permet donc une conservation de renseignements au-delà de la durée normalement applicable, dans la mesure strictement nécessaire à ces travaux de recherche et de développement et à l'exclusion de toute utilisation pour la surveillance des personnes concernées, sous réserve que ces renseignements soient expurgés des motifs et des finalités ayant justifié leur recueil et conservés dans des conditions ne permettant pas de rechercher l'identité des personnes concernées. A cette fin, les paramètres techniques applicables à chaque programme de recherche destinés à garantir le respect de ces conditions sont préalablement soumis à une autorisation préalable du Premier ministre, délivrée après avis de la CNCTR. Enfin, ces renseignements sont, en outre, uniquement accessibles aux agents spécialement habilités à cet effet et exclusivement affectés à cette mission puis détruits dès qu'ils ne sont plus

utiles aux besoins précités et au plus tard cinq ans après leur recueil. Le II de l'article 8 prévoit que le service du Premier ministre assurant la centralisation de certains renseignements collectés par les services de renseignements pourra également les conserver, aux mêmes fins et dans les mêmes conditions, après accord des services à l'origine de leur recueil.

L'**article 9** modifie l'article L. 853-2 du code de la sécurité intérieure relatif aux techniques de recueil des données informatiques (1°) et de captation des données informatiques (2°). Ces deux techniques de renseignement, qui présentent des finalités identiques, ne bénéficient toutefois pas d'une même durée d'autorisation : la première peut être autorisée pour une durée maximale de trente jours quand la seconde peut être autorisée pour une durée maximale de deux mois. Or, le recueil des données informatiques nécessite souvent une mise en œuvre technique complexe et longue, peu compatible avec la particulière brièveté de cette autorisation. C'est pourquoi la durée d'autorisation de cette technique est alignée sur celle de captation des données informatiques, à savoir deux mois, soit un niveau qui demeure inférieur de moitié à la durée d'autorisation normalement applicable aux autres techniques de renseignement.

L'**article 10** modifie l'article L. 871-6 du code de la sécurité intérieure afin de compléter la liste des techniques de renseignement pour lesquelles la coopération des opérateurs de communications électroniques peut être requise afin qu'ils réalisent sur leurs réseaux des opérations matérielles nécessaires à leur mise en œuvre et de garantir qu'elles ne porteront pas atteinte au fonctionnement et à la sécurité des réseaux, ni à la qualité du service rendu par les opérateurs. L'article 10 ajoute ainsi au champ de cette disposition les techniques de recueil ou de captation des données informatiques, prévues à l'article L. 853-2 du code de la sécurité intérieure, qui peuvent être mise en œuvre de deux manières : soit par accès direct au support informatique concerné, soit par les réseaux des opérateurs de communications électroniques. La seconde extension vise la technique de renseignement visée à l'article L. 851-6 du même code, soit celle qui permet *le recueil au moyen d'un appareil* de type « IMSI–*catchers* de données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés. En effet, le déploiement de la 5G (communications mobiles de 5^{e} génération) aura pour conséquence que les identifiants des terminaux mobiles deviendront temporaires, évolueront à une fréquence élevée et seront attribués par le réseau.

Seul l'opérateur pourra établir le lien entre ces identifiants temporaires et les identifiants pérennes des abonnements ou des équipements terminaux utilisés. Il sera donc nécessaire, pour que la technique de l'« IMSI–*catcher* » conserve un intérêt opérationnel, de pouvoir obtenir des opérateurs de communications électroniques le lien entre ces deux types d'identifiants. Une modification corrélative est effectuée à l'article L. 871-3 du même code aux mêmes fins s'agissant cette fois du concours des opérateurs de communications électroniques au profit de l'autorité judiciaire.

L'**article 11** autorise, à titre expérimental, les services de renseignement à intercepter, par le biais d'un dispositif de captation de proximité, les correspondances transitant par la voie satellitaire. L'interception de ce type de communications représente un enjeu opérationnel majeur pour les services de renseignement, en raison du déploiement de nouvelles constellations satellitaires et du développement à venir d'une offre alternative de télécommunications de nature à concurrencer des opérateurs de communications électroniques traditionnels.

Face à cet enjeu, le cadre légal actuel se révèle très largement inadapté, d'une part, car les réseaux en cours de déploiement sont tous exploités par des opérateurs étrangers, qui ne peuvent être facilement réquisitionnés dans le cadre de la loi renseignement, d'autre part, car les communication satellitaires se caractérisent par une plus grande instabilité technique, qui rend plus complexe d'opérer un ciblage des interceptions au stade de la captation, sur le modèle des interceptions de sécurité.

Afin de ne pas désarmer les services de renseignement face à cette évolution des modes de communication, le dispositif proposé tend à créer, à titre expérimental, un nouveau cas d'interception de correspondances par le biais d'un dispositif de proximité, restreint à certaines des finalités prévues à l'article L. 811-3 du code de la sécurité intérieure et entouré de garanties fortes.

L'**article 12** a d'abord pour objet de pérenniser la technique de renseignement prévue à l'article L. 851-3 du code de la sécurité intérieure, dite algorithme, instaurée au titre d'une expérimentation dont l'échéance a été reportée au 31 décembre 2021 en application de l'article 25 modifié de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement et dont le bilan est concluant. Cette technique vise ainsi à permettre la détection de manière précoce des menaces terroristes. L'un des enjeux les plus cruciaux de l'activité de renseignement consiste en effet à être en mesure de détecter une nouvelle menace, par définition inconnue, afin de la caractériser et de

l'évaluer. Lorsque cette menace émane d'un groupe ou d'une organisation structurée et identifiable, une surveillance ciblée du groupe ou de l'organisation permet le plus souvent d'en détecter les acteurs et de les identifier. Néanmoins, de nouveaux comportements sont apparus, à la faveur notamment de la diffusion informatique d'une vaste propagande terroriste et de l'émergence de nouveaux moyens de communication électronique. Les actions terroristes sont ainsi, de plus en plus, le fait d'individus qui s'inspirent des messages de propagande qui émanent des organisations terroristes, incitant au passage à l'acte en fournissant les tutoriels pour leur réalisation, mais qui ne sont pas entrés en contact visible ou direct avec des organisations, réseaux ou groupes terroristes, échappant ainsi à toute capacité de détection par le biais d'une surveillance ciblée. En effet, si le maillage territorial des services de renseignement et de sécurité ainsi que la sensibilisation des différents acteurs administratifs et sociaux permettent de détecter une évolution du comportement social d'un individu susceptible de révéler l'existence d'une menace terroriste, cette capacité disparaît lorsque ces indices n'apparaissent que par l'activité numérique de la personne.

La pérennisation de ce dispositif se justifie ainsi, en premier lieu, par sa pertinence opérationnelle, cette capacité de détection ne pouvant être remplie par aucun des moyens traditionnels des services de renseignement. Cette technique est par ailleurs entourée de garanties spécifiques et substantielles : les traitements automatisés ne peuvent recueillir d'autres données que celles répondant à leurs paramètres de conception ni ne peuvent, par eux-mêmes, permettre l'identification des personnes auxquelles les données traitées se rapportent ; leur mise en œuvre suppose une procédure de double autorisation par le Premier ministre, chacune étant précédée d'un avis d'une autorité administrative indépendante, la Commission nationale de contrôle des techniques de renseignement (CNCTR) ; celle-ci, dotée de moyens d'investigation étendus, est munie de l'ensemble des informations utiles pour se prononcer sur le paramétrage des traitements ainsi que sur la pertinence des signalements qu'ils détectent.

Cette phase expérimentale a également permis d'identifier les ajustements nécessaires, auxquels le projet procède par ailleurs. Aussi, **l'article 13** modifie ainsi l'article L. 851-3 du code de la sécurité intérieure encadrant les traitements automatisés pouvant être appliqués sur les données afférentes aux communications électroniques aux seules fins de détecter des connexions susceptibles de révéler une menace terroriste. Il rend compte de manière plus précise des modalités d'exécution des algorithmes, résultant de choix techniques opérés au cours de la phase expérimentale. Il inclut, parmi les données pouvant faire l'objet des traitements automatisés prévus par

l'article L. 851-3, tous les types d'URL. Il peut s'agir, comme la loi le permet aujourd'hui, des données permettant l'accès des équipements terminaux aux services de communication au public en ligne qui relèvent, par nature, de la catégorie des données de connexion ; il peut également s'agir, comme le prévoit l'article 13, des « adresses complètes de ressources sur internet » pouvant faire référence au contenu des informations consultées, qui échappent aujourd'hui au champ d'application de l'article L. 851-3, alors pourtant que leur recueil permettrait de fournir des renseignements particulièrement utiles à la prévention du terrorisme. Il est donc déterminant que les traitements automatisés prévus à l'article L. 851-3 puissent également s'appliquer à ce type d'URL pour que soient détectées les consultations d'informations présentant un lien avéré avec les activités terroristes et, *in fine*, après autorisation, pour que soient identifiés les individus à l'origine de ces connexions.

Outre que la mise en œuvre des traitements ne pourra plus être sollicitée que par les seuls services spécialisés de renseignement, plusieurs garanties supplémentaires sont introduites.

D'une part, la possibilité de proroger la durée de conservation des données correspondant aux paramètres de détection et dont le Premier ministre autorise le recueil est supprimée. En l'état de la loi, cette durée est fixée à soixante jours mais peut être prolongée, en cas d'éléments sérieux confirmant l'existence d'une menace terroriste, jusqu'à quatre ans. L'expérimentation a fait apparaître qu'une telle prolongation n'était pas nécessaire, dès lors que le délai normal de soixante jours permettait de solliciter la mise en œuvre d'une technique de renseignement ciblée sur la personne à laquelle se rapportent les données détectées par les traitements.

D'autre part, la mission d'exécuter les traitements automatisés sera exclusivement confiée à un service du Premier ministre, le groupement interministériel de contrôle, service à compétence nationale distinct des services de renseignement. Les données qui ne sont pas susceptibles de révéler une menace terroriste sont par ailleurs immédiatement détruites. Ces dispositions reflètent la pratique actuelle de la mise en œuvre des algorithmes autorisés, dans les conditions définies par la loi et sous le contrôle de la CNCTR.

L**'article 14** procède à l'inclusion des adresses complètes de ressources sur internet utilisées par une personne, dans le champ des données pouvant faire l'objet d'une détection en temps réel sur les réseaux de communications électroniques, au titre de la technique prévue à l'article L. 851-2 du code de

la sécurité intérieure. Cette détection est effectuée pour les seuls besoins de la prévention du terrorisme, à l'encontre de personnes préalablement identifiées comme étant susceptibles d'être en lien avec une menace terroriste, ou de personnes de leur entourage. Par voie de conséquence, la durée de conservation des URL recueillies au moyen de la technique de détection en temps réel (article L. 851-2) est alignée sur celle fixée au 2° de l'article L. 822-2 (120 jours) déjà applicable à des données de même nature.

L'article **15** tend à modifier les dispositions de l'article L. 34-1 du code des postes et des communications électroniques qui organise le régime de conservation des données relatives aux communications électroniques par les opérateurs pour prévoir, par dérogation au principe selon lequel ces opérateurs effacent ou rendent anonymes sans délai les données de connexion afférentes aux communications de leurs abonnés, les hypothèses dans lesquelles il peut être dérogé à cette obligation, conformément aux exigences posées par le Conseil d'Etat dans sa décision du 21 avril 2021.

Ainsi, le II *bis* prévoit que l'effacement des données relatives à l'identité civile du client peut être différé pour un délai de cinq ans après la fin de validité du contrat d'abonnement tandis que l'effacement des autres informations fournies par l'utilisateur lors de la souscription du contrat ou de l'ouverture du compte, les informations relatives au paiement, ainsi que les données techniques permettant d'identifier la source de la connexion ou relatives aux équipements terminaux de connexion utilisés (adresses IP et assimilés), peut être différé d'un an.

En complément de ces données dont l'effacement est différé dans tous les cas, le III prévoit, dans l'hypothèse d'une menace grave, actuelle ou prévisible sur la sécurité nationale, la possibilité pour le Premier ministre d'enjoindre aux opérateurs de conserver de manière générale et indifférenciée, pendant une durée d'un an, certaines catégories de données relatives aux communications électroniques. Cette injonction prend la forme d'un décret dont la durée d'application ne peut excéder un an, renouvelable si les conditions prévues pour son édiction continuent d'être réunies. L'expiration de l'injonction du Premier ministre est en tout état de cause sans effet sur la durée de conservation de chacune de ces données, fixée à un an.

Le III *bis* permet aux différentes autorités disposant, en vertu de la loi, d'un droit d'accès aux données de connexion d'accéder aux données conservées en application de l'article L. 34-1 du code des postes et des communications électroniques au moyen d'une injonction de conservation rapide aux fins de prévention et de répression de la criminalité grave et des

autres manquements graves aux règles dont elles ont la charge d'assurer le respect.

Le VI de l'article L. 34-1 est modifié pour prévoir qu'un décret en Conseil d'État devra préciser, d'une part, les informations et catégories de données qui pourront faire l'objet d'une conservation sur le fondement des nouveaux II *bis* et III et, d'autre part, dans quelles conditions les surcoûts induits par ces obligations de conservation devront être compensés par l'État auprès des opérateurs concernés.

Enfin, l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, relatif aux fournisseurs d'accès à des services de communication au public en ligne est modifié pour prévoir que ces derniers conservent, dans les mêmes conditions que celles prévues aux nouveaux II *bis*, III et III *bis* de l'article L. 34-1, les données qu'ils détiennent.

L'article **16** tire également les conséquences des décisions précitées de la Cour de justice de l'Union européenne et du Conseil d'État, selon lesquelles la mise en œuvre des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 doit, sauf cas d'urgence dûment justifiée, être subordonnée à un contrôle préalable par une juridiction ou une autorité indépendante dont la décision est dotée d'un effet contraignant.

Cet article modifie donc les dispositions de l'article L. 821-1 du code de la sécurité intérieure pour étendre à toute technique de renseignement autorisée après avis défavorable de la commission nationale de contrôle des techniques de renseignement le mécanisme, actuellement prévu au III de l'article L. 853-3 du code de la sécurité intérieure en ce qui concerne l'introduction dans un lieu privé à usage d'habitation, de saisine obligatoire de la formation spécialisée du Conseil d'État par la commission. La formation spécialisée du Conseil d'État dispose alors d'un délai de vingt-quatre heures pour statuer, délai pendant lequel la technique de renseignement en cause ne peut pas être mise en œuvre.

Toutefois, en cas d'urgence dûment justifiée et si le Premier ministre a ordonné la mise en œuvre immédiate de la technique ainsi autorisée, il est possible de passer outre ce caractère suspensif. Cette faculté n'est en revanche pas possible s'agissant des autorisations délivrées pour la mise en œuvre de la technique de l'algorithme, en application des I et II de l'article L. 851-3 du code de la sécurité intérieure, ou concernant des personnes exerçant les professions protégées mentionnées à l'article L. 821-7. Elle par ailleurs est limitée aux seules finalités prévues aux 1°, 4° ou a) du 5° de

l'article L. 811-3, s'agissant de la mise en œuvre des techniques de recueil de renseignement prévues aux articles L. 853-1, L. 853-2 et L. 853-3, seule la finalité de prévention du terrorisme justifiant cette procédure lorsque l'introduction dans un lieu privé concerne une habitation.

Compte tenu de la création de cette nouvelle procédure d'urgence, la procédure d'urgence absolue prévue à l'article L. 821-5 du code de la sécurité intérieure est supprimée.

L**'article 17** qui introduit un nouvel article 706-105-1 au sein du chapitre II du titre XXV du livre IV du code de procédure pénale, étend, par dérogation à l'article 11 du code de procédure pénale, les possibilités de transmission par l'autorité judiciaire, d'éléments de toute nature figurant dans des procédures judiciaires, pour deux types de finalités : d'une part, l'autorité judiciaire peut transmettre à certains services visés à l'article L. 2321-2 du code de la défense, de sa propre initiative ou à la demande de ces services, des éléments nécessaires à l'exercice de leur mission en matière de sécurité et de défense des systèmes d'information ; d'autre part, elle peut également transmettre à certains des services de renseignement visés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure, des éléments de toute nature figurant dans des procédures en matière de trafic de stupéfiants, traite des êtres humain, lutte contre les filières d'immigration clandestines ou en matière d'armes lorsque ces éléments sont nécessaires à l'exercice des missions des services concernés au titre de la prévention de la criminalité et de la délinquance organisées.

Ces transmissions sont assurées par le Procureur de la République de Paris, qui dispose d'une compétence territoriale spéciale dans ces deux matières. Si la procédure fait l'objet d'une information judiciaire, cette communication ne peut intervenir qu'avec l'avis favorable du juge d'instruction de Paris. Le juge d'instruction peut également procéder à cette communication pour les procédures d'information dont il est saisi après avoir recueilli l'avis du procureur de la République de Paris. Les informations communiquées ne peuvent être transmises à des services étrangers ou à des organismes internationaux compétents dans le domaine du renseignement. Toute personne qui en est destinataire est tenue au secret professionnel.

Par ailleurs, le nouveau chapitre IV, constitué d'un unique **article 19**, modifie l'article L. 213-2 du code du patrimoine pour clarifier le régime de communicabilité des archives classifiées dans le sens d'une plus grande ouverture au bénéfice de l'ensemble des usagers des services d'archives, et, en particulier, des chercheurs et des historiens, tout en garantissant la

protection des documents les plus sensibles pour la défense nationale, en particulier ceux des services de renseignement, vis-à-vis des puissances étrangères ou des organisations qui seraient hostiles à notre pays.

L'article L. 213-2 du code du patrimoine, tel qu'il résulte de la loi n° 2008-696 du 15 juillet 2008 relative aux archives, concilie droit d'accès aux archives publiques et préservation de certaines informations sensibles en prévoyant que 25, 50, 75, voire 100 ans devront s'écouler avant que certains documents, touchant notamment au secret des affaires, à la vie privée des personnes, à une affaire portée devant une juridiction ou encore dont la divulgation porterait atteinte à la sécurité d'une personne, puissent être librement communiquées. Il existe cependant une catégorie d'archives publiques dont la consultation reste impossible à jamais parce que les informations qu'elles renferment permettraient de concevoir, de fabriquer, d'utiliser ou de localiser des armes de destruction massive.

La définition du secret de la défense nationale prévue par le code pénal est, au contraire de l'approche du code du patrimoine, purement formelle. L'article 413-9 du code pénal énonce ainsi que présentent un caractère de secret de la défense nationale toutes les informations, quel que soit leur support, « *qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès* ».

Compte tenu de cette articulation malaisée, l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale prescrit, avant toute communication d'un document portant un timbre de classification, une opération formelle de déclassification par application d'un timbre spécifique. Cette opération de déclassification préalable est toutefois à l'origine de retards parfois importants dans l'instruction des demandes de communication.

C'est afin de mettre un terme à cette situation, qui obère les ressources des services d'archives et rend difficiles certains travaux de recherche historique portant sur l'époque contemporaine, qu'il est proposé de revoir l'articulation entre les deux codes afin de prévoir qu'en principe, les documents protégés par le secret de la défense nationale deviennent communicables sans déclassification préalable à l'issue d'un délai de 50 ans.

Le 3° du I de l'article L. 213-2 est d'abord modifié pour faire correspondre la désignation d'un document classifié à la définition de référence qu'en donne le code pénal. Il est par ailleurs complété pour prévoir que, pour certaines catégories de documents dont la sensibilité peut perdurer malgré l'écoulement du temps, la fin de l'incommunicabilité est reportée

au-delà du délai de cinquante, jusqu'à un terme précisément défini : il s'agit notamment, pour les documents relatifs aux caractéristiques techniques des ouvrages nucléaires civils ou des installations utilisées pour la détention des personnes, de la fin de leur utilisation, constatée par un acte publiée, ou encore, pour les documents relatifs à la protection des moyens de la dissuasion nucléaire, de la perte de leur valeur opérationnelle.

En outre, un III est introduit afin de poser le principe de la coïncidence entre la communicabilité et la déclassification automatique. Cette disposition est de nature à fluidifier la transmission aux historiens des documents classifiés ayant atteint le terme de l'incommunicabilité, dès lors qu'elle supprime toute nécessité d'une opération formelle de déclassification. Une disposition transitoire précise enfin que les documents non-classifiés qui sont actuellement communicables le demeureront à l'avenir, quand bien même ils relèveraient des nouveaux délais d'incommunicabilité qui sont institués.

Le chapitre III, constitué d'un unique **article 18**, tire la conséquence du développement du trafic aérien des aéronefs sans personnes à bord, qui soulève d'importants enjeux de sécurité publique et de défense. En effet, ces appareils sont susceptibles d'être équipés de dispositifs d'attaque ou de captation d'images employés à des fins malveillantes. Pour parer à cette menace émergente, il modifie l'article L. 33-3-1 du code des postes et des communications électroniques pour prévoir les conditions dans lesquelles l'autorité administrative peut recourir, sur le territoire national, à des opérations de brouillage des aéronefs sans personne à bord, usuellement dénommés drones, afin de prévenir les menaces susceptibles d'affecter la sécurité de grands événements (sommets internationaux, manifestations sportives) ou de certains convois (convois officiels, convois de matières dangereuses…). Il prévoit en outre la possibilité de procéder à de telles opérations de brouillage en cas de survol par un drone d'une zone faisant l'objet d'une interdiction permanente ou temporaire de circulation aérienne sur le fondement de l'article L. 6211-4 du code des transports. Il dispose en outre que la mise en œuvre du brouillage, dont les modalités précises sont renvoyées à un décret en Conseil d'Etat, doivent être strictement proportionnée à ces finalités. Enfin, il renvoie également à un décret en Conseil d'Etat la détermination des autorités compétentes pour y procéder.

Enfin, le chapitre V, composé des **articles 20 à 29**, concerne l'application outre-mer des dispositions du projet de loi.

CHAPITRE IER

Dispositions renforçant la prévention d'actes de terrorisme

Article 1er

Le II de l'article 5 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme est abrogé.

Article 2

① Le chapitre VII du titre II du livre II du code de la sécurité intérieure est ainsi modifié :

② 1° L'article L. 227-1 est ainsi modifié :

③ *a)* Au début du premier alinéa, est ajoutée la mention : « I. – » ;

④ *b)* Il est ajouté un II ainsi rédigé :

⑤ « II. – Peuvent également faire l'objet d'une mesure de fermeture, selon les modalités prévues aux deux derniers alinéas du I, des locaux dépendant du lieu de culte dont la fermeture est prononcée sur le fondement du I et dont il existe des raisons sérieuses de penser qu'ils seraient utilisés aux mêmes fins pour faire échec à l'exécution de cette mesure. La fermeture de ces locaux prend fin à l'expiration de la mesure de fermeture du lieu de culte. » ;

⑥ 2° À l'article L. 227-2, après les mots : « lieu de culte », sont insérés les mots : « ou d'un lieu en dépendant ».

Article 3

① Le chapitre VIII du titre II du livre II du code de la sécurité intérieure est ainsi modifié :

② 1° L'article L. 228-2 est ainsi modifié :

③ *a)* Au 3°, après le mot : « Déclarer », sont insérés les mots : « et fournir un justificatif de » et le mot : « et » est remplacé par les mots : « ainsi que de » ;

④ *b)* Après le 3°, il est inséré un alinéa ainsi rédigé :

⑤ « L'obligation prévue au 1° peut être assortie d'une interdiction de paraître dans un ou plusieurs lieux déterminés se trouvant au sein du périmètre géographique de cette obligation et dans lesquels se tient un événement exposé, par son ampleur ou ses circonstances particulières, à un risque de menace terroriste. Cette interdiction tient compte de la vie familiale et professionnelle de la personne. Sa durée est strictement limitée à celle de l'événement, dans la limite de trente jours. Sauf urgence dûment justifiée, elle doit être notifiée à la personne concernée au moins quarante-huit heures avant son entrée en vigueur. » ;

⑥ 2° Au 1° de l'article L. 228-4, après le mot : « Déclarer », sont insérés les mots : « et fournir un justificatif de » et le mot : « et » est remplacé par les mots : « ainsi que de » ;

⑦ 3° Après le cinquième alinéa de l'article L. 228-2, le cinquième alinéa de l'article L. 228-4 et le deuxième alinéa de l'article L. 228-5, il est inséré un alinéa ainsi rédigé :

⑧ « Par dérogation à la durée totale cumulée de douze mois prévue à l'alinéa précédent, lorsque ces obligations sont prononcées dans un délai de six mois à compter de la libération d'une personne condamnée à une peine privative de liberté non assortie du sursis d'une durée supérieure ou égale à cinq ans pour l'une des infractions mentionnées aux articles 421-1 à 421-6 du code pénal, à l'exception de celles définies aux articles 421-2-5 et 421-2-5-1 du même code, ou d'une durée supérieure ou égale à trois ans lorsque l'infraction a été commise en état de récidive légale, et si les conditions prévues à l'article L. 228-1 continuent d'être réunies, la durée totale cumulée de ces obligations peut atteindre vingt-quatre mois. Pour les douze premiers mois de sa mise en œuvre, la mesure est renouvelée dans les conditions prévues au deuxième alinéa ; chaque renouvellement au-delà est subordonné à l'existence d'éléments nouveaux et complémentaires. » ;

⑨ 4° Après le sixième alinéa de l'article L. 228-2, le sixième alinéa de l'article L. 228-4 et le troisième alinéa de l'article L. 228-5, il est inséré un alinéa ainsi rédigé :

⑩ « En cas de saisine d'un tribunal territorialement incompétent, le délai de jugement de soixante-douze heures court à compter de l'enregistrement de la requête par le tribunal auquel celle-ci a été renvoyée. La mesure en cours demeure en vigueur jusqu'à l'expiration de ce délai, et au plus pour une durée maximale de sept jours à compter de son terme initial. La décision de renouvellement ne peut entrer en vigueur avant que le juge ait statué sur la demande. » ;

⑪ 5° Après la première phrase de l'article L. 228-6, est insérée une phrase ainsi rédigée :

⑫ « La définition des obligations prononcées sur le fondement de ces dispositions tient compte, dans le respect des principes de nécessité et de proportionnalité, des obligations déjà prescrites par l'autorité judiciaire. » ;

⑬ 6° Les mesures prononcées sur le fondement des articles L. 228-1 et suivants du code de la sécurité intérieure en cours à la date de promulgation de la présente loi et dont le terme survient moins de sept jours après cette promulgation demeurent en vigueur sept jours à compter de ce terme, si le ministre de l'intérieur a procédé au plus tard au lendemain de la publication de la présente loi, à la notification de leur renouvellement selon la procédure prévue aux huitième et neuvième alinéas de l'article L. 228-2, aux septième et huitième alinéas de l'article L. 228-4 et aux quatrième et cinquième alinéa de l'article L. 228-5.

Article 4

① Au chapitre IX du titre II du livre II du code de la sécurité intérieure, après le premier alinéa du I de l'article L. 229-5, il est inséré un alinéa ainsi rédigé :

② « Lorsque la personne mentionnée au troisième alinéa de l'article L. 229-2 fait obstacle à l'accès aux données contenues dans tout système informatique ou équipement terminal présent sur les lieux de la visite, mention en est faite au procès-verbal prévu au même article. Il peut alors être procédé à la saisie de ces supports, dans les conditions prévues au I du présent article. »

Article 5

① Le titre XV du livre IV du code de procédure pénale est complété par une section 5 ainsi rédigée :

②

« Section 5

③

« De la mesure judiciaire de prévention de la récidive terroriste et de réinsertion

④ « *Art. 706-25-16.* – I. – Lorsqu'une personne a été condamnée à une peine privative de liberté non assortie du sursis d'une durée supérieure ou égale à cinq ans pour une ou plusieurs des infractions mentionnées aux

articles 421-1 à 421-6 du code pénal, à l'exclusion de celles définies aux articles 421-2-5 et 421-2-5-1 du même code, ou d'une durée supérieure ou égale à trois ans lorsque l'infraction a été commise en état de récidive légale, et qu'il est établi, à l'issue d'un réexamen de sa situation intervenant à la fin de l'exécution de sa peine, qu'elle présente une particulière dangerosité caractérisée par une probabilité très élevée de récidive et par une adhésion persistante à une idéologie ou à des thèses incitant à la commission d'actes de terrorisme, faisant ainsi obstacle à sa réinsertion, le tribunal de l'application des peines de Paris peut, sur réquisitions du procureur de la République antiterroriste, ordonner, aux seules fins de prévenir la récidive et d'assurer la réinsertion, une mesure judiciaire de prévention de la récidive terroriste et de réinsertion.

⑤ « La décision définit les conditions d'une prise en charge sanitaire, sociale, éducative ou psychologique, destinée à permettre la réinsertion et l'acquisition des valeurs de la citoyenneté. Cette prise en charge peut, le cas échéant, intervenir au sein d'un établissement d'accueil adapté

⑥ « Elle peut imposer à l'intéressé d'exercer une activité professionnelle, de suivre un enseignement ou une formation professionnelle ; elle peut également lui interdire de se livrer à l'activité dans l'exercice ou à l'occasion de laquelle l'infraction a été commise.

⑦ « La décision précise les conditions dans lesquelles l'intéressé doit communiquer au service pénitentiaire d'insertion et de probation les renseignements ou documents de nature à permettre le contrôle de ses moyens d'existence et de l'exécution de ses obligations, et répondre aux convocations du juge de l'application des peines ou du service pénitentiaire d'insertion et de probation. Elle peut aussi l'astreindre à établir sa résidence en un lieu déterminé.

⑧ « Les obligations auxquelles la personne concernée est astreinte sont mises en œuvre par le juge de l'application des peines du tribunal judiciaire de Paris assisté du service pénitentiaire d'insertion et de probation et, le cas échéant, avec le concours des organismes habilités à cet effet.

⑨ « II. – Le tribunal de l'application des peines de Paris ne peut prononcer la mesure judiciaire de prévention de la récidive terroriste et de réinsertion qu'après s'être assuré que la personne condamnée a été mise en mesure de bénéficier, pendant l'exécution de sa peine, de mesures de nature à favoriser sa réinsertion.

⑩ « III. – La mesure judiciaire de prévention de la récidive terroriste et de réinsertion prévue au I peut être ordonnée pour une période d'une durée maximale d'un an. À l'issue de cette période, la mesure peut être renouvelée sur réquisitions du procureur de la République antiterroriste par le tribunal de l'application des peines de Paris, après avis de la commission pluridisciplinaire des mesures de sûreté, et pour au plus la même durée, périodes de suspension comprises, dans la limite de cinq ans ou, lorsque le condamné est mineur, dans la limite de trois ans. Chaque renouvellement est subordonné à l'existence d'éléments nouveaux ou complémentaires.

⑪ « IV. – La mesure prévue au I ne peut être ordonnée que si cette mesure apparaît strictement nécessaire pour prévenir la récidive et assurer la réinsertion. Elle n'est pas applicable si la personne a été condamnée à un suivi socio-judiciaire en application de l'article 421-8 du code pénal ou si elle fait l'objet d'une mesure de surveillance judiciaire prévue à l'article 723-29 du présent code, d'une mesure de surveillance de sûreté prévue à l'article 706-53-19 ou d'une rétention de sûreté prévue à l'article 706-53-13.

⑫ « *Art. 706-25-17.* – La situation des personnes détenues susceptibles de faire l'objet de la mesure prévue à l'article 706-25-16 est examinée, sur réquisitions du procureur de la République antiterroriste, au moins trois mois avant la date prévue pour leur libération par la commission pluridisciplinaire des mesures de sûreté prévue à l'article 763-10, afin d'évaluer leur dangerosité et leur capacité à se réinsérer.

⑬ « À cette fin, la commission demande le placement de la personne concernée, pour une durée d'au moins six semaines, dans un service spécialisé chargé de l'observation des personnes détenues aux fins notamment d'une évaluation pluridisciplinaire de dangerosité.

⑭ « À l'issue de cette période, la commission adresse au tribunal de l'application des peines de Paris et à la personne concernée un avis motivé sur la pertinence de prononcer la mesure mentionnée à l'article 706-25-16 au vu des critères définis au I du même article.

⑮ « *Art. 706-25-18.* – La décision prévue à l'article 706-25-16 est prise, avant la date prévue pour la libération du condamné, par un jugement rendu après un débat contradictoire et, si le condamné le demande, public, au cours duquel le condamné est assisté par un avocat choisi ou commis d'office. Elle doit être spécialement motivée au regard des conclusions de l'évaluation et de l'avis mentionnés à l'article 706-25-17, ainsi que des conditions mentionnées au V de l'article 706-25-16.

⑯ « Le jugement précise les obligations auxquelles le condamné est tenu ainsi que la durée de celles-ci.

⑰ « La décision est exécutoire immédiatement à l'issue de la libération.

⑱ « Le tribunal de l'application des peines de Paris peut, sur réquisitions du procureur de la République antiterroriste ou à la demande de la personne concernée, selon les modalités prévues à l'article 706-53-17 et, le cas échéant, après avis du procureur de la République antiterroriste, modifier la mesure ou ordonner sa mainlevée. Cette compétence s'exerce sans préjudice de la possibilité, pour le juge de l'application des peines, d'adapter à tout moment les obligations de la mesure.

⑲ « *Art. 706-25-19.* – Les décisions du tribunal de l'application des peines de Paris prévues à la présente section peuvent faire l'objet du recours prévu au second alinéa de l'article 712-1.

⑳ « *Art. 706-25-20.* – Les obligations prévues à l'article 706-25-16 sont suspendues par toute détention intervenue au cours de leur exécution.

㉑ « Si la détention excède une durée de six mois, la reprise d'une ou de plusieurs des obligations prévues au même article 706-25-16 doit être confirmée par le tribunal de l'application des peines de Paris au plus tard dans un délai de trois mois après la cessation de la détention, à défaut de quoi il est mis fin d'office à la mesure.

㉒ « *Art. 706-25-21.* – Le fait pour la personne soumise à une mesure prise en application de l'article 706-25-16 de ne pas respecter les obligations auxquelles elle est astreinte est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

㉓ « *Art. 706-25-22.* – Un décret en Conseil d'État précise les conditions et les modalités d'application de la présente section. »

Article 6

① Au chapitre I^{er} du titre I^{er} du livre II de la troisième partie du code de la santé publique, il est inséré un article L. 3211-12-7 ainsi rédigé :

② « *Art. L. 3211-12-7.* – Aux seules fins d'assurer le suivi d'une personne qui représente une menace grave pour la sécurité et l'ordre publics à raison de sa radicalisation à caractère terroriste, le représentant de l'État dans le département et, à Paris, le préfet de police, ainsi que ceux des services de

renseignement mentionnés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure désignés à cette fin par un décret en Conseil d'État, peuvent se voir communiquer les informations strictement nécessaires à l'accomplissement de leurs missions portées à la connaissance du représentant de l'État dans le département d'hospitalisation ou, à Paris, du préfet de police en application des articles L. 3212-5, L. 3212-8 et L. 3213-9 du présent code et de l'article 706-135 du code de procédure pénale, sans que ces informations puissent porter sur des faits antérieurs de plus de trois ans à compter de la date de levée de la mesure de soins sans consentement. »

CHAPITRE II

Dispositions relatives au renseignement

Article 7

① I. – L'article L. 822-3 du code de la sécurité intérieure est ainsi modifié :

② 1° Au premier alinéa est ajoutée, au début, la mention : « I. – » et les mots : « ou extraits » sont remplacés par les mots : « , extraits ou transmis » ;

③ 2° La seconde phrase du premier alinéa est supprimée ;

④ 3° Après le premier alinéa, sont insérés sept alinéas ainsi rédigés :

⑤ « 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.

⑥ « II. – Sous réserve des dispositions des deuxième à quatrième alinéas du présent II, 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 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.

⑦ « Sont subordonnées à une autorisation préalable du Premier ministre après avis de la Commission nationale de contrôle des techniques de

renseignement, délivrée dans les conditions de forme et de procédure prévues aux articles L. 821-1 à L. 821-5 :

⑧ « 1° Les transmissions de renseignements collectés, lorsqu'elles poursuivent une finalité différente de celle qui en a justifié le recueil ;

⑨ « 2° Les transmissions de renseignements collectés, extraits ou transcrits qui sont issus de la mise en œuvre d'une technique de recueil de renseignement à laquelle le service destinataire n'aurait pu recourir au titre de la finalité motivant la transmission.

⑩ « 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. A l'issue de cette durée, chaque service procède à la destruction des renseignements selon les modalités définies à l'article L. 822-4.

⑪ « Le responsable de chaque service spécialisé de renseignement mentionné à l'article L. 811-2 ou de chaque service désigné par le décret en Conseil d'État prévu à l'article L. 811-4 désigne un agent chargé de veiller, sous son contrôle, au respect de l'application des dispositions du présent II. Ce dernier est informé par ses homologues dans les autres services de la destruction, dans les conditions fixées au cinquième alinéa du présent II, des renseignements que le service auprès duquel il a été placé a été autorisé à recueillir. Il rend compte sans délai au responsable du service auprès duquel il est placé de toute difficulté dans l'application du présent II. » ;

⑫ 3° Au début du dernier alinéa, est ajoutée la mention : « III. – » et les mots : « de ces finalités » sont remplacés par les mots : « des finalités mentionnées au I » ;

⑬ 4° Il est ajouté un IV ainsi rédigé :

⑭ « IV. – Les opérations mentionnées aux I à III sont soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement. »

⑮ II. – L'article L. 822-4 du même code est ainsi rédigé :

⑯ « *Art. L. 822-4.* – Les opérations de destruction des renseignements collectés mentionnées à l'article L. 822-2, les transcriptions et les extractions ainsi que les transmissions mentionnées au II de l'article L. 822-3 sont effectuées par des agents individuellement désignés et habilités. Elles font l'objet de relevés tenus à la disposition de la Commission nationale de contrôle des techniques de renseignement qui précisent :

⑰ « 1° S'agissant des transcriptions ou des extractions, si elles ont été effectuées pour une finalité différente de celle qui en a justifié le recueil ;

⑱ « 2° S'agissant des transmissions, leur nature, leur date et leur finalité ainsi que le ou les services qui en ont été destinataires.

⑲ « Lorsque les transcriptions, extractions ou les transmissions poursuivent une finalité différente de celle au titre de laquelle les renseignements ont été recueillis, les relevés sont immédiatement transmis à la Commission nationale de contrôle des techniques de renseignement. »

⑳ III. – Au 2° de l'article L. 833-2 du même code, les mots : « et extractions » sont remplacés par les mots : « , extractions et transmissions ».

㉑ IV. – L'article L. 854-6 du même code est ainsi modifié :

㉒ 1° Après le deuxième alinéa, il est inséré un alinéa ainsi rédigé :

㉓ « Un service spécialisé de renseignement mentionné à l'article L. 811-2 peut, dans les conditions définies aux quatre premiers alinéas du II de l'article L. 822-3, transmettre tout renseignement transcrit ou extrait à un autre de ces services ou à un service désigné par le décret en Conseil d'État prévu à l'article L. 811-4. » ;

㉔ 2° Le dernier alinéa est ainsi rédigé :

㉕ « Les opérations de destruction des renseignements collectés, les transcriptions, les extractions et les transmissions sont effectuées dans les conditions prévues à l'article L. 822-4. »

㉖ V. – Au premier alinéa de l'article L. 854-9, les mots : « et extractions » sont remplacés par les mots : « , extractions et transmissions ».

㉗ VI. – Au 3° de l'article L. 833-6 du même code, les mots : « ou la destruction » sont remplacés par les mots : « , la destruction » et après les mots : « renseignements collectés », sont insérés les mots : « ou leur transmission entre services ».

㉘ VII. – L'article L. 863-2 du même code est ainsi modifié :

㉙ 1° Le premier et le dernier alinéas sont supprimés ;

㉚ 2° Le deuxième alinéa est remplacé par cinq alinéas ainsi rédigés :

(31) « Les autorités administratives mentionnées à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives peuvent transmettre aux services spécialisés de renseignement mentionnés à l'article L. 811-2 et aux services désignés par le décret en Conseil d'État prévu à l'article L. 811-4, de leur propre initiative ou sur requête de ces derniers, toute information même couverte par un secret protégé par la loi, strictement nécessaire à l'accomplissement des missions de ces services et susceptible de concourir à la défense et la promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3.

(32) « Les informations mentionnées au premier alinéa sont détruites dès lors qu'elles ne sont pas ou plus nécessaires à l'accomplissement des missions du service auquel elles ont été transmises.

(33) « Les conditions dans lesquelles la traçabilité des transmissions mentionnées au premier alinéa est mise en œuvre dans les traitements de données à caractère personnel des autorités administratives mentionnées au même alinéa sont, le cas échéant, fixées par décret.

(34) « Toute personne qui en est rendue destinataire est tenue au secret professionnel, dans les conditions et sous les peines prévues aux articles 226-13 et 226-14 du code pénal.

(35) « L'agent mentionné au sixième alinéa du II de l'article L. 822-3 est chargé d'assurer une traçabilité de ces transmissions et de veiller au respect de l'application des dispositions du présent article. »

(36) VIII. – L'article L. 135 S du livre des procédures fiscales et l'article 22 de la loi n° 2007-1824 du 25 décembre 2007 de finances rectificative pour 2007 sont abrogés.

(37) IX. – La loi n° 78-17 du 6 janvier 1978 est ainsi modifiée :

(38) 1° À l'article 48 est ajouté un dernier alinéa ainsi rédigé :

(39) « Les dispositions du premier alinéa ne s'appliquent pas à l'information selon laquelle des données à caractère personnel ont été transmises en application du premier alinéa de l'article L. 863-2 du code de la sécurité intérieure. » ;

(40) 2° Le dernier alinéa de l'article 49 est ainsi rédigé :

(41) « Les dispositions du premier alinéa ne s'appliquent pas :

(42) « 1° Lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée et à la protection des données des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de réalisation de recherche scientifique ou historique ;

(43) « 2° À l'information selon laquelle des données à caractère personnel ont été transmises en application du premier alinéa de l'article L. 863-2 du code de la sécurité intérieure. »

Article 8

(1) I. – L'article L. 822-2 du code de la sécurité intérieure est complété par un III ainsi rédigé :

(2) « III. – Aux seules fins de recherche et développement en matière de capacités techniques de recueil et d'exploitation des renseignements et à l'exclusion de toute utilisation pour la surveillance des personnes concernées, les services spécialisés de renseignement mentionnés à l'article L. 811-2 peuvent conserver au-delà des durées prévues au présent article les renseignements mentionnés au I. Cette conservation 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.

(3) « Les renseignements mentionnés au premier alinéa du présent III sont conservés de manière à ce qu'ils ne soient accessibles qu'aux seuls agents spécialement habilités à cet effet et exclusivement affectés à cette mission et dans des conditions ne faisant plus apparaître les motifs et finalités pour lesquels ils ont été collectés et ne permettant pas de rechercher l'identité des personnes concernées.

(4) « Les paramètres techniques applicables à chaque programme de recherche afin de garantir le respect des conditions prévues aux alinéas précédents, ainsi que toute évolution substantielle de ces paramètres sont soumis à une autorisation préalable du Premier ministre délivrée après avis de la Commission nationale de contrôle des techniques de renseignement.

(5) « Les renseignements mentionnés au premier alinéa du présent III sont détruits dès que leur conservation n'est plus indispensable à la validation de capacités techniques de recueil et d'exploitation mentionnées au premier alinéa et, au plus tard, cinq ans après leur recueil.

⑥ « La Commission nationale de contrôle des techniques de renseignement veille à ce que la mise en œuvre des programmes de recherche respecte les conditions prévues au présent III. Elle peut adresser au Premier ministre une recommandation tendant à la suspension d'un programme de recherche dont elle estime qu'il ne respecte plus ces conditions. »

⑦ II. – Après l'article L. 822-2 du même code, il est inséré un article L. 822-2-1 ainsi rédigé :

⑧ « *Art. L. 822-2-1.* – Le service du Premier ministre mentionné aux articles L. 851-1, L. 851-3, L. 851-4, L. 851-6 et L. 852-1 peut conserver, dans les conditions prévues au III de l'article L. 822-2 et avec l'accord du ou des services pour lesquels ces renseignements ont été collectés, les renseignements mentionnés au I du même article dont il organise la centralisation. »

⑨ III. – Après les mots « présent livre », le 2° de l'article 833-2 du même code est ainsi rédigé : « aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements en application de l'article L. 822-1 ainsi qu'aux renseignements mentionnés au III de l'article L. 822-2 ».

Article 9

La première phrase du II de l'article L. 853-2 du code de la sécurité intérieure est ainsi rédigée : « Par dérogation à l'article L. 821-4, l'autorisation de mise en œuvre des techniques mentionnées au I est délivrée pour une durée maximale de deux mois. »

Article 10

① I. – À l'article L. 871-3 du code de la sécurité intérieure, les mots : « et de la section 3 du chapitre I^{er} du titre III du livre I^{er} du code de procédure pénale relatives aux interceptions de correspondances émises par la voie des télécommunications ordonnées par l'autorité judiciaire » sont remplacés par les mots : « , de la section 3 du chapitre I^{er} du titre III du livre I^{er} du code de procédure pénale relatives aux interceptions de correspondances émises par la voie des télécommunications ordonnées par l'autorité judiciaire et des sections 5 et 6 du chapitre II du titre XXV du livre IV du code de procédure pénale ».

② II. – À l'article L. 871-6 du même code, les mots : « aux articles L. 851-1 à L. 851-4 et L. 852-1 » sont remplacés par les mots : « aux articles L. 851-1 à L. 851-4, L. 851-6, L. 852-1 et L. 853-2 ».

③ III. – À l'article L. 871-7 du même code, les mots : « et L. 852-1 » sont remplacés par les mots : « , L. 851-6, L. 852-1 et L. 853-2 ».

Article 11

① I. – Le code de la sécurité intérieure est ainsi modifié :

② 1° Au 1° du I de l'article L. 822-2, les mots : « et L. 852-2 » sont remplacés par les mots : « , L. 852-2 et L. 852-3 » ;

③ 2° Après l'article L. 852-2, il est inséré un article L. 852-3 ainsi rédigé :

④ « *Art. L. 852-3.* – I. – Dans les conditions prévues au chapitre I[er] du titre II du présent livre et pour les seules finalités prévues aux 1°, 2°, 4° et 6° de l'article L. 811-3, peut être autorisée l'utilisation d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal afin d'intercepter des correspondances émises ou reçues par la voie satellitaire, lorsque cette interception ne peut être mise en œuvre sur le fondement du I de l'article L. 852-1 du présent code**,** pour des raisons techniques ou pour des motifs de confidentialité faisant obstacle au concours des opérateurs ou des personnes mentionnés à l'article L. 851-1. Les correspondances interceptées dans ce cadre sont détruites dès qu'il apparaît qu'elles sont sans lien avec la personne concernée par l'autorisation, et au plus tard au terme du délai prévu au 1° du I de l'article L. 822-2.

⑤ « II. – Par dérogation à l'article L. 821-4, l'autorisation est délivrée pour une durée maximale de trente jours, renouvelable dans les mêmes conditions de durée. Elle vaut autorisation de recueil des informations ou documents mentionnés à l'article L. 851-1 associés à l'exécution de l'interception et à son exploitation.

⑥ « III. – Un service du Premier ministre organise la centralisation des correspondances interceptées et des informations ou documents recueillis en application des I et II du présent article. Cette centralisation intervient dès l'interception des communications, sauf impossibilité technique. Dans ce cas, les données collectées font l'objet d'un chiffrement dès leur collecte et jusqu'à leur centralisation effective au sein du service du Premier ministre mentionné au présent alinéa. La demande prévue à l'article L. 821-2 précise

les motifs faisant obstacle à la centralisation immédiate des correspondances interceptées.

⑦ « Les opérations de transcription et d'extraction des communications interceptées, auxquelles la Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat, sont effectuées au sein du service du Premier ministre mentionné à l'alinéa précédent.

⑧ « IV. – Le nombre maximal des autorisations d'interception en vigueur simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 ainsi que le nombre d'autorisations d'interception délivrées sont portés à la connaissance de la commission.

⑨ « V. – Un décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement, désigne les services 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, au regard des missions qu'ils exercent, peuvent être autorisés à recourir à la technique prévue au I. »

⑩ II. – Le I est applicable jusqu'au 31 juillet 2025. Le Gouvernement adresse au Parlement un rapport d'évaluation sur l'application de cette disposition au plus tard six mois avant cette échéance.

Article 12

L'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement est abrogé.

Article 13

① L'article L. 851-3 du code de la sécurité intérieure est ainsi modifié :

② 1° Le I est ainsi modifié :

③ *a)* Au premier alinéa, les mots : « il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de » sont remplacés par les mots : « peuvent être autorisés, à la demande des services spécialisés de renseignement mentionnés à l'article

L. 811-2, sur les données transitant par les réseaux des opérateurs et des personnes mentionnées à l'article L. 851-1, des » ;

④ *b)* Au deuxième alinéa, après les mots : « à l'article L. 851-1 », sont insérés les mots : « ainsi que les adresses complètes de ressources utilisées sur internet » et les mots : « ou documents se rapportent » sont remplacés par les mots : « , documents ou adresses se rapportent » ;

⑤ 2° Au III, les mots : « pour cette mise en œuvre » sont supprimés ;

⑥ 3° Le IV est ainsi modifié :

⑦ *a)* Les mots : « sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste attachée à une ou plusieurs des personnes concernées » sont supprimés ;

⑧ *b)* Il est inséré un deuxième alinéa ainsi rédigé :

⑨ « Les données non détectées par les traitements comme susceptibles de révéler une menace à caractère terroriste sont détruites immédiatement. » ;

⑩ 4° Il est ajouté un VI ainsi rédigé :

⑪ « VI. – Un service du Premier ministre est seul habilité à exécuter les traitements et opérations mis en œuvre sur le fondement des I et IV, sous le contrôle de la Commission nationale de contrôle des techniques de renseignement. »

Article 14

① Le code de la sécurité intérieure est ainsi modifié :

② 1° Au I de l'article L. 851-2, la première phrase est complétée par les mots : « , ainsi que les adresses complètes de ressources sur internet utilisées par cette personne » ;

③ 2° Au 2° du I de l'article L. 822-2, après les mots : « de leur recueil pour », sont insérés les mots : « les adresses complètes de ressources sur internet recueillies par la mise en œuvre de la technique prévue à l'article L. 851-2 et ».

Article 15

① I. – L'article L. 34-1 du code des postes et des communications électroniques est ainsi modifié :

② 1° Au II, les mots : « toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI » sont remplacés par les mots : «, sous réserve des dispositions des II *bis* à VI, les données relatives aux communications électroniques » ;

③ 2° Après le II, il est inséré un II *bis* ainsi rédigé :

④ « II *bis*. – Les opérateurs de communications électroniques sont tenus de conserver :

⑤ « 1° 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, les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans après la fin de validité de son contrat ;

⑥ « 2° Pour les mêmes finalités que celles énoncées au 1°, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte, ainsi que les informations relatives au paiement, jusqu'à l'expiration d'un délai d'un an après la fin de validité de son contrat ou la clôture de son compte ;

⑦ « 3° Pour les besoins de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les données techniques permettant d'identifier la source de la connexion ou relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux. » ;

⑧ 3° Le III est remplacé par les dispositions suivantes :

⑨ « III. – Pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible contre cette dernière, le Premier ministre peut enjoindre aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic et de localisation, en complément de celles mentionnées au II *bis*.

⑩ « L'injonction du Premier ministre, qui prend la forme d'un décret dont la durée d'application ne peut excéder un an, peut être renouvelée si les

conditions prévues pour son édiction continuent d'être réunies. Son expiration est sans incidence sur la durée de conservation des données mentionnées à l'alinéa précédent. » ;

⑪ 4° Il est inséré après le III un III *bis* ainsi rédigé :

⑫ « III *bis*. – Les données, telles que mentionnées au présent article, conservées par les opérateurs peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant en vertu de la loi d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect afin d'y accéder. » ;

⑬ 5° Au V, les mots : « et sous réserve des nécessités des enquêtes judiciaires » sont supprimés ;

⑭ 6° Le VI est ainsi modifié :

⑮ *a)* Au premier alinéa, les mots : « aux III, IV et V » sont remplacés par les mots : « aux II bis à V » ;

⑯ *b)* Après le deuxième alinéa, il est inséré un alinéa ainsi rédigé :

⑰ « Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, détermine, selon l'activité des opérateurs et la nature des communications, les informations et catégories de données conservées en application des II *bis* et III, ainsi que les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs. »

⑱ II. – Le II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est ainsi modifié :

⑲ 1° Au premier alinéa, les mots : « Les personnes mentionnées aux 1 et 2 du I » sont remplacés par les mots : « Dans les conditions fixées aux II *bis*, II et III *bis* de l'article L. 34-1 du code des postes et communications électroniques, les personnes mentionnées aux 1 et 2 du I du présent article » ;

⑳ 2° Les troisième et quatrième alinéas sont supprimés.

Article 16

① Le code de la sécurité intérieure est ainsi modifié :

② 1° L'article L. 821-1 est ainsi modifié :

③ *a)* Après le premier alinéa, il est inséré un alinéa ainsi rédigé :

④ « Lorsque l'autorisation est délivrée après avis défavorable de la Commission nationale de contrôle des techniques de renseignement, le Conseil d'État est immédiatement saisi par le président de la commission ou, à défaut, par l'un des membres de la commission parmi ceux mentionnés aux 2° et 3° de l'article L. 831-1 du présent code. 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 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. » ;

⑤ *b)* Au deuxième alinéa, les mots : « Ces techniques » sont remplacés par les mots : « Les techniques de recueil de renseignement » ;

⑥ 2° L'article L. 821-5 est abrogé ;

⑦ 3° L'article L. 821-7 est ainsi modifié :

⑧ *a)* La dernière phrase du premier alinéa est supprimée ;

⑨ *b)* Après le premier alinéa, il est inséré un deuxième alinéa ainsi rédigé :

⑩ « Le caractère d'urgence mentionné à la troisième phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué pour les autorisations concernant l'une des personnes mentionnées au premier alinéa du présent article ou ses véhicules, ses bureaux ou ses domiciles. » ;

⑪ 4° L'article L. 833-9 est ainsi modifié :

⑫ *a)* Le sixième alinéa est supprimé ;

⑬ *b)* Au septième alinéa, la numérotation : « 6° » est remplacée par la numérotation : « 5° » ;

⑭ 5° Le II de l'article L. 851-2 est abrogé ;

⑮ 6° Le V de l'article L. 851-3 est remplacé par les dispositions suivantes :

⑯ « V. – Le caractère d'urgence mentionné à la troisième phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué pour les autorisations délivrées sur le fondement des I et II du présent article. » ;

⑰ 7° Après le IV de l'article L. 853-1, il est inséré un IV *bis* ainsi rédigé :

⑱ « IV *bis*. – Le caractère d'urgence mentionné à la troisième phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué que si l'autorisation a été délivrée au titre du 1°, du 4° ou du *a* du 5° de l'article L. 811-3. » ;

⑲ 8° Après le IV de l'article L. 853-2, il est inséré un IV *bis* ainsi rédigé :

⑳ « IV *bis*. – Le caractère d'urgence mentionné à la troisième phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué que si l'autorisation a été délivrée au titre du 1°, du 4° ou du *a* du 5° de l'article L. 811-3. » ;

㉑ 9° Le second alinéa du III de l'article L. 853-3 est remplacé par les dispositions suivantes :

㉒ « Le caractère d'urgence mentionné à la troisième phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué que si l'autorisation a été délivrée au titre du 1°, du 4° ou du *a* du 5° de l'article L. 811-3. Lorsque l'introduction mentionnée au I du présent article porte sur un lieu privé à usage d'habitation, le caractère d'urgence ne peut être invoqué que si l'autorisation a été délivrée au titre du 4° de l'article L. 811-3. »

Article 17

① La section 8 du chapitre II du titre XXV du livre IV du code de procédure pénale est complétée par un article 706-105-1 ainsi rédigé :

② « *Art. 706-105-1*. – I. – Par dérogation à l'article 11, le procureur de la République de Paris peut, pour les procédures d'enquête ou d'instruction entrant dans le champ d'application de l'article 706-72-1, communiquer aux services de l'État mentionnés au second alinéa de l'article L. 2321-2 du code de la défense, de sa propre initiative ou à la demande de ces services, des éléments de toute nature figurant dans ces procédures et nécessaires à l'exercice de leur mission en matière de sécurité et de défense des systèmes d'information. Si la procédure fait l'objet d'une information, cette

communication ne peut intervenir qu'avec l'avis favorable du juge d'instruction.

③ « Le juge d'instruction peut également procéder à cette communication dans les mêmes conditions et pour les mêmes finalités que celles mentionnées au précédent alinéa pour les procédures d'information dont il est saisi après avoir recueilli l'avis du procureur de la République de Paris.

④ « II. – Par dérogation à l'article 11, le procureur de la République de Paris peut, pour les procédures d'enquête ou d'instruction relevant de la compétence des juridictions mentionnées au quatrième alinéa de l'article 706-75 et portant sur les infractions mentionnées aux 3°, 5°, 12° et 13° de l'article 706-73 ainsi qu'au blanchiment de ces infractions, communiquer aux services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure ainsi qu'aux services mentionnés à l'article L. 811-4 du même code désignés, au regard de leurs missions, par décret en Conseil d'État, de sa propre initiative ou à la demande de ces services, des éléments de toute nature figurant dans ces procédures et nécessaires à l'exercice des missions de ces services au titre de la prévention de la criminalité et de la délinquance organisées. Si la procédure fait l'objet d'une information, cette communication ne peut intervenir qu'avec l'avis favorable du juge d'instruction.

⑤ « Le juge d'instruction peut également procéder à cette communication dans les mêmes conditions et pour les mêmes finalités que celles mentionnées au précédent alinéa pour les procédures d'information dont il est saisi après avoir recueilli l'avis du procureur de la République de Paris.

⑥ « III. – Les informations communiquées en application du présent article ne peuvent être transmises à des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement.

⑦ « Sauf si l'information porte sur une condamnation prononcée publiquement, toute personne qui en est destinataire est tenue au secret professionnel, dans les conditions et sous les peines prévues aux articles 226-13 et 226-14 du code pénal. »

CHAPITRE III

Dispositions relatives à la lutte contre les aéronefs circulant sans personne a bord présentant une menace

Article 18

① L'article L. 33-3-1 du code des postes et des communications électroniques est ainsi modifié :

② 1° Au I, les mots : « appareils de communications électroniques », sont remplacés par les mots : « équipements radioélectriques ou des appareils intégrant des équipements radioélectriques, » ;

③ 2° Après le premier alinéa du II, il est inséré un alinéa ainsi rédigé :

④ « L'utilisation par les services de l'État de dispositifs destinés à rendre inopérant l'équipement radioélectrique d'un aéronef circulant sans personne à bord est autorisée, en cas de menace imminente, pour les besoins de l'ordre public, de la défense et de la sécurité nationale ou du service public de la justice ou afin de prévenir le survol d'une zone en violation d'une interdiction prononcée dans les conditions prévues au premier alinéa de l'article L. 6211-4 du code des transports. Un décret en Conseil d'État détermine les modalités de mise en œuvre de ces dispositifs afin de garantir leur nécessité et leur proportionnalité au regard des finalités poursuivies ainsi que les autorités compétentes pour y procéder. »

CHAPITRE IV

Dispositions relatives aux archives intéressant la défense nationale

Article 19

① I. – L'article L. 213-2 du code du patrimoine est ainsi modifié :

② 1° Le I est ainsi modifié :

③ *a)* Au premier alinéa du 3°, après les mots : « dont la communication porte atteinte au secret de la défense nationale » sont ajoutés les mots : « , et ayant pour ce motif fait l'objet d'une mesure de classification mentionnée à l'article 413-9 du code pénal » ;

④ *b)* Le second alinéa du 3° est remplacé par cinq alinéas ainsi rédigés :

⑤ « Ce délai est prolongé pour les documents relatifs :

⑥ « *a)* Aux caractéristiques techniques des installations militaires, des installations et ouvrages nucléaires civils, des barrages hydrauliques de grande hauteur, des locaux des missions diplomatiques et consulaires françaises et des installations utilisées pour la détention des personnes, jusqu'à la date, constatée par un acte publié, de fin de l'affectation à ces usages de ces infrastructures ou d'infrastructures présentant des caractéristiques similaires ;

⑦ *« b)* À la conception technique et aux procédures d'emploi des matériels de guerre et matériels assimilés mentionnés au second alinéa de l'article L. 2335-2 du code de la défense, désignés par un arrêté du ministre de la défense révisé chaque année, jusqu'à la fin de leur emploi par les forces armées et les formations rattachées mentionnées à l'article L. 3211-1-1 du code de la défense. » ;

⑧ « *c)* Aux procédures opérationnelles et aux capacités techniques des services de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure ainsi qu'à ceux des services mentionnés à l'article L. 811-4 du même code désignés, au regard de leurs missions, par décret en Conseil d'État, jusqu'à la date de la perte de leur valeur opérationnelle ;

⑨ « *d)* À l'organisation, la mise en œuvre et la protection des moyens de la dissuasion nucléaire, jusqu'à la date de la perte de leur valeur opérationnelle. » ;

⑩ *c)* La première phrase du second alinéa du 5° est ainsi rédigée : « Les mêmes délais s'appliquent aux documents dont la communication est de nature à porter atteinte à la sécurité de personnes nommément désignées ou facilement identifiables impliquées dans des activités de renseignement, que ces documents aient fait ou fassent ou non l'objet d'une mesure de classification. » ;

⑪ 2° Au premier alinéa du II, après les mots : « armes nucléaires, » est inséré le mot : « radiologiques, » ;

⑫ 3° Il est ajouté un III ainsi rédigé :

⑬ « III. – Toute mesure de classification mentionnée à l'article 413-9 du code pénal prend automatiquement fin à la date à laquelle le document qui en a fait l'objet devient communicable de plein droit en application du présent chapitre.

⑭ « Par exception, les mesures de classification dont font l'objet, le cas échéant, les documents mentionnés au 4° du I prennent automatiquement fin dès l'expiration du délai prévu au 3° du I. »

⑮ II. – Les règles de communicabilité prévues par le I ne sont pas applicables aux documents n'ayant pas fait l'objet d'une mesure de classification et pour lesquels le délai de 50 ans prévu au 3° du I de l'article L. 213-2 a expiré avant l'entrée en vigueur du présent article.

CHAPITRE V

Dispositions relatives aux outre-mer

Article 20

Les articles 1er et 12 de la présente loi sont applicables dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises.

Article 21

① Le code de la sécurité intérieure est ainsi modifié :

② 1° Au premier alinéa des articles L. 285-1, L. 286-1, L. 287-1 et L. 288-1, la référence : « l'ordonnance n° 2019-738 du 17 juillet 2019 » est remplacée par la référence : « la loi n° du relative à la prévention d'actes de terrorisme et au renseignement » ;

③ 2° Au premier alinéa des articles L. 895-1, L. 896-1, L. 897-1 et L. 898-1, les mots : « l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel » sont remplacés par les mots : « la loi n° .du relative à la prévention d'actes de terrorisme et au renseignement » ;

④ 3° Au 2° des articles L. 895-1 et L. 896-1, après les mots : « L. 871-2, », sont insérés les mots : « L. 871-3, ».

Article 22

Au premier alinéa de l'article 804 du code de procédure pénale, la référence : « loi n° 2020-1721 du 29 décembre 2020 de finances pour 2021 » est remplacée par la référence : « loi n° du relative à la prévention d'actes de terrorisme et au renseignement ».

Article 23

① Le deuxième alinéa du I de l'article L. 3844-1 du code de la santé publique est ainsi modifié :

② 1° Après la référence : « L. 3211-12-2, », est insérée la référence : « L. 3211-12-7, » ;

③ 2° La référence : « loi n° 2016-41 du 26 janvier 2016 » est remplacée par la référence : « loi n° du relative à la prévention d'actes de terrorisme et au renseignement ».

Article 24

À l'article 125 de la loi n° 78-17 du 6 janvier 1978, la référence : « l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel » est remplacée par la référence : « la loi n° du relative à la prévention d'actes de terrorisme et au renseignement ».

Article 25

Au premier alinéa du I de l'article 57 de la loi n° 2004-575 du 21 juin 2004, la référence : « loi n° 2020 766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet » est remplacée par la référence : « loi n° du relative à la prévention d'actes de terrorisme et au renseignement ».

Article 26

① Le code des postes et des communications électroniques est ainsi modifié :

② I. – À l'article L. 33-3-2, après les mots : « Nouvelle-Calédonie », sont insérés les mots : « dans sa rédaction résultant de la loi n° du » ;

③ II. – À l'article L. 34-4, après les mots : « îles Wallis et Futuna », sont insérés les mots : « dans leur rédaction résultant de la loi n° du ».

Article 27

① L'article L. 760-2 du code du patrimoine est ainsi modifié :

② 1° Au 1°, après les mots : « L. 213-1 » sont insérés les mots : « , L. 213-3 » ;

③ 2° Après le 2°, il est ajouté un alinéa ainsi rédigé :

④ « 3° L'article L. 213-2 dans sa rédaction résultant de la loi n° du ».

Article 28

À l'article L. 770-1 du code du patrimoine, la référence : « loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice » est remplacée par la référence : « loi n° du relative à la prévention d'actes de terrorisme et au renseignement ».

Article 29

La présente loi entre en vigueur le lendemain de sa publication au *Journal officiel* de la République française dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

ÉTUDE D'IMPACT

PROJET DE LOI

RELATIF A LA PREVENTION D'ACTES DE TERRORISME ET AU RENSEIGNEMENT

ET LETTRE RECTIFICATIVE

NOR : INTD2107675L/INTD2113198L/Bleue-1

11 mai 2021

TABLE DES MATIERES

INTRODUCTION GENERALE **5**

TABLEAU SYNOPTIQUE DES CONSULTATIONS 7

TABLEAU SYNOPTIQUE DES MESURES D'APPLICATION 10

TABLEAU D'INDICATEURS 12

CHAPITRE I[ER] – DISPOSITIONS RENFORÇANT LA PREVENTION D'ACTES DE TERRORISME **13**

Article 1er : Pérennisation des articles 1er à 4 de la loi n° 2017-1510 du 31 octobre 2017 (dite Loi « SILT ») 13

Article 2 : Élargir le champ d'application des mesures de fermeture des lieux de culte aux lieux en dépendant 55

Article 3 (1° a et 2°) : Imposer la fourniture d'un justificatif du lieu d'habitation ou de domicile68

Article 3 (1° b) : Faire obligation à certaines personnes placées sous surveillance, dans le cadre de l'article L. 228-2 du code de la sécurité intérieure, de ne pas paraître temporairement dans certains lieux dans lesquels se tiennent des évènements exposés, par leur ampleur ou leurs circonstances particulières, à une menace terroriste 72

Article 3 (3°) : Prévoir la possibilité de prolonger la MICAS pendant une durée maximale de deux ans lorsque l'intéressé a été condamné pour des faits de terrorisme 80

Article 3 (4°) : Sécuriser la procédure juridictionnelle applicable au renouvellement des MICAS 94

Article 3 (5°) : Prendre en compte les obligations déjà prescrites par l'autorité judiciaire lors de la définition des obligations imposées dans le cadre d'une MICAS 99

Article 3 (6°) : Prolonger la validité des MICAS en cours à la date de promulgation de la présente loi pour permettre leur éventuel renouvellement selon la procédure prévue aux articles L. 228-2, L 228-4 et L. 228-5 du code de la sécurité intérieure 104

Article 4 : Permettre la saisie d'un support informatique présent sur les lieux de la visite domiciliaire lorsque la personne fait obstacle à l'accès aux données informatiques qu'il contient 107

Article 5 : Création d'une mesure judiciaire de prévention de la récidive terroriste et de réinsertion 111

Article 6 : Droit de communication aux préfets et services de renseignement des informations relatives aux soins psychiatrique sans consentement 124

CHAPITRE II – DISPOSITIONS RELATIVES AU RENSEIGNEMENT **134**

Article 7 : Transmission de renseignements entre services – Communication d'information aux services de renseignement 134

Article 8 : Conservation de données pour les travaux de recherche et développement 147

Article 9 : Harmonisation des durées d'autorisation pour les techniques de recueil et de captation de données informatiques 154

Article 10 : Extension des possibilités de réquisition des opérateurs télécom pour la mise en œuvre des techniques de renseignement et des techniques spéciales d'enquête 158

Article 11 : Expérimentation d'une technique d'interception des communications empruntant la voie satellitaire 163

Article 12 : Pérennisation des dispositions relatives à l'algorithme 175

Article 13 : Modalités d'exécution des traitements automatisés et extension aux adresses complètes de ressources sur internet (URL) 186

Article 14 : Ajout des adresses complètes de ressource sur internet (URL) aux données susceptibles d'être recueillies en temps réel (1°) et définition de leur durée de conservation (2°) 195

Article 15 : Modalités de conservation des données de connexion en cas de menace grave, actuelle ou prévisible sur la sécurité nationale 201

Article 16 : Procédure de contrôle préalable à la mise en œuvre des techniques de renseignement sur le territoire national 216

Article 17 : Echanges d'informations entre les services judiciaires et les services de renseignement dans le cadre de la lutte contre la cybercriminalité et la criminalité organisée et entre les services judiciaires et l'ANSSI dans le cadre de la lutte contre la cybercriminalité 227

CHAPITRE III – DISPOSITIONS RELATIVES A LA LUTTE CONTRE LES AERONEFS CIRCULANT SANS PERSONNE A BORD PRESENTANT UNE MENACE 235

Article 18 : Lutte contre les aéronefs circulant sans personne à bord présentant une menace 235

CHAPITRE IV – DISPOSITIONS RELATIVES AUX ARCHIVES INTERESSANT LA DEFENSE NATIONALE 242

Article 19 : Accès aux archives publiques 242

INTRODUCTION GENERALE

Le 1er novembre 2017 à minuit, l'état d'urgence a pris fin en France et les dispositions de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (dite loi « SILT ») sont entrées en vigueur avec effet immédiat.

La liste des instruments de lutte contre le terrorisme et les atteintes aux intérêts fondamentaux de la Nation, prévue par le titre II du livre II du code de la sécurité intérieure, s'est ainsi trouvée enrichie de quatre nouveaux chapitres créés par les quatre premiers articles de la loi : périmètres de protection (art. 1er), fermeture des lieux de cultes (art. 2), mesures individuelles de contrôle administratif et de surveillance (art. 3) et visites domiciliaires et saisies (art. 4). L'autorité administrative dispose ainsi désormais de moyens juridiques étendus, mais ayant pour seule finalité la prévention des actes de terrorisme.

En raison du caractère novateur de ces mesures qui accroissent les pouvoirs de police de l'autorité administrative, le Parlement a souhaité, dans un premier temps, limiter au 31 décembre 2020 la durée d'application de ces quatre séries de dispositions.

Si le Gouvernement a, au premier trimestre 2020, saisi le Conseil d'État d'un projet de loi visant à pérenniser ces mesures dans l'ordonnancement juridique, tout en les modifiant pour corriger quelques lacunes apparues ou malfaçons apparues lors de leur mise en œuvre, cette exercice n'a pu prospérer totalement. En effet, l'émergence de la crise sanitaire liée à la covid-19 et de ses conséquences sur le fonctionnement normal des institutions puis la nécessité d'adopter d'autres mesures législatives plus urgentes, notamment pour faire face à cette épidémie, n'ont pas permis l'organisation d'un débat parlementaire serein sur lesdites mesures. C'est pourquoi un nouveau projet de loi a été présenté le 17 juin 2020 en conseil des ministres visant à seulement à proroger ces mesures pour laisser au Parlement le temps nécessaire à cet examen approfondi. La loi n° 2020-1671 du 24 décembre 2020 a donc reporté au 31 juillet 2021 la fin de la durée d'application des mesures précitées.

Le **chapitre Ier** du présent projet de la loi vise donc à pérenniser ces dispositions (article 1er) mais aussi à les modifier ou compléter (articles 2 à 6).

Le **chapitre II** a trait à la modification de certaines dispositions relatives au renseignement. Près de cinq ans après l'adoption de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, il vise à apporter au livre VIII du code de sécurité intérieure les ajustements nécessaires pour que les services de renseignement continuent de disposer de moyens d'action adéquats et proportionnés face aux menaces persistantes qui pèsent sur les intérêts fondamentaux de la Nation.

Les dispositions ont pour objet d'adapter les techniques de renseignements, de partage de renseignement entre service et de développement des capacités de renseignement à l'évolution

des comportements de personnes faisant l'objet d'une surveillance, afin de ne pas perdre en efficacité ou de compléter ces techniques pour faire face à des besoins nouveaux.

Préservant l'équilibre adopté par le législateur en 2015, il a d'abord pour objet de pérenniser la technique de renseignement prévue à l'article L. 851-3 du code de sécurité intérieure, dite algorithme, instaurée au titre d'une expérimentation dont l'échéance est fixée au 31 décembre 2021, conformément à l'article 25 modifié de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement. Les autres dispositions ont pour objet d'adapter les techniques de renseignements, de partage de renseignement entre service et de développement des capacités de renseignement à l'évolution des comportements de personnes faisant l'objet d'une surveillance, afin de ne pas perdre en efficacité ou de compléter ces techniques pour faire face à des besoins nouveaux.

Le **chapitre III**, constitué d'un unique article 18, instaure, au sein du code des postes et communications électroniques, des dispositions relatives à la lutte contre les drones malveillants.

Enfin, le **chapitre IV**, constitué d'un unique article 19, modifie l'article L. 213-2 du code du patrimoine pour clarifier le régime de communicabilité des archives classifiées, gage d'ouverture envers les chercheurs et les historiens.

TABLEAU SYNOPTIQUE DES CONSULTATIONS

Article	Objet de l'article	Consultations obligatoires	Consultations facultatives
1er	Pérennisation des articles 1er à 4 de la loi n° 2017-1510 du 31 octobre 2017 (dite Loi « SILT »)		Commission nationale de l'informatique et des libertés
2	Élargir le champ d'application des mesures de fermeture des lieux de culte aux lieux en dépendant		Commission nationale de l'informatique et des libertés
3 (1° a et 2°)	Imposer la fourniture d'un justificatif du lieu d'habitation ou de domicile		Commission nationale de l'informatique et des libertés
3 (1° b)	Faire obligation à certaines personnes placées sous surveillance, dans le cadre de l'article L. 228-2 du code de la sécurité intérieure, de ne pas paraître temporairement dans certains lieux dans lesquels se tiennent des évènements exposés, par leur ampleur ou leurs circonstances particulières, à une menace terroriste		Commission nationale de l'informatique et des libertés
3 (3°)	Prévoir la possibilité de prolonger la MICAS pendant une durée maximale de deux ans lorsque l'intéressé a été condamné pour des faits de terrorisme		Commission nationale de l'informatique et des libertés
3 (4°)	Sécuriser la procédure juridictionnelle applicable au renouvellement des MICAS		Commission nationale de l'informatique et des libertés
3 (5°)	Prendre en compte les obligations déjà prescrites par l'autorité judiciaire lors de la définition des obligations imposées dans le cadre d'une MICAS		Commission nationale de l'informatique et des libertés
3 (6°)	Prolonger la validité des MICAS en cours à la date de promulgation de la présente loi pour permettre leur éventuel renouvellement selon la procédure prévue aux articles L. 228-2, L 228-4 et L. 228-5 du CSI		
4	Permettre la saisie d'un support informatique présent sur les lieux de la visite domiciliaire lorsque la personne fait obstacle à l'accès aux données informatiques qu'il contient	Commission nationale de l'informatique et des libertés	
5	Création d'une mesure judiciaire de prévention de la récidive terroriste et de réinsertion		Commission nationale de l'informatique et des libertés
6	Droit de communication aux préfets et services de renseignement des informations relatives aux soins psychiatrique sans consentement	Commission nationale de l'informatique et des libertés	

Article	Objet de l'article	Consultations obligatoires	Consultations facultatives
7	Transmission de renseignements entre services – Communication d'information aux services de renseignement	Commission nationale de contrôle des techniques de renseignement Commission nationale de l'informatique et des libertés	
8	Conservation de données pour les travaux de recherche et développement	Commission nationale de contrôle des techniques de renseignement Commission nationale de l'informatique et des libertés	
9	Harmonisation des durées d'autorisation pour les techniques de recueil et de captation de données informatiques	Commission nationale de contrôle des techniques de renseignement Commission nationale de l'informatique et des libertés	
10	Extension des possibilités de réquisition des opérateurs télécom pour la mise en œuvre des techniques de renseignement et des techniques d'enquêtes judiciaires	Commission nationale de contrôle des techniques de renseignement Commission nationale de l'informatique et des libertés Autorité de régulation des communications électroniques, des postes et de la distribution de la presse	
11	Expérimentation d'une technique d'interception des communications empruntant la voie satellitaire	Commission nationale de contrôle des techniques de renseignement Autorité de régulation des communications électroniques, des postes et de la distribution de la presse	Commission nationale de l'informatique et des libertés
12	Pérennisation des dispositions relatives à l'algorithme	Commission nationale de contrôle des techniques de renseignement Commission nationale de l'informatique et des libertés Autorité de régulation des communications électroniques, des postes et de la distribution de la presse	
13	Ajout des adresses complètes de ressources sur internet (URL) aux données traitées par l'algorithme	Commission nationale de contrôle des techniques de renseignement Commission nationale de l'informatique et des libertés Autorité de régulation des communications électroniques,	

Article	Objet de l'article	Consultations obligatoires	Consultations facultatives
		des postes et de la distribution de la presse	
14	Ajout des adresses complètes de ressource sur internet (URL) aux données susceptibles d'être recueillies en temps réel (1°) et définition de leur durée de conservation (2°)	Commission nationale de contrôle des techniques de renseignement Commission nationale de l'informatique et des libertés Autorité de régulation des communications électroniques, des postes et de la distribution de la presse	
15	Modalités de conservation des données de connexion en cas de menace grave, actuelle ou prévisible sur la sécurité nationale	Commission nationale de contrôle des techniques de renseignement Commission nationale de l'informatique et des libertés Autorité de régulation des communications électroniques, des postes et de la distribution de la presse	
16	Procédure de contrôle préalable à la mise en œuvre des techniques de renseignement sur le territoire national	Commission nationale de contrôle des techniques de renseignement	
17	Échanges d'informations entre les services judiciaires et les services de renseignement dans le cadre de la lutte contre la cybercriminalité et la criminalité organisée et l'ANSSI dans le cadre de la lutte contre la cybercriminalité	Commission nationale de l'informatique et des libertés	
18	Lutte contre les aéronefs circulant sans personne à bord présentant une menace	Autorité de régulation des communications électroniques, des postes et de la distribution de la presse	
19	Accès aux archives publiques		Commission nationale de l'informatique et des libertés

TABLEAU SYNOPTIQUE DES MESURES D'APPLICATION

Article	Objet de l'article	Textes d'application	Administration compétente
1er	Pérennisation des articles 1er à 4 de la loi n° 2017-1510 du 31 octobre 2017 (dite Loi « SILT »)		
2	Élargir le champ d'application des mesures de fermeture des lieux de culte aux lieux en dépendant.		
3 (1° a et 2°)	Imposer la fourniture d'un justificatif du lieu d'habitation ou de domicile		
3 (1° b)	Faire obligation à certaines personnes placées sous surveillance, dans le cadre de l'article L. 228-2 du code de la sécurité intérieure, de ne pas paraître temporairement dans certains lieux dans lesquels se tiennent des évènements exposés, par leur ampleur ou leurs circonstances particulières, à une menace terroriste		
3 (3°)	Prévoir la possibilité de prolonger la MICAS pendant une durée maximale de deux ans lorsque l'intéressé a été condamné pour des faits de terrorisme		
3 (4°)	Sécuriser la procédure juridictionnelle applicable au renouvellement des MICAS		
3 (5°)	Prendre en compte les obligations déjà prescrites par l'autorité judiciaire lors de la définition des obligations imposées dans le cadre d'une MICAS		
3 (6°)	Prolonger la validité des MICAS en cours à la date de promulgation de la présente loi pour permettre leur éventuel renouvellement selon la procédure prévue aux articles L. 228-2, L 228-4 et L. 228-5 du CSI		
4	Permettre la saisie d'un support informatique présent sur les lieux de la visite domiciliaire lorsque la personne fait obstacle à l'accès aux données informatiques qu'il contient		
5	Création d'une mesure judiciaire de prévention de la récidive terroriste et de réinsertion	Décret en Conseil d'État	Ministère de la justice
6	Droit de communication aux préfets et services de renseignement des informations relatives aux soins psychiatrique sans consentement	Décret en Conseil d'État : modification du décret n° 2018-383 du 23 mai 2018	Ministère des solidarités et de la santé
7	Transmission de renseignements entre services – Communication d'information aux services de renseignement	Décret en Conseil d'État	Ministère de l'intérieur
8	Conservation de données pour les travaux de recherche et développement		

Article	Objet de l'article	Textes d'application	Administration compétente
9	Harmonisation des durées d'autorisation pour les techniques de recueil et de captation de données informatiques		
10	Extension des possibilités de réquisition des opérateurs télécom pour la mise en œuvre des techniques de renseignement et des techniques d'enquête	Arrêté	Ministère de l'économie et des finances
11	Expérimentation d'une technique d'interception des communications empruntant la voie satellitaire	Décret en Conseil d'Etat	Ministère de l'intérieur
12	Pérennisation des dispositions relatives à l'algorithme		
13	Ajout des adresses complètes de ressources sur internet (URL) aux données traitées par l'algorithme		
14	Ajout des adresses complètes de ressource sur internet (URL) aux données susceptibles d'être recueillies en temps réel (1°) et définition de leur durée de conservation (2°)		
15	Modalités de conservation des données de connexion en cas de menace grave, actuelle ou prévisible sur la sécurité nationale	Décret en Conseil d'Etat	
16	Procédure de contrôle préalable à la mise en œuvre des techniques de renseignement sur le territoire national		
17	Échanges d'informations entre les services judiciaires et les services de renseignement dans le cadre de la lutte contre la cybercriminalité et la criminalité organisée et l'ANSSI dans le cadre de la lutte contre la cybercriminalité		
18	Lutte contre les aéronefs circulant sans personne à bord présentant une menace	Décret en Conseil d'Etat	Premier ministre (SGDSN)
19	Accès aux archives publiques	Décret en Conseil d'Etat	Ministère de l'intérieur

TABLEAU D'INDICATEURS

Indicateurs	Horizon temporel et périodicité	Modalités de suivi
Evolution du nombre de périmètres de protection	Annuel (N/ N-1)	Rapport annuel réalisé par le ministère de l'intérieur
Evolution du nombre de fermetures de lieux culte	Annuel (N/ N-1)	Rapport annuel réalisé par le ministère de l'intérieur
Evolution du nombre de MICAS prononcées 1an/2 ans	Annuel (N/ N-1)	Rapport annuel réalisé par le ministère de l'intérieur
Evolution du nombre de mesures de réinsertion judiciaire	Annuel (N/ N-1)	Rapport annuel réalisé par le ministère de la justice
Evolution du nombre de saisies d'un support informatique	Annuel (N/ N-1)	Rapport annuel réalisé par le ministère de l'intérieur

CHAPITRE I^ER – DISPOSITIONS RENFORÇANT LA PREVENTION D'ACTES DE TERRORISME

Article 1^er : Pérennisation des articles 1^er à 4 de la loi n° 2017-1510 du 31 octobre 2017 (dite Loi « SILT »)

1. ÉTAT DES LIEUX

Les articles 1^er à 4 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (dite loi « SILT ») ont instauré de nouvelles mesures de police administrative : les périmètres de protection (L. 226-1 du code de sécurité intérieure), la fermeture des lieux de culte (L. 227-1), les mesures individuelles de contrôle administratif et de surveillance (L. 228-1) et les visites domiciliaires et saisies (L. 229-1). L'article 5 de la même loi prévoit que ces dispositions sont applicables jusqu'au 31 juillet 2021.

Ces dispositions constituent des outils supplémentaires d'une stratégie de prévention des actes de terrorisme fondée à la fois sur la protection d'événements et de lieux aux caractéristiques particulières et sur la surveillance de personnes dont le comportement et/ou le relationnel peut présenter un risque d'une particulière gravité pour l'ordre et la sécurité publics.

En raison du caractère novateur de ces mesures qui accroissent de manière significative les pouvoirs de l'autorité de police administrative, l'article 5 de la loi a subordonné leur exécution à une information permanente du Parlement, à une évaluation annuelle et a limité leur durée d'application au 31 décembre 2020, puis au 31 juillet 2021, leur pérennisation étant subordonnée à l'appréciation de leur caractère nécessaire, adapté et proportionné.

Après désormais plus de trois ans d'application, la mise en œuvre de ces mesures a permis de mettre en évidence leur utilisation raisonnée par l'autorité administrative (voir synthèse statistique ci-après), leur utilité opérationnelle et leur complémentarité avec les autres dispositifs d'entrave administrative ou judiciaire, soit en amont de l'intervention de l'autorité judiciaire et de l'ouverture d'une procédure, soit en aval, à la sortie de prison. En effet, l'expérience a montré, comme cela avait d'ailleurs été indiqué lors des débats parlementaires, que l'autorité judiciaire n'est pas toujours en mesure de judiciariser immédiatement une situation, alors que l'individu peut en revanche déjà être entravé administrativement.

Par ailleurs, leur utilisation mesurée, le faible taux de contestation et leur encore plus faible taux d'annulation démontre leur bonne appropriation par l'autorité de police administrative et leur usage modéré et proportionné.

	Périmètres de protection	Fermetures de lieux de culte	Mesures individuelles de contrôle administratif et de surveillance	Visites et saisies	
				Visites domiciliaires	***Saisies réalisées***
CUMUL depuis le 1er novembre 2017	610	8	401	451	439

Source : Ministère de l'intérieur, chiffres au 5 mars 2021

1.1. LES PERIMETRES DE PROTECTION

L'article L. 226-1 du code de la sécurité intérieure (CSI) donne au préfet, lorsqu'un lieu ou un événement est exposé à un risque d'acte de terrorisme à raison de sa nature ou de l'ampleur de sa fréquentation, la possibilité d'instaurer par arrêté un périmètre de protection où l'accès et la circulation à l'intérieur même de la zone sont réglementés.

Cette mesure diffère des zones de protection et de sécurité prévues à l'article 5 de la loi du 3 avril 1955 relative à l'état d'urgence, dont la justification était en partie liée à la déclaration même de l'état d'urgence, à l'existence d'une menace terroriste diffuse et aux circonstances propres à la zone à protéger.

L'instauration d'un périmètre de protection permet aux forces de sécurité de l'État et, le cas échéant, aux policiers municipaux et aux agents privés de sécurité sous le contrôle d'officiers de police judiciaire, de dissuader ou d'empêcher les personnes susceptibles de commettre un acte à caractère terroriste de pénétrer dans un lieu ou à l'intérieur de l'enceinte d'un événement particulièrement exposé.

Cette mesure leur permet ainsi :

- de procéder à l'inspection visuelle, à la fouille de bagages et à des palpations de sécurité à l'entrée et au sein du périmètre, afin de s'assurer que les personnes souhaitant y accéder ou y circulant ne sont pas porteuses d'objets dangereux ;
- d'empêcher l'accès au périmètre de sécurité des personnes qui refuseraient de se soumettre au contrôle ou de les reconduire à l'extérieur, lorsqu'elles y ont pénétré ;
- d'empêcher ou de contrôler l'accès ou le stationnement des véhicules à l'intérieur du périmètre.

Ces pouvoirs sont confiés aux policiers et aux gendarmes (officiers et agents de police judiciaire) et, sous leur contrôle et uniquement pour filtrer l'accès au périmètre protégé, à des agents de police municipale ou, le cas échéant, à des agents privés de sécurité.

1.1.1. Une mesure jugée conforme à la Constitution

Saisi d'une question prioritaire de constitutionnalité, le Conseil constitutionnel a, dans sa décision n° 2017-695 QPC du 29 mars 2018, considéré que, dès lors qu'un arrêté préfectoral déterminait de façon précise les conditions de mise en place d'un périmètre de protection (étendue et durée) et énonçait des règles d'accès et de circulation en son sein (vérifications) de

nature à respecter les impératifs de la vie privée, familiale et professionnelle, le champ d'application de la mesure était *« strictement borné »* et apportait *« les garanties nécessaires »* pour assurer l'équilibre *« entre d'une part, l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et, d'autre part, la liberté d'aller et de venir et le droit au respect de la vie privée. »*

Il a toutefois rappelé que les vérifications opérées pour l'accès au périmètre de protection ou la circulation en son sein devaient se fonder *« sur des critères excluant toute discrimination de quelque nature que ce soit entre les personnes »* et que, compte tenu de la rigueur des mesures de vérification associées à un périmètre de protection, le renouvellement de ce dernier ne pouvait être décidé par l'autorité préfectorale qu'en établissant la persistance du risque d'actes de terrorisme.

De même, répondant au grief tiré de la méconnaissance des exigences de l'article 12 de la Déclaration des droits de l'Homme et du citoyen de 1789, qui dispose que la force publique est *« instituée pour l'avantage de tous et non pour l'utilité particulière de ceux auxquels est confiée »*, le Conseil constitutionnel a confirmé la possibilité pour les agents de la force publique de recourir à l'assistance d'agents agréés exerçant une activité privée de sécurité pour la mise en œuvre de palpations de sécurité et d'inspections et fouilles de bagages. Il a néanmoins formulé trois réserves en indiquant que ces derniers devaient se borner à assister les agents de police judiciaire, qu'ils étaient placés *« sous l'autorité d'un officier de police judiciaire »* et qu'il appartenait *« aux autorités publiques de prendre les dispositions afin de s'assurer que soit continûment garantie l'effectivité du contrôle exercé sur ces personnes par les officiers de police judiciaire. ».*

1.1.2. Une utilisation raisonnée et proportionnée par l'autorité de police administrative

Compte tenu de la nécessité pour les préfets de continuer à assurer un niveau de sécurité aussi élevé que sous l'état d'urgence et en l'absence de doctrine d'emploi sur ce dispositif, du fait même de son caractère novateur, les périmètres de protection ont pu, dans un premier temps, être parfois utilisés dans un but étranger à la seule prévention du terrorisme ou selon un mode permanent, aux lieu et place d'autres réglementations spéciales permettant d'atteindre le même objectif (points d'importance vitale[1], gares[2], installations portuaires[3] et aéroportuaires[4]).

Les premiers arrêtés souffraient en outre de quelques défauts de conception ou de rédaction :

[1] Articles L. 1332-3 et R. 1332-23 et suivants du code de la défense.

[2] Articles L. 2251-1 et suivants du code des transports.

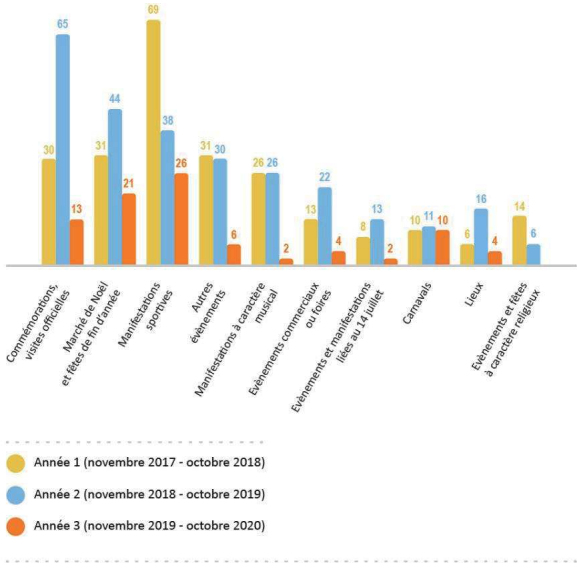
[3] Articles L. 5332-1 A et suivants du code des transports.

[4] Articles L. 6341-1 et suivants du code des transports, résultant de l'application du règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile.

- Absence de mesure spécifique pour prendre en compte la situation des personnes devant accéder habituellement à l'intérieur du périmètre pour des raisons familiales ou professionnelles ;
- Imprécision de la délimitation géographique des zones par l'absence de mention des noms des rues bordant la zone ou par le renvoi à un plan ou carte en annexe de l'arrêté ;
- Absence de précision des horaires de début et de fin d'activation du périmètre ainsi que des points d'accès ;
- La motivation ne reposait généralement que sur *« la prégnance de la menace terroriste sur le territoire national »* et l'importance de la fréquentation, sans démontrer en quoi l'événement réunissait les critères prévus par la loi : nombre de participants prévus au regard des éventuelles éditions précédentes, nature particulière de l'événement ou du lieu liée à son caractère symbolique, éventuelles menaces identifiées localement, etc.

Le rappel aux préfets des conditions dans lesquelles il devait être fait usage de cette mesure ainsi que des différents dispositifs de sécurisation auxquels il pouvait être fait appel en fonction du type d'installation a permis de renforcer rapidement la sécurité juridique des décisions préfectorales et de rééquilibrer l'usage du périmètre de protection.

Pendant les trois premières années d'application de la mesure, 597 périmètres ont été établis (238 la première année, 271 la deuxième et 88 depuis la troisième année), cette baisse significative la dernière année s'expliquant par la réduction drastique des évènements ou rassemblements sur la voie publique résultant de la crise sanitaire liée à la Covid-19, à compter de mars 2020. Ainsi, par exemple, aucun arrêté instaurant un périmètre de protection n'a été pris entre le 26 février 2020 et le 30 juin 2020.



Types de lieu ou d'événement ayant justifié un périmètre de protection (source : ministère de l'intérieur 30 octobre 2020)

Le recours à ces périmètres de protection a permis, durant ces trois années, et nonobstant la prégnance de la menace terroriste, de sécuriser certains évènements qui ont, dès lors pu se tenir avec un niveau de sécurisation important : il en est ainsi d'évènements officiels ou de sommets internationaux (G5 Sahel ou G7…), de manifestations sportives (Tour de France…), d'évènements festifs ou culturels (marchés de Noël, carnavals, fête nationale) ou religieux, ou encore d'évènements commerciaux ou foires (21e édition du salon Milipol à Paris en novembre 2019).

Ces mesures ont parfois été complétées par d'autres mesures de police administrative (arrêtés du préfet ou du maire) afin de renforcer l'efficacité du dispositif :

- pour la majorité des dispositifs, l'accès a été interdit aux personnes porteuses d'objets dangereux (armes ou artifices) ou de tout objet pouvant constituer une arme, étant entendu qu'en l'absence d'une telle disposition, les vérifications opérées pour l'accès à la zone protégée permettent déjà d'interdire cet accès ;
- les périmètres de protection mis en œuvre à l'occasion de manifestations sportives ou festives ont également interdit tous les contenants en verre pouvant constituer un projectile ;
- dans certains cas, les manifestations, au sens de l'article L. 211-1 du code de la sécurité intérieure, ont été interdites dans la mesure où elles se seraient révélées incompatibles avec l'événement ; toutefois, pour ne pas porter une atteinte disproportionnée au droit de manifester, l'interdiction n'était valable que lors des pics de fréquentation ;
- des interdictions de survol du périmètre de protection par des drones ont parfois été prévues, bien que le survol d'agglomérations par des drones civils[5] soit déjà strictement réglementé ;
- ont enfin, dans certains cas, été interdits l'accès de véhicules aux vitres teintées, l'accès de personnes portant des tenues destinées à dissimuler le visage ou l'accès de chiens dangereux.

La durée de ces périmètres est le plus souvent limitée à celle de l'évènement concerné, avec une durée moyenne de cinq jours.

1.1.3. Une appropriation confirmée du dispositif par l'autorité administrative

Les retours d'expérience réalisés par les préfectures sur la mise en œuvre des périmètres de protection au cours des deux premières années ont permis d'affiner la stratégie opérationnelle au cours de la troisième année d'application et d'adapter la définition et les modalités de mise en œuvre de ces périmètres de protection, notamment pour ceux qui concernent des évènements récurrents, d'année en année.

[5] Arrêtés du 17 décembre 2015 relatif d'une part à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et d'autre part à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent

Face à la difficulté de réaliser les contrôles d'accès systématiques et « d'étanchéifier » les périmètres pour des événements par nature très importants, le tracé des périmètres a été réduit et/ou affiné, et le recours aux policiers municipaux et aux agents privés de sécurité a été réaffirmé.

Les services de la police nationale restent les plus mobilisés, les périmètres de protection étant créés dans les grandes agglomérations (452 périmètres sont en effet situés en zone police soit environ 76% des cas).

Le recours aux policiers municipaux est de plus en plus sollicité, même s'il n'est pas systématique. Les policiers municipaux ont en effet été mis à contribution pour la sécurité de 60 périmètres de protection (soit dans 68 % des cas comme l'année précédente, contre 57 % lors de la première année), essentiellement pour des manifestations à l'initiative des communes (marchés de Noël et carnavals notamment).

En revanche, le recours aux agents privés de sécurité est plus systématique, soit dans 75 % des cas, tendance constante par rapport aux deux premières années d'application de la loi SILT (77 % la première année et 78 % la deuxième année).

La bonne appropriation de ces mesures et leur utilisation raisonnée est confirmée par la bonne acceptation de la mesure au sein de la population. Les enquêtes de terrain réalisées par les préfets ou les maires démontrent que les mesures mises en place à ce titre sont en effet bien tolérées par les riverains et professionnels concernés par la zone à protéger, notamment en raison des durées limitées des mesures, de l'information préalable réalisée par les différents acteurs institutionnels ainsi que des mesures de contrôle spécifiques à leur égard, pour tenir compte de l'atteinte portée à leur vie privée et familiale, lorsque le périmètre inclut leur domicile, leur lieu de travail ou des lieux en lien avec leur vie privée et familiale.

Conformément aux exigences posées par l'article L. 226-1 du code de la sécurité intérieure, les règles d'accès et de circulation au sein des périmètres sont adaptées à ces impératifs, les personnes étant invitées à se signaler à l'avance auprès de la préfecture pour se voir délivrer un badge permettant de se présenter à un point d'accès dédié et de bénéficier d'un filtrage accéléré (pour 38 des 88 périmètres soit 43 %, contre 35 % l'année précédente et seulement 19 % la 1ère année). Les seules mesures qui ont été considérées par les riverains comme contraignantes sont celles qui ont été mises en place sur une plus longue période, comme au moment des marchés de Noël qui se sont étendues sur un mois.

De fait, depuis le 1er novembre 2017, ces mesures n'ont fait l'objet que d'un seul contentieux concernant une mesure prise dans le cadre du sommet du G7 organisé à Biarritz en août 2019 : un périmètre de protection avait ainsi été instauré autour du commissariat de Bayonne et du tribunal judiciaire appelés à poursuivre et juger, au même moment que celui du sommet, les infractions commises en marge du sommet du G7 et de son contre-sommet. Le juge des référés a estimé que la mesure était légitime et ne portait pas une atteinte grave et manifestement illégale à la liberté d'aller et de venir. Il l'a toutefois suspendue en tant qu'elle concernait les avocats, au motif qu'elle ne prévoyait pas de les exonérer des mesures d'inspection de leurs

porte-documents, alors que ceux-ci peuvent contenir des documents couverts par le secret professionnel, corollaire des droits à la défense de leurs clients (TA Pau, ordonnance du 23 août 2019, n° 1901885).

A l'exception de cette décision singulière dont les effets sont très limités, l'absence de contentieux à l'encontre de ces mesures constitue le signe de l'utilité de la mesure et de son acceptation sociale. Il est assez rare qu''une mesure nouvelle encadrant l'exercice de la liberté d'aller et venir ne donnent lieu à aucun contentieux. Deux explications peuvent être apportées :

- soit ces mesures ont été vécues comme un « mal nécessaire », au regard de la prégnance de la menace terroriste, pour pouvoir continuer à vivre normalement, illustrant par là même le principe selon lequel l'ordre public est garant de l'exercice des libertés ;
- soit leur mise en œuvre a été suffisamment adaptée et proportionnée pour ne susciter aucune contestation.

De fait, la présence ostensible des forces de l'ordre et d'agents privés de sécurité sur la voie publique à l'occasion d'événements de grande ampleur et rassemblant un public important présente à la fois un effet rassurant pour la population et dissuasif pour les personnes susceptibles de constituer une menace à caractère terroriste.

1.1.4. Une utilité opérationnelle réaffirmée

La mise en œuvre des périmètres de protection a permis depuis le 1er novembre 2017 une meilleure sécurisation d'événements s'étendant sur une période relativement longue. En effet, pour des raisons de disponibilité et de multiplicité de leurs missions, les effectifs de la police ou de la gendarmerie nationales ne peuvent pas assurer seuls des contrôles d'accès pour des événements organisés pendant une longue durée. Ces mesures ont ainsi permis une meilleure sécurisation des grandes manifestations organisées en France (fête nationale du 14 juillet, fêtes de Noël, sommet du G7 ou du G5 Sahel, Tour de France…).

Ces mesures sont avant tout dissuasives : on ne saurait donc inférer du faible nombre de personnes auxquelles il est fait interdiction de pénétrer à l'intérieur du périmètre de protection, au regard du nombre de personnes y pénétrant, ou encore du faible nombre d'armes découvertes lors de la mise en œuvre de ces mesures, pour considérer qu'elles ne sont pas utiles. En effet, leur utilité consiste bien à dissuader ces personnes de pénétrer au sein des lieux protégés, au regard du caractère systématique des contrôles. Par suite, la faiblesse du nombre des personnes repérées lors de ces contrôles illustre précisément la pertinence de cette mesure.

Toutefois, si elles permettent de réduire l'exposition à la menace terroriste, de telles mesures ne permettent pas de conjurer tout risque de passage à l'acte d'une personne déterminée. Aucune mesure ne saurait ainsi garantir un « risque zéro » ainsi que l'illustre l'attentat survenu au marché de Noël de Strasbourg, en décembre 2018, en dépit de l'existence d'un périmètre de protection. En effet, lorsque le périmètre est géographiquement très large et demeure en place pendant une période assez longue (comme c'est le cas pour ce type d'évènement), il est sans

doute plus difficile de maintenir un contrôle permanent de l'accès au lieu, de surcroit lorsque l'auteur de l'attentat réside à l'intérieur du périmètre.

1.2. LES FERMETURES DES LIEUX DE CULTE

L'article 2 de la loi SILT, codifié à l'article L. 227-1 du code de la sécurité intérieure, permet à l'autorité de police administrative, en l'occurrence au représentant de l'État dans le département, de procéder à la fermeture de lieux de culte qui *« en raison des propos qui y sont tenus, des idées ou théories qui y sont diffusées ou des activités qui s'y déroulent, incitent à la discrimination, à la haine, à la violence, à la commission d'actes de terrorisme en France ou à l'étranger, ou font l'apologie de tels agissements ou de tels actes. ».*

1.2.1. Le champ d'application de la mesure est particulièrement encadré :

La finalité de cette mesure est la prévention des actes de terrorisme : elle ne vise donc pas tous les lieux de culte dont le fonctionnement porterait atteinte à l'ordre public, comme pendant l'état d'urgence, mais seulement ceux répondant aux critères précités, très encadrés.

Ces éléments peuvent concerner :

- les messages véhiculés par le lieu de culte de manière active (prêches, organisation de conférences, diffusion d'écrits, invitation de personnalités connues pour leur soutien à l'organisation terroriste Daech, etc.) ou passive (renvoi à des idées ou théories par mise à disposition des fidèles d'ouvrages, de liens internet renvoyant à des sites prosélytes, etc.) ;
- les fréquentations : implication des membres dirigeant le lieu de culte ou de fidèles dans des organisations terroristes ou liens entretenus avec des individus en lien avec ces organisations ;
- les activités organisées au sein du lieu de culte (enseignement coranique exaltant les valeurs du *djihad*, activités sportives constituant des lieux d'endoctrinement ou d'entraînement au *djihad* ; organisation d'une filière de combattants ; activités de soutien aux vétérans du *djihad* ou aux détenus pour des motifs en lien avec le terrorisme, etc.).

Ces indices, dont la liste n'est pas exhaustive, doivent avoir pour objet de provoquer à la violence, à la haine et à la discrimination, de provoquer à la commission d'actes de terrorisme ou de faire l'apologie de tels actes.

1.2.2. La mesure est encadrée par des garanties procédurales classiques en la matière, inhérentes à toute mesure de police restreignant l'exercice d'une liberté :

La décision est **motivée et doit être précédée d'une procédure contradictoire** préalable, conformément au code des relations entre le public et l'administration ;

Elle doit être **nécessaire**, reposer sur des éléments précis et circonstanciés rapportés par l'autorité administrative.

Elle doit être **proportionnée**, il doit être tenu compte, notamment, de la possibilité pour les fidèles d'être accueillis dans d'autres lieux de culte existants dans le voisinage et du risque de création de lieux de culte alternatifs, plus ou moins encadrés (chapiteaux ou salles mis à disposition des fidèles ou prières de rue), qui engendrent alors d'autres troubles à l'ordre public ou favorisent la poursuite de ceux à l'origine de la fermeture.

La **durée** est également encadrée et ne peut excéder six mois. Cette durée doit être mise à profit par les gestionnaires du lieu de culte pour en corriger le fonctionnement (changement du prêcheur, mise en place de mesures de surveillance pour éviter la constitution de groupes dissidents, condamnation explicite des actions terroristes et des thèses véhiculées par les organisations terroristes, etc.) afin de favoriser la réouverture du lieu dans des conditions qui ne permettent pas la réitération des dysfonctionnements ayant justifié la fermeture.

Enfin, la mesure doit être notifiée dans un **délai qui ne peut être inférieur à 48 heures avant son entrée en application**, afin de permettre un éventuel recours en référé devant le juge administratif, dans les conditions prévues à l'article L. 521-2 du code de justice administrative. Ce recours, suspensif, permet de faire trancher la question de l'atteinte grave et manifestement illégale à une liberté fondamentale avant la mise à exécution de la fermeture, sans préjudice d'un éventuel recours en annulation. En revanche, passé le délai de 48 heures, à défaut de saisine du juge ou en cas de rejet de la requête par le tribunal administratif, la mesure peut être exécutée d'office.

Il s'agit là d'une conciliation entre la préservation de la liberté fondamentale que constitue le libre exercice du culte et l'objectif d'efficacité de la mesure, dont la violation est au surplus assortie d'une sanction pénale dissuasive prévue à l'article L. 227-2 du CSI (six ans d'emprisonnement et 7 500 € d'amende).

1.2.3. Une mesure jugée conforme à la Constitution

Dans sa décision n° 2017-695 QPC du 29 mars 2018 précitée, le Conseil constitutionnel a jugé que le législateur a assuré une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public, au nombre desquels figure la prévention du terrorisme et, d'autre part, la liberté de conscience et le libre exercice des cultes.

Il a relevé à cet égard, en particulier, que lorsque la justification de la mesure de fermeture d'un lieu de culte repose sur la provocation à la violence, à la haine ou à la discrimination, il appartient au préfet d'établir que cette provocation est bien en lien avec le risque de commission d'actes de terrorisme.

En outre, le Conseil constitutionnel a souligné l'existence de plusieurs garanties : le législateur a limité à six mois la durée de la mesure et n'a pas prévu qu'elle puisse être renouvelée. L'adoption ultérieure d'une nouvelle mesure de fermeture ne peut reposer que sur des faits intervenus après la réouverture du lieu de culte. La fermeture du lieu de culte doit être justifiée et proportionnée, notamment dans sa durée, aux raisons l'ayant motivée. Enfin, elle peut faire l'objet d'un recours en référé devant le juge administratif. Elle est alors suspendue jusqu'à la décision du juge de tenir ou non une audience publique. S'il décide de tenir cette audience, la suspension de la mesure se prolonge jusqu'à sa décision sur le référé, qui doit intervenir dans les quarante-huit heures.

1.2.4. Une utilisation très mesurée

Depuis le 1er novembre 2017, huit lieux de culte ont été fermés pour une durée de six mois, trois n'ayant pas rouvert à l'échéance de la mesure du fait de l'intervention de mesures complémentaires, l'association gérant ce lieu de culte ayant ensuite été dissoute, le bail ayant été résilié ou non renouvelé, ou l'imam expulsé et non remplacé. Au nombre desquelles :

- la mosquée « Dar Es Salam » (dite « mosquée Calendal ») à Aix-en-Provence (13), fermée par arrêté du préfet de police des Bouches-du-Rhône du 16 novembre 2017, arrivé à échéance le 18 mai 2018 ; le propriétaire des locaux ayant résilié le bail en novembre 2017, ce lieu de culte est désormais définitivement fermé ;
- la salle de prière « salle des Indes » à Sartrouville (78), fermée par arrêté du préfet des Yvelines du 17 novembre 2017, arrivé à échéance le 20 mai 2018 ; le propriétaire des locaux a résilié le bail et la résiliation a été confirmée par le juge des référés du tribunal de grande instance de Versailles par ordonnance du 17 mai 2018 ; le lieu de culte n'a donc pas rouvert ;
- la mosquée « As Sounna » à Marseille (13), fermée par arrêté du préfet de police des Bouches-du-Rhône du 11 décembre 2017, arrivé à échéance le 13 juin 2018 ; le bail concernant la partie locative des locaux a été résilié fin 2017, le reste de la mosquée appartenant à un membre de l'association ; l'association gestionnaire du lieu de culte (« Association des musulmans du boulevard national (AMN Assouna) ») a été dissoute par décret du 31 août 2018 et son président, M. El Hadi DOUDI, a été expulsé du territoire français ; le président et l'association gestionnaire font par ailleurs l'objet d'un arrêté ministériel de gel des avoirs en date du 28 novembre 2017, renouvelé par arrêté du 31 mai 2018 ;
- la salle de prière « Abu Darda » de Gigean (34), fermée par arrêté du préfet de l'Hérault du 14 mai 2018 au 16 novembre 2018 ; le lieu de culte n'a pas rouvert depuis ; le président de l'association gestionnaire de ce lieu de culte a démissionné de ses fonctions en juillet 2018 et n'a toujours pas été remplacé ; l'imam, qui fait l'objet d'un arrêté ministériel de gel de ses avoirs, a cessé ses fonctions au sein de la salle de prière ;
- la salle de prière du « centre Zahra » à Grande-Synthe (59), fermée par arrêté du préfet du Nord du 15 octobre 2018, en vigueur jusqu'au 17 avril 2019 ; l'association gestionnaire et les trois associations en lien avec cette association, à savoir le Fédération *Chiite de France,*

l'association « *Parti Anti Sioniste* » et l'association « *France Marianne Télé* ont ensuite été dissoutes, par décret en date du 20 mars 2019 ;

- la mosquée « As-Sunnah » à Hautmont (59), fermée par arrêté du préfet du Nord du 13 décembre 2018, arrivé à échéance le 15 juin 2019. Le lieu de culte n'a pas rouvert à l'expiration de la mesure ;
- la mosquée « Al-Kawthar » à Grenoble (38), fermée par arrêté du préfet de l'Isère du 4 février 2019, arrivé à échéance le 7 août 2019. Le lieu de culte a rouvert le 11 août 2019. L'arrêté préfectoral prononçant la fermeture de la mosquée « Al-Kawthar » de Grenoble (38) était essentiellement motivé par les propos tenus par l'imam (qui a fait l'objet d'un arrêté d'expulsion le 12 juillet 2019 et a depuis quitté le territoire) ainsi que par la diffusion de ces propos sur Internet.
- la grande mosquée de Pantin (93) fermée par arrêté du préfet de la Seine-Saint-Denis du 19 octobre 2020 pour une durée de six mois, fermeture toujours en cours.

Il est relevé qu'aucune de ces fermetures n'a pu être prononcée en prenant en compte les seuls propos tenus par l'imam au sein du lieu de culte, ceux-ci étant désormais « lissés », jusqu'à contenir des condamnations expresses des actes de terrorisme. Seuls quelques soutiens explicites aux *djihadistes*, mais le plus souvent, ce soutien prend la forme de messages subliminaux, contenus dans les prêches ou dans des images.

C'est donc par le critère des *« idées et théories diffusées* » par le lieu de culte par d'autres vecteurs que les prêches (sites internet, réseaux sociaux, ouvrages mis à la disposition des fidèles, conférences organisées ou prêcheurs invités, publicités pour des conférences ou des ouvrages, activités organisées, etc.) qu'il est seulement désormais possible de démontrer qu'au sein de tel ou tel lieu de culte il est soit provoqué à la violence, à la haine ou à la discrimination en vue d'inciter à la commission d'un acte de terrorisme, soit provoqué à la commission d'actes de terrorisme ou en fait l'apologie (cf. TA Lille, 19 octobre 2018, *Centre Zahra*, n° 1809278).

C'est également en se fondant sur ce critère que le Conseil d'État a estimé que la diffusion, le 9 octobre 2020, sur le compte « Facebook » de la Grande mosquée de Pantin, d'une vidéo exigeant l'éviction d'un professeur d'histoire parce qu'il avait dispensé quelques jours plus tôt un cours sur la liberté d'expression au travers notamment de caricatures, ainsi que d'un commentaire mentionnant sur ce même compte l'identité de ce professeur, M. Samuel Paty, lequel a ensuite été assassiné, constitue des propos provoquant à la violence et à la haine en lien avec le risque de commission d'actes de terrorisme (cf. CE, 25 novembre 2020, *Fédération musulmane de Pantin*, n° 446303

La difficulté à établir directement les critères permettant de prononcer une fermeture oblige à une enquête longue et minutieuse, ce qui explique le faible nombre de mesures prononcées. Il s'agit toutefois, pour les autorités publiques, d'étayer suffisamment ces mesures pour que l'atteinte portée à la liberté de conscience et au libre exercice du culte soit parfaitement justifiée et proportionnée.

D'ailleurs, à l'exception de celle de la mosquée de Gigean, toutes les fermetures de lieu de culte ont donné lieu à contentieux, le juge ayant, dans tous les cas, considéré que la mesure était justifiée.

1.2.5. Des décisions systématiquement confirmées par le juge administratif

De manière constante, le juge administratif reconnaît que la liberté du culte a le caractère d'une liberté fondamentale qui ne se limite pas au droit de tout individu d'exprimer les convictions religieuses de son choix dans le respect de l'ordre public, mais porte également sur la libre disposition des biens nécessaires à l'exercice d'un culte. Aussi, un arrêté prescrivant la fermeture d'un lieu de culte est susceptible de porter atteinte à la liberté de culte et au droit de propriété.

Pour autant, compte tenu des motifs allégués et des buts poursuivis par ces mesures, toutes les fermetures prononcées sous l'empire de l'état d'urgence, mais également de la loi « SILT », ont été considérées comme ne portant pas une atteinte grave et manifestement illégale à ces libertés fondamentales, que ce soit dans l'appréciation de la menace que constitue le lieu de culte ou dans la détermination des modalités de la fermeture.

La méthode du faisceau d'indices à laquelle a recouru le juge est illustrative de la variété des motifs permettant de recourir à la fermeture d'un lieu de culte, les propos tenus par l'imam lors des prêches ne constituant que l'un des indices, minoritaire aujourd'hui, de la radicalisation d'un lieu de culte.

Ainsi, pour la fermeture de la salle de prière des Indes à Sartrouville, le tribunal administratif de Versailles, puis le Conseil d'État ont retenu « *que l'imam principal et les imams invités de ce lieu de culte tenaient des propos radicaux incitant notamment à la haine envers les fidèles d'autres religions et au rejet des valeurs de la République, que compte tenu de son orientation, la mosquée était fréquentée, de manière habituelle, tant pour les prières que pour les enseignements qui y étaient dispensés, par des personnes radicalisées venant de différents départements voisins, en particuliers des jeunes femmes dont plusieurs portant le voile intégral et dont l'une a rejoint la Syrie, ainsi que des individus en lien avec des filières terroristes, que dans la salle de prière se trouvait en juillet 2017 un tableau évoquant l'organisation de sports de combat surmonté de l'inscription " guerre sainte des jeunes musulmans " et que l'influence radicale de ce lieu de culte s'étendait à l'ensemble de la vie locale, en particulier sur les plus jeunes »* (CE, 11 janvier 2018, n° 416398).

S'agissant de la mosquée Assouna, à Marseille, le Conseil d'Etat a retenu que cette mosquée *« a diffusé, à travers les prêches de son imam, M. Doudi, également président de l'association requérante gestionnaire de ce lieu de culte, dont certains sont publiés sur son site internet, des appels à la haine et à la violence contre les Chrétiens, les Juifs, les Chiites et les personnes adultères, en des termes particulièrement explicites »* (CE, 31 janvier 2018, *Association AMN Assouna*, n° 417332).

S'agissant de la mosquée du Centre Zahra de Grande Synthe, le juge des référés du tribunal administratif a considéré que *« si les allusions faites aux différentes formes de djihad lors des*

prêches des 22 décembre 2017 et 5 janvier 2018 ne constituent pas, dans les circonstances de l'espèce, une provocation à la violence, à la haine ou à la discrimination ou à la commission d'actes de terrorisme et ne peuvent davantage être regardés comme ayant pour objet de faire l'apologie de tels actes (….) le préfet s'est également fondé sur la mise à la disposition des fidèles fréquentant le lieu de culte ainsi que sur la mise en ligne sur les sites internet de l'association de même que sur celui du parti antisioniste, de passages appelant à la violence, à la haine et à la discrimination ainsi qu'à la commission d'actes de terrorisme ou faisant l'apologie de tels actes. Parmi les ouvrages et les écrits mis à la disposition des personnes fréquentant le « centre Zahra » ou dont il est assuré la promotion sur les sites internet de l'association requérante et du parti antisioniste, certains comportent des passages incitant explicitement à la destruction de l'Etat d'Israël, à tuer des personnes de confession juive ou justifiant la possibilité de l'asservissement des prisonniers de guerre dans le cadre d'une guerre menée au nom du djihad ou le recours à celui-ci. Un communiqué du 19 mai 2016 présent sur le site de la requérante rend par ailleurs expressément hommage, à l'occasion de son décès, au combat mené par le commandant militaire en chef du Hezbollah contre « l'entité sioniste », alors que la branche armée de cette organisation est inscrite sur la liste des organisations terroristes établie par l'Union européenne. En outre, les écrits ainsi diffusés génèrent sur le site Internet de l'association requérante et du « parti antisioniste », de la part de leurs lecteurs, des commentaires qui constituent par eux-mêmes une provocation à la haine et à la discrimination notamment envers les personnes de confession juive, sans que les associations responsables de ces sites ne procèdent à une quelconque modération des propos diffusés. Par ailleurs, la circonstance que certains de ces ouvrages et écrits puissent être disponibles au sein d'institutions telle que la Bibliothèque nationale de France est sans incidence sur la portée du contenu de ces ouvrages et des idées et théories qui y sont énoncées ou sur la portée du contenu de ces ouvrages et des idées et théories qui y sont énoncées ou sur l'utilisation qui peut en être faite à des fins de provocation à la haine et à la violence ou à l'apologie du terrorisme » (TA Lille, 19 octobre 2018, *Association centre Zahra France*, n° 1809278)**.**

Enfin, s'agissant de la Grande mosquée de Pantin, le Conseil d'État a estimé que « *la diffusion, le 9 octobre 2020, sur le compte « Facebook » de la Grande mosquée de Pantin, d'une vidéo exigeant l'éviction d'un professeur d'histoire parce qu'il avait dispensé quelques jours plus tôt un cours sur la liberté d'expression au travers notamment de caricatures, ainsi que d'un commentaire mentionnant sur ce même compte l'identité de ce professeur, M. Samuel Paty, constitue des propos provoquant à la violence et à la haine en lien avec le risque de commission d'actes de terrorisme ».* En outre, le Conseil d'État a relevé que *« l'imam principal de la mosquée a été formé dans un institut fondamentaliste du Yémen, que ses prêches sont retransmis, avec la mention de son rattachement à la « Grande mosquée de Pantin », sur un site internet qui diffuse des fatwas salafistes de cheikhs saoudiens et qu'il est impliqué dans la mouvance islamiste radicale d'Île-de-France »* et que « *la Grande mosquée de Pantin est devenue un lieu de rassemblement pour des individus appartenant à la mouvance islamique radicale dont certains n'habitent pas le département de Seine-Saint-Denis et ont été impliqués dans des projets d'actes terroristes ».*

1.2.6. Une durée de fermeture fixée à six mois et un contrôle du juge sur les

mesures correctrices mises en avant pour obtenir la fin anticipée de la fermeture

Si l'ensemble des mesures de fermeture de lieux de culte ont été prononcées pour une durée de six mois, aucune n'a pu être abrogée de manière anticipée en raison d'un changement d'orientation du lieu dans un délai compatible avec une abrogation.

En effet, l'expérience montre que les quelques lieux de culte qui ont souhaité apporter des gages d'un changement d'orientation n'ont pas été à même de mener à bien toutes les procédures nécessaires de manière à permettre d'anticiper la fin de la fermeture.

Chaque fois qu'il a été saisi du refus d'abrogation anticipée de la décision de fermeture, le juge des référés a estimé que si les mesures correctrices proposées étaient de la nature de celles qui pourraient permettre de fonder une telle demande, elles n'étaient intervenues que très récemment et les modalités de mise en œuvre de plusieurs d'entre elles, en particulier la désignation de l'imam ou des personnes autorisées à intervenir dans la mosquée et les mesures de surveillance, tant du contenu des prêches que des personnes se rendant dans ce lieu, n'étaient pas précisées. Dans ces conditions, l'association a été regardée comme n'établissant pas qu'elle serait en mesure d'éviter la réitération des graves dérives constatées dans un passé récent et la menace à l'ordre et la sécurité publics qui en étaient résulté (CE, 11 janvier 2018, n° 416398).

De fait, il est très difficile de réduire la durée de fermeture d'un lieu de culte à moins de six mois, cette durée semblant entièrement nécessaire à ses gestionnaires pour adopter les mesures correctrices qui s'imposent, afin d'éviter de réitérer les dysfonctionnements ayant justifié la fermeture.

Enfin, l'application de la loi a montré que certains lieux de culte faisant l'objet d'une fermeture continuaient néanmoins à fonctionner dans des lieux annexes dépendant du lieu de culte (école coranique, bibliothèque, centre de loisirs…) faisant ainsi échec à la mesure de fermeture. C'est pourquoi, l'article 2 du présent projet de loi propose une modification de l'article L. 227-1 du code de la sécurité intérieure permettant de fermer, outre le lieu de culte lui-même, les lieux en dépendant, lorsqu'ils sont susceptibles de faire échec à la mesure de fermeture du lieu de culte (voir *infra*).

1.3. LES MESURES INDIVIDUELLES DE CONTROLE ADMINISTRATIF ET DE SURVEILLANCE (MICAS)

La mesure introduite par les articles L. 228-1 et suivants du code de la sécurité intérieure est inspirée de celle prévue à l'article L. 225-1 du même code relative au contrôle administratif des retours sur le territoire national ainsi que de la mesure d'assignation à résidence prévue à l'article 6 de la loi du 3 avril 1955 relative à l'état d'urgence. Elle s'inscrit cependant dans un cadre juridique beaucoup plus exigeant que celui des assignations à résidence de l'état d'urgence, qu'il s'agisse des finalités de la mesure, des conditions de sa mise en œuvre ainsi que des personnes concernées.

1.3.1. Un régime très encadré jugé conforme à la Constitution

Les mesures individuelles de contrôle administratif et de surveillance ne peuvent être mises en œuvre qu'à des fins de prévention d'actes de terrorisme et non au regard d'une simple menace pour l'ordre et la sécurité publics, comme en période d'état d'urgence.

Une personne est susceptible de voir prononcer à son encontre une telle mesure lorsque sont remplis au moins deux critères dont le premier est obligatoire et le second alternatif :

- son comportement doit constituer une menace d'une particulière gravité pour la sécurité et l'ordre publics, cette menace devant, selon l'interprétation qu'en a donnée le Conseil constitutionnel, être en lien avec la commission d'actes de terrorisme ;
- et elle doit par ailleurs entrer en relation de manière habituelle avec des personnes ou organisations incitant, facilitant ou participant à des actes de terrorisme et/ou soutenir, diffuser ou adhérer à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes, ces deux derniers critères pouvant être cumulés.

La mesure est prononcée pour une durée maximale de trois mois, renouvelable dans la limite d'une durée cumulée de douze mois. En outre, des éléments nouveaux ou complémentaires sont nécessaires pour renouveler la mesure au-delà de six mois. Enfin, chaque renouvellement est subordonné à sa notification au moins cinq jours avant l'expiration de la mesure en cours, la personne concernée pouvant saisir le juge de l'excès de pouvoir dans les 48h, celui-ci devant statuer sous 72h et la mesure n'entrant pas en vigueur avant sa décision.

Cet encadrement a amené le Conseil constitutionnel a déclaré les dispositions du code de la sécurité intérieure relatives aux MICAS conformes à la Constitution (décision n° 2017-691 QPC du 16 février 2018) en relevant tout d'abord qu'en créant ces mesures, le législateur avait poursuivi l'objectif de lutte contre le terrorisme, qui participe de l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et défini avec précision les conditions de recours à la mesure de police en cause en limitant son champ d'application à des personnes soupçonnées de présenter une menace d'une particulière gravité pour l'ordre public.

En outre, le Conseil constitutionnel a relevé que :

- la définition du champ géographique de la mesure et des modalités de présentation aux services de police doit permettre à l'intéressé de poursuivre une vie familiale et professionnelle ;
- la durée de la mesure et ses conditions de renouvellement sont strictement encadrées et proportionnées.

Si ce cadre général, qui assure l'équilibre entre l'objectif de lutte contre le terrorisme et le respect des droits et libertés constitutionnellement garantis des personnes concernées, a donc été validé par le juge constitutionnel, quelques détails du dispositif ont néanmoins été censurés et ont fait l'objet d'une correction immédiate par le législateur.

En premier lieu, le législateur avait initialement prévu que les décisions de renouvellement des mesures individuelles de contrôle administratif et de surveillance prise sur le fondement ses articles L. 228-2 et L. 228-5 du code de la sécurité intérieure soient notifiées cinq jours au moins avant leur entrée en vigueur pour permettre à la personne concernée de saisir éventuellement le juge du référé, sur le fondement de l'article L. 521-2 du code de justice administrative, dans un délai de 48h à compter de la notification, le juge des référés disposant alors d'un délai de 72h pour statuer et l'entrée en vigueur étant différée jusqu'à l'intervention de la décision du juge.

Le Conseil constitutionnel a toutefois considéré, dans sa décision n° 2017-691 QPC du 16 février 2018, que l'office du juge fondé sur l'article L. 521-2 du code de justice administrative (CJA) et limité au contrôle des seules atteintes graves et manifestement illégales à une liberté fondamentale était insuffisant et devait au contraire porter sur la régularité et le bien-fondé de la décision de renouvellement.

Afin de concilier un contrôle du juge de l'excès de pouvoir et un délai de jugement compatible avec les exigences de continuité entre la mesure initiale et son renouvellement, le législateur a, dans la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice (article 65) modifié les articles L. 228-2 et L. 228-5 en maintenant les mêmes délais (notification cinq jours avant l'entrée en vigueur du renouvellement, délai de recours de 48h et délai de jugement de 72h) en prévoyant toutefois que le juge statuait sur la légalité de la mesure, moyennant des aménagements de procédure (délai de recours de 48h, délai de jugement de 72h et dispense de rapporteur public).

En deuxième lieu, s'agissant des recours classiques contre les décisions prises sur le fondement de l'article L. 228-1 et suivants, donc hors les cas de renouvellement précités, le Conseil constitutionnel (décision n° 2017-691 QPC du 16 février 2018) avait estimé les délais initialement prévus trop courts s'agissant du délai de recours et trop long s'agissant du délai de jugement, compte tenu de la durée de trois mois des mesures en cause. La loi n° 2019-222 du 23 mars 2019 précitée a modifié ces délais en rétablissant un délai de recours de droit commun de deux mois mais en imposant un délai de jugement de quinze jours ou d'un mois selon la nature de la mesure en cause.

Le décret n° 2019-1495 du 27 décembre 2019 portant application de l'article L. 773-10 du code de la justice administrative a tiré les conséquences de ces aménagements de procédure.

Ces critères exigeants, garants de l'équilibre entre l'objectif de lutte contre le terrorisme et le respect des droits et libertés constitutionnellement protégés des personnes concernées, expliquent le faible nombre de MICAS sollicitées et prononcées. Ainsi, sur la dernière année d'application, seulement 166 propositions de MICAS ont été sollicitées et 143 ont effectivement été prononcées, les autres individus ayant été pris en compte autrement, parfois du fait de leur placement en détention postérieurement à la demande ou par d'autres moyens de surveillance.

	Mesures initiales	Abrogations	Renouvellements		
			3 mois	6 mois	9 mois

1ère année d'application	**73**	13	41	27	5
2e année d'application	**134**	33	67	19	7
3e année d'application	**143**	42	73	19	7
Cumul depuis le 01/11/2017	**350**	88	181	65	19

1.3.2. Des modalités de surveillance adaptées à chaque situation

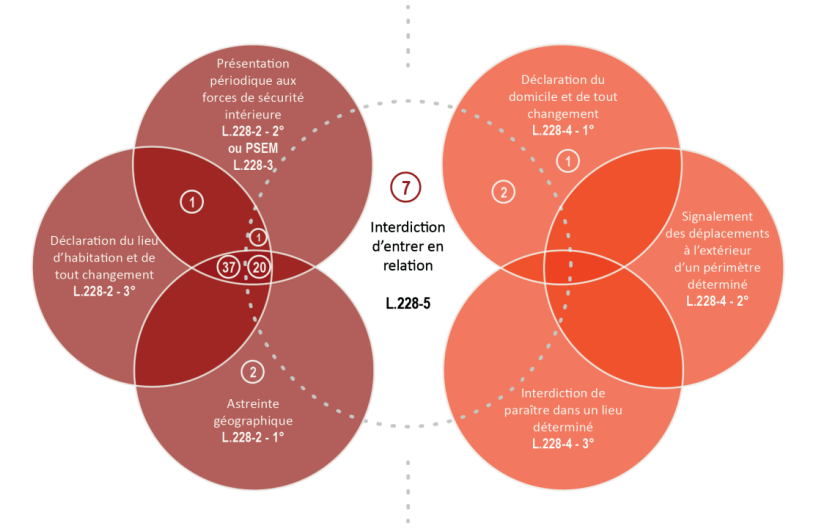
L'article L. 228-1 du code de la sécurité intérieure prévoit la possibilité pour le ministre de l'intérieur d'enjoindre à une personne à l'égard d'une personne faisant l'objet d'une MICAS. de respecter un certain nombre d'obligations, pouvant varier en fonction du degré de surveillance nécessité par son comportement.

La personne placée sous une telle mesure peut ainsi faire l'objet de deux régimes d'obligations, alternatifs, dont la durée est variable au regard de leur intensité :

- celui prévu aux articles L. 228-2 et L. 228-3 du code de la sécurité intérieure, parmi lesquelles figurent l'obligation de ne pas se déplacer à l'extérieur d'un périmètre géographique déterminé, de se présenter périodiquement aux services de police ou aux unités de gendarmerie, dans la limite d'une fois par jour, ou à défaut de faire l'objet d'un placement sous surveillance électronique mobile, de déclarer son lieu d'habitation et tout changement de lieu d'habitation. Ces obligations peuvent être prononcées pour une durée maximale de trois mois, renouvelable dans la limite d'une durée cumulée de douze mois, leur renouvellement étant subordonné à la démonstration d'éléments nouveaux et complémentaires au-delà d'une durée de six mois.

- celui prévu à l'article L. 228-4 du même code, lorsque l'intéressé ne fait pas l'objet des obligations prévues aux articles L. 228-2 et L. 228-3, par lequel le ministre peut faire obligation à la personne concernée de déclarer son domicile et tout changement de domicile, de signaler ses déplacements à l'extérieur d'un périmètre déterminé ne pouvant être plus restreint que le territoire de la commune de son domicile, de ne pas paraître dans un lieu déterminé, qui ne peut inclure le domicile de la personne intéressée, en tenant compte de la vie familiale et professionnelle de la personne intéressée. Ces obligations peuvent être prononcées pour une durée maximale de six mois, renouvelable dans la limite d'une durée cumulée de douze mois, leur renouvellement étant subordonné à la démonstration d'éléments nouveaux et complémentaires au-delà d'une durée de six mois.

Enfin, au titre de l'article L. 228-5, le ministre peut faire interdiction aux personnes soumises à l'un ou l'autre régime, de ne pas se trouver en relation directe ou indirecte avec certaines personnes, nommément désignées, dont il existe des raisons sérieuses de penser que leur comportement constitue une menace pour la sécurité publique. Cette interdiction peut être prononcée pour une durée maximale de six mois, renouvelable dans la limite d'une durée cumulée de douze mois, son renouvellement étant subordonné à la démonstration d'éléments nouveaux et complémentaires au-delà d'une durée de six mois.



Obligations prévues par les articles L. 228-2 à L. 228-5 CSI

1.3.3. Le placement sous surveillance électronique mobile comme alternative à l'obligation de présentation périodique aux forces de police ou de gendarmerie (art. L. 228-3 CSI)

Un tel dispositif permet de vérifier à distance – mais sans géolocalisation – le respect par l'intéressé de l'obligation de résidence dans un périmètre géographique déterminé, sans qu'il y ait besoin pour ce dernier de se déplacer au commissariat de police ou à la brigade de gendarmerie.

Le placement sous surveillance électronique mobile est décidé par le ministre de l'intérieur mais est subordonné à l'accord préalable de l'intéressé. Dans ce cas, le périmètre géographique est élargi au département. En cas de dysfonctionnement temporaire du dispositif ou à tout instant sur décision ministérielle (dans l'hypothèse par exemple d'un refus réitéré de l'intéressé de se conformer à ses obligations), l'obligation de présentation périodique aux forces de police ou de gendarmerie peut être rétablie.

Les modalités de mise en œuvre du placement sous surveillance électronique mobile ont été précisées par le décret n° 2018-167 du 7 mars 2018[6], qui couvre à la fois les mesures

[6] Décret pris pour application de l'article 6 de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et de l'article L. 228-3 du code de la sécurité intérieure.

individuelles de contrôle administratif et de surveillance et les assignations à résidence décidées sur le fondement de l'article 6 de la loi du 3 avril 1955 relative à l'état d'urgence[7].

Compte tenu du faible nombre de personnes susceptibles de bénéficier simultanément de cette possibilité (une dizaine au maximum), il a été convenu, dans un souci de bonne administration, de recourir au dispositif utilisé par les services de l'administration pénitentiaire pour la surveillance des personnes placées sous surveillance électronique mobile par l'autorité judiciaire.

Pour ce faire, une convention de délégation de gestion entre le ministère de la justice et le ministère de l'intérieur a été signée le 6 août 2018 par les directeurs de l'administration pénitentiaire d'une part et des libertés publiques et des affaires juridiques d'autre part ; elle précise l'objet de la délégation, les prestations accomplies par le ministre de la justice et les obligations incombant à chaque partie.

Aucun placement sous surveillance électronique mobile (PSEM) comme modalité alternative de surveillance n'a été demandé par les personnes concernées alors que pourtant ce mode de surveillance est moins contraignant puisqu'il permet d'élargir le périmètre de résidence à l'échelle du département.

1.3.4. Une prise en compte de la vie privée, familiale et professionnelle

Si le régime de l'assignation à résidence prévu par la loi du 3 avril 1955 permet au ministre de l'intérieur de choisir lui-même à la fois le ressort géographique de la personne qui en fait l'objet et le lieu d'habitation où elle peut être, de surcroît, astreinte à résider pendant une plage horaire d'une durée maximum de douze heures, celui de la mesure individuelle de contrôle administratif et de surveillance impose de déterminer un périmètre géographique permettant à l'intéressé de *« poursuivre une vie familiale et professionnelle »* – en principe le ressort communal – et qui *« s'étend, le cas échéant, aux territoires d'autres communes ou d'autres départements que ceux de son lieu habituel de résidence. ».*

Dans ces conditions, lorsqu'elles préexistent à la mesure, les obligations d'ordre familial (par exemple une garde d'enfant alternée) ou professionnel (p. ex. le lieu de travail situé sur le territoire d'une autre commune que celle de résidence) sont systématiquement prises en compte dans l'arrêté.

En revanche, une obligation professionnelle qui découlerait d'une décision de l'intéressé postérieure au prononcé de la mesure (nécessité par exemple d'effectuer des déplacements de plusieurs dizaines, voire centaines de kilomètres) n'implique pas, par elle-même, de

[7] La loi n° 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions a donné la possibilité au ministre de l'intérieur d'ordonner le placement sous surveillance électronique mobile de toute personne assignée à résidence, lorsque cette dernière a été condamnée à une peine privative de liberté pour un crime qualifié d'acte de terrorisme ou pour un délit recevant la même qualification puni de dix ans d'emprisonnement et a fini l'exécution de sa peine depuis moins de huit ans, et avec son accord.

modification systématique du périmètre géographique, si cet aménagement est jugé incompatible avec l'objectif de surveillance de la mesure.

Autrement dit, il appartient à l'autorité administrative d'apprécier si l'aménagement de la mesure sollicité (élargissement du périmètre, réduction des présentations…) est compatible ou non avec l'objectif de surveillance poursuivi (CE, 26 juillet 2018, n° 422322 : *« Eu égard au déplacements qui doivent être quotidiennement effectués par le titulaire de cet emploi et à leur caractère imprévisible, il n'apparait pas qu'en l'état de l'instruction, le refus du ministre d'Etat, ministre de l'intérieur, d'élargir le périmètre de la mesure pour permettre à M. X l'exercice de cet emploi aurait apporté une atteinte grave et manifestement illégale aux libertés fondamentales invoquées. »*).

1.3.5. Des obligations aménageables de façon durable ou ponctuelle

Toute personne faisant l'objet d'une mesure individuelle de contrôle administratif et de surveillance a également la possibilité de bénéficier, sur justificatif (contrat de travail, document faisant apparaître le lieu de travail et les horaires de présence au travail, emploi du temps scolaire, obligations familiales, trajet emprunté et temps de trajet, etc.), d'un **aménagement** de ses obligations afin d'accomplir une activité ou une démarche en dehors du périmètre géographique fixé par l'arrêté ou à un moment qui empêche la présentation au service de police ou de gendarmerie à l'heure fixée par l'arrêté.

Aucun aménagement n'est de droit, y compris pour accomplir des démarches administratives ou participer à une audience. Cette tolérance est toujours appréciée avec la plus grande attention par l'autorité administrative, au regard des considérations opérationnelles qui doivent primer dans tous les cas. Il a d'ailleurs été jugé que le refus d'octroyer un aménagement ponctuel à un individu pour se rendre à l'audience ne méconnaissait pas le droit au procès équitable, dès lors que l'intéressé avait la possibilité de se faire représenter par un avocat et compte tenu de sa dangerosité (cf. TA Paris, 6 avril 2017, n° 1704886 : *« Considérant que M. D. soutient que, en refusant de lui délivrer un sauf-conduit pour lui permettre d'assister à l'audience de référé du tribunal administratif, la présente procédure juridictionnelle méconnait les dispositions de l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et le droit à un procès équitable ; que, toutefois, M. D. est représenté à l'audience par son avocat et n'était pas tenu de comparaitre personnellement devant le juge des référés ; qu'en outre le ministre de l'intérieur, dans l'exercice de son pouvoir d'appréciation, a motivé son refus de délivrer un sauf-conduit par des raisons de sécurité publique ; que, dans ces conditions, la circonstance que M. D. n'ait pas été autorisé à assister en personne à l'audience des référés n'entache pas d'irrégularité la présente procédure juridictionnelle »*).

Sont ainsi généralement acceptés les aménagements ponctuels exigés pour des démarches administratives, professionnelles, médicales ou liées à la vie familiale. Sont en revanche refusées les demandes d'aménagement pour des motifs de consommation ou de loisirs, lorsque notamment l'aménagement implique un trop grand écart avec les objectifs poursuivis par la

mesure ou permet à l'intéressé de se trouver dans une situation lui ouvrant la possibilité de commettre un acte dangereux.

Il est en outre impossible d'obtenir la **suspension temporaire** de la mesure de contrôle administratif et de surveillance pour se rendre à l'étranger, qu'il s'agisse d'un voyage pour convenances personnelles ou d'ordre professionnel. A noter tout de même une décision juridictionnelle rendue sur une mesure très voisine, l'interdiction de sortie du territoire prévue à l'article L. 224-1 du CSI, dans laquelle le tribunal administratif de Paris a autorisé une personne faisant l'objet d'une telle interdiction à se rendre dans son pays d'origine pour assister aux funérailles de sa mère (cf. TA Paris, ordonnance du 7 avril 2016, *M. K.*, n° 1605032 : *« si à la date à laquelle la mesure d'interdiction de sortie du territoire a été renouvelée, le 6 novembre 2015, l'actualité des craintes de déplacement de M. K. à l'étranger pour participer à des activités terroristes ou pour se rendre sur un théâtre d'opérations de groupements terroristes, dans des conditions susceptibles de porter une atteinte à la sécurité publique doit être regardée comme établie, ces craintes ont, dans le contexte très particulier du deuil dans lequel se trouve l'intéressé et eu égard à son comportement actuel, perdu de leur intensité ; que, dans ces conditions, l'arrêté du 6 novembre 2015 porte une atteinte manifestement illégale au droit de M. K. à sa vie privée et familiale et à sa liberté d'aller et de venir ; que, par suite, il y a lieu de suspendre l'exécution de cet arrêté durant 48 heures, ainsi que le requérant le demande, et de remettre à M. K. tout document lui permettant de se présenter à la frontière franco-tunisienne afin qu'il puisse assister aux obsèques de sa mère dans la région de Tunis. »).*

Selon les cas et après examen de la requête, lorsque la demande est considérée comme dûment justifiée et ne compromet par les objectifs de la surveillance, un **sauf-conduit** délivré par le ministre de l'intérieur peut autoriser l'intéressé à quitter temporairement le périmètre géographique dans lequel il a l'obligation de résider ou à déroger à son obligation de présentation au service de police ou de gendarmerie. Il en va de même lorsque la demande implique une modification permanente des obligations initiales, le plus souvent à des fins professionnelles. Dans ce cas, un arrêté modifiant les dispositions de l'arrêté initial est notifié à l'intéressé.

A noter que le nombre des demandes de sauf-conduits ponctuels est en nette augmentation (477 demandes contre 383 l'année précédente et 174 la première année), soit un total de 1055 demandes sur les trois premières années d'application de la loi, et ce, malgré le confinement et la crise sanitaire au cours de l'année 2020. 848 demandes ont été acceptées principalement pour des motifs professionnels ou en raison de démarches administratives en lien avec le suivi judiciaire des personnes en raison de l'augmentation corrélative du nombre d'individus sortants de prison placés sous MICAS (convocations judiciaires auprès du tribunal et du service pénitentiaire d'insertion et de probation, obligation de trouver un emploi, suivi associatif, etc). Par ailleurs, 107 demandes ont été refusées car liées à des convenances personnelles sans lien avec le maintien de la vie privée et familiale et 100 abandonnées pour disparition du besoin.

1.3.6. La nécessité d'éléments nouveaux ou complémentaires pour renouveler les obligations au-delà de six mois et la durée cumulée maximale de douze

mois rendent encore plus restrictif le régime de ces mesures

La durée pour laquelle peuvent être imposées, par le ministre de l'intérieur, des obligations à une personne entrant dans le champ d'application des mesures de contrôle administratif et de surveillance varie selon que ces obligations relèvent du premier groupe (art. L. 228-2) ou du second groupe (art. L. 228-4 et L. 228-5) d'obligations : trois mois dans le premier cas, six mois dans le second. Dans tous les cas, lorsque le ministre de l'intérieur souhaite maintenir une obligation au-delà de six mois, il doit justifier de l'existence :

- soit d'éléments nouveaux : il s'agit de faits survenus postérieurement à la date de notification de l'obligation à l'intéressé et venant s'ajouter aux faits ayant justifié la surveillance de ce dernier ;
- soit d'éléments complémentaires : les faits qui ont motivé la mise en œuvre d'une mesure individuelle de contrôle administratif et de surveillance peuvent parfois être précisés (par les enquêtes des services de renseignement) ou avoir des conséquences à plus long terme (condamnation judiciaire survenant plusieurs mois ou années après la commission des faits).

A l'usage, cette condition tenant à l'existence d'éléments nouveaux ou complémentaires apparaît peu pertinente :

- d'une part, se sachant surveillées, les personnes visées adoptent diverses stratégies destinées à éviter d'être repérées, de sorte qu'il est difficile, pour les services, de mettre en évidence les éléments nouveaux ou complémentaires exigés par la loi ;
- d'autre part, compte tenu de la nécessité de verser au débat contentieux l'ensemble des éléments qui fondent la décision, les services de renseignement peuvent hésiter à livrer des informations issues de la mise en œuvre de techniques de renseignement en cours, qui permettraient de démontrer la satisfaction de la condition posée par la loi mais dont la communication, dans le cadre de la procédure contentieuse contradictoire, donnerait à la personne surveillée des informations sur l'existence et la nature des moyens mis en œuvre tant à son égard qu'à celui de certains de ses interlocuteurs.

Les services de renseignement doivent donc composer, dans certains cas, avec l'impossibilité juridique de renouveler au-delà de six mois des mesures de contrôle administratif et de surveillance. Ainsi, parmi les mesures devant être renouvelées au-delà de six mois, 65 ont effectivement conduit à la signature et à la notification d'un arrêté de renouvellement au cours des trois dernières années et 19 au-delà de neuf mois : ainsi bien que certaines personnes voient leur MICAS abrogée à la suite d'un placement en détention provisoire ou en hospitalisation, les renouvellements subordonnées à la démonstration d'éléments nouveaux ou complémentaires sont particulièrement faibles, faute de pouvoir caractériser ces éléments ou de pouvoir les verser au débat contradictoire.

Enfin et en tout état de cause, quelles que soient la nature des obligations prononcées, la durée cumulée de ces mesures ne peut, en principe, légalement et constitutionnellement excéder douze mois, sauf à ce que l'allongement de cette durée soit justifiée par des circonstances particulières

permettant de traiter différemment une catégorie spécifique de personnes, comme c'est le cas de la mesure figurant au 3° de l'article 3 du présent projet. Ce qui conduit les services, le cas échéant et dans le respect du cadre légal applicable au renseignement, à envisager la mise en œuvre d'autres formes de surveillance à l'une ou l'autre de ces échéances.

1.3.7. Un dialogue approfondi avec l'autorité judiciaire

La mise en œuvre de ces mesures a été l'occasion d'un dialogue approfondi entre les autorités publiques et l'autorité judiciaire, d'une part, pour que cette dernière puisse évoquer les situations qu'elle souhaite judiciariser, d'autre part, pour adapter les obligations prononcées au titre des mesures de surveillance à celles pouvant avoir déjà été prononcées par l'autorité judiciaire.

Ainsi, préalablement au prononcé d'une obligation sur le fondement des articles L. 228-2, L. 228-4 et L. 228-5 du CSI, le ministre de l'intérieur informe le procureur de la République territorialement compétent et le parquet national antiterroriste (PNAT), compétent en matière de terrorisme, lesquels disposent ainsi de la possibilité de faire valoir des observations. Cette information permet notamment à l'autorité judiciaire de s'assurer que cette mesure ne risque pas de compromettre une enquête en cours, que les obligations qui en découlent n'entrent pas en contradiction avec des mesures de suivi judiciaire ou, lorsque tel risque d'être le cas, de convenir de leur aménagement avec l'autorité administrative. Le PNAT est enfin systématiquement destinataire de toutes les mesures de surveillance : nouvelles mesures, renouvellements, modifications ou abrogations.

Il n'existe en effet, aucun obstacle de principe à ce qu'une personne placée sous contrôle judiciaire ou faisant l'objet d'un suivi post-peine fasse également l'objet d'une mesure de contrôle administratif et de surveillance, dès lors que chacune des deux mesures répond à un objectif propre. Ainsi, le contrôle judiciaire vise à s'assurer de la présence de la personne qui en fait l'objet lors de son procès pénal tout en protégeant les victimes et en préservant le bon déroulement de l'enquête, tandis que le suivi post-peine vise à favoriser la réinsertion de l'individu sortant de prison et que la mesure individuelle de contrôle administratif et de surveillance vise à prévenir la commission d'acte en lien avec le terrorisme.

Aussi n'est-il pas rare que ces mesures se conjuguent et que la mesure individuelle de contrôle administratif et de surveillance soit, au regard de ses finalités, plus restrictive que celle du contrôle judiciaire :

- par exemple, le contrôle judiciaire interdira la sortie du territoire national, alors que la mesure individuelle de contrôle administratif et de surveillance interdira la sortie d'un périmètre plus restreint, avec obligation de présentation régulière ;
- de même, l'autorité administrative peut juger utile, compte tenu des éléments d'information dont elle dispose, d'interdire à une personne sous contrôle judiciaire et déjà débitrice à ce titre d'obligations de présentation identiques à celles qui auraient pu être mise en œuvre au titre de la mesure de surveillance administrative, de se trouver en relation directe ou

indirecte avec certaines personnes, nommément désignées, dont il existe des raisons sérieuses de penser que leur comportement constitue une menace pour la sécurité publique.

Au final, s'est instaurée, dans la plupart des cas, une véritable complémentarité entre les mesures prises au titre du contrôle judiciaire et celles prises au titre de la surveillance administrative, les obligations étant contractées lorsqu'elles sont identiques. Plusieurs interventions de l'autorité judiciaire ont permis de signaler des difficultés résultant d'incompatibilités entre ces deux régimes (suivi socio-judiciaire dans un lieu distinct du périmètre d'assignation ou horaires incompatibles, impossibilité d'occuper un emploi pourtant imposé dans ce cadre). A chaque fois, les modalités de la surveillance administrative ont été aménagées. Il est néanmoins nécessaire que les diverses obligations qui découlent de ces deux régimes soient à la fois conciliables et, lorsqu'elles sont identiques, contractées, de sorte que la contrainte qui en découle ne présente pas un caractère disproportionné au regard de l'obligation de tenir compte de la vie privée, familiale et professionnelle (cf. TA Toulouse, 7 novembre 2017, n° 1705075 : *« Considérant qu'il résulte de l'instruction que les obligations de son contrôle judiciaire se confondent avec l'obligation de présentation quotidienne prévue par la mesure individuelle de contrôle administratif et de surveillance ; dès lors que, par une ordonnance de modification du contrôle judiciaire en date du 18 janvier 2016, le magistrat instructeur du tribunal de grande instance de Paris s'est borné à imposer à l'intéressé de se présenter au commissariat de police de Toulouse deux fois par semaine, le mardi et le vendredi, sans précision d'horaire ; que ladite obligation de présentation quotidienne, une fois par jour, ne présente pas un caractère excessif, compte tenu de la menace pour la sécurité et l'ordre publics constituée par le comportement de M. X ; qu'eu égard à l'ensemble de ces éléments, il n'apparaît pas, en l'état de l'instruction, que les modalités de contrôle administratif et de surveillance de l'intéressé revêtiraient un caractère disproportionné. »*).

L'exigence de proportionnalité, figurant déjà à l'article L. 228-6 du code de la sécurité intérieure s'agissant des MICAS, sera renforcée dans le projet de loi, cet article précisant en outre que les obligations prononcées au titre de cette mesure tiennent compte de celles déjà prononcées par l'autorité judiciaire (voir *infra*, 5° de l'article 3).

1.3.8. Au final, l'usage de cette mesure a été proportionné, compte tenu de son encadrement strict, et son utilité opérationnelle est confirmée, notamment à l'encontre des sortants de prison.

Cette mesure constitue en effet un outil d'entrave supplémentaire mis à la disposition des services en charge de la prévention du terrorisme. De plus, l'absence de procédure préalable à l'édiction de ces mesures permet leur mise en œuvre rapide, en urgence, dès qu'un comportement apparaît préoccupant au regard des conditions fixées par la loi.

Ainsi, 143 mesures ont été prises au titre de la troisième année de mise en œuvre de la loi du 30 octobre 2017, 66 mesures étant toujours en vigueur au 31 octobre 2020. Ces chiffres, en légère augmentation de 7 % par rapport à l'année précédente, s'expliquent par un nombre

important d'individus condamnés pour terrorisme et radicalisés qui sont sortis de prison en 2020.

Lors de la présentation du plan d'action contre le terrorisme (PACT), le 13 juin 2018, le Gouvernement a rappelé que près de 10 % des détenus terroristes islamistes et plus d'un tiers des détenus de droit commun susceptibles de radicalisation, qu'ils soient prévenus ou condamnés, étaient libérables d'ici fin 2019, et plus de 80 % des 143 détenus terroristes islamistes déjà condamnés l'étaient d'ici 2022.

L'augmentation importante de ce nombre sur les deux dernières années d'application de la loi s'explique par le fait que de nombreux individus condamnés pour association de malfaiteurs en lien avec le terrorisme, ou participation à des actes terroristes, dans les années 2014-2015 ont désormais purgé leur peine et sortent de détention. Cette augmentation s'est traduite par une coopération croissante avec le service national du renseignement pénitentiaire du ministère de la Justice, par la mise à disposition de renseignements permettant de qualifier les faits pouvant justifier une mesure de police administrative.

Plusieurs détenus terroristes islamistes sunnites (TIS) incarcérés dans les prisons françaises ont ainsi été ou seront prochainement : 45 en 2020 ; 64 en 2021 ; 47 en 2022 ; 38 en 2023. Ces individus présentent des profils divers pour lesquels les enjeux sécuritaires posés sont multiples : prosélytisme, menace à court terme représentée par des profils impulsifs, menace à moyen et long terme relative à des projets d'attentats ou encore tentative de redéploiement vers des zones de jihad à l'étranger.

Afin de favoriser leur suivi a donc été instauré, un dispositif d'anticipation et de prise en compte, par les services, des sorties de ces individus a été mis en place dès juillet 2018. Une unité permanente a été créée au sein de l'unité de coordination de la lutte antiterroriste (UCLAT) et un comité de suivi rassemblant des représentants des services des ministères de l'intérieur et de la justice se réunit tous les mois pour envisager, au regard des mesures judiciaires mises en place, les modalités de suivi sur le plan administratif des personnes dont la libération est proche. Il s'agit ainsi d'éviter tout conflit négatif de compétence et de s'assurer d'un suivi effectif par un service à l'issue de l'incarcération.

Ce dispositif a conduit le ministre de l'intérieur à prononcer, entre le 1er novembre 2019 et le 31 octobre 2020, 202 mesures individuelles de contrôle administratif et de surveillance à l'encontre de personnes sortant de prison et ayant fait l'objet d'une condamnation pour des faits en lien avec le terrorisme ou ayant été signalées comme radicalisées au cours de leur incarcération (contre 77 mesures seulement l'année précédente). Parmi les 66 mesures en vigueur au 31 octobre 2020, 51 concernent des individus sortant de prison (soit 77 %).

La mesure individuelle de contrôle administratif et de surveillance permet donc de surveiller l'individu sortant de prison, lorsqu'en détention, il a manifesté la pérennité de son engagement radical, par le biais de ses fréquentations, des visites qu'il a reçues, de ses activités licites ou non. Ces mesures s'articulent le plus souvent avec celles résultant du contrôle post-peine, dont le service pénitentiaire d'insertion et de probation est en charge.

Y compris lorsqu'elles interviennent en complément d'une mesure de surveillance judiciaire, les mesures individuelles de contrôle administratif et de surveillance prises à l'égard des individus sortant de détention présentent un grand intérêt, dans la mesure où il est difficile d'anticiper leur comportement, au regard de celui qu'ils ont adopté en prison. Cette surveillance permet alors d'observer leurs relations habituelles (volontaires et non pas imposées comme en détention), leur pratique religieuse (fréquentation de telle ou telle mosquée), leur activité sur les réseaux sociaux, leurs efforts de réinsertion, etc…

Dans ce cadre, outre la pérennisation du dispositif des MICAS, le 3° de l'article 3 du présent projet vise à permettre de prononcer une telle mesure pour une durée totale cumulée de 24 mois, lorsque les personnes concernées ont déjà été condamnées à une peine de prison de plus de cinq ans ou trois ans en cas de récidive, pour des infractions en lien avec le terrorisme *(voir infra).*

1.3.9. L'utilité de ce dispositif de surveillance est majorée par la sévérité de la répression de la violation des obligations

L'article L. 228-7 du CSI punit de trois ans d'emprisonnement et de 45 000 euros d'amende le fait pour une personne de se soustraire à une ou plusieurs des obligations qui lui sont imposées par le ministre de l'intérieur sur le fondement des articles L. 228-2 à L. 228-5 du même code.

En l'espèce, les sanctions ainsi encourues présentent un caractère dissuasif et visent à garantir l'effectivité de la mesure. Elles sont régulièrement rappelées aux personnes qui en font l'objet : dans l'arrêté initial et, le cas échéant, dans les arrêtés renouvelant la mesure, dans la notice d'information qui accompagne chaque arrêté et dans tout sauf-conduit et arrêtés modificatifs dérogeant ponctuellement aux obligations.

Au cours des trois premières années d'application de la loi SILT[8], 127 cas de non-respect des obligations imposées en vertu de la mesure individuelle de contrôle administratif et de surveillance concernent ont été signalés concernant 88 personnes. 96 de ces violations ont donné lieu à poursuite pénale.

Les sanctions prononcées en cas de non-respect des obligations définies par la mesure individuelle de contrôle administratif et de surveillance sont dans 37 cas des peines d'emprisonnement, dans 2 cas une peine d'amende et dans 15 cas, des rappels à la loi. Par ailleurs, 26 procédures judiciaires sont en cours.

Dans deux cas, les individus ont été relaxés dans la mesure où le juge pénal a considéré que la mesure de MICAS fondant les poursuites était illégale, les conditions exigées par la loi n'étant, selon lui, par remplies.

[8] Sous réserve de l'exhaustivité des remontées des préfectures et des services judiciaires

1.4. LES VISITES DOMICILIAIRES ET LES SAISIES

Si les quelques 4 500 perquisitions administratives conduites sous l'état d'urgence[9] entre le 14 novembre 2015 et le 1er novembre 2017 ont été décidées unilatéralement par l'autorité préfectorale au regard de la seule menace que pouvaient constituer certains individus pour l'ordre et la sécurité publics, les visites domiciliaires (et le cas échéant les saisies et l'exploitation des données saisies) créées par l'article 4 de la loi « SILT » du 30 octobre 2017 doivent au contraire répondre à des critères définis de façon plus restrictive et sont soumis à une autorisation préalable de l'autorité judiciaire.

Ces visites, et le cas échéant les saisies et l'exploitation des données saisies au cours des opérations, sont soumises à une autorisation préalable du juge des libertés et de la détention (JLD) près le tribunal judiciaire de Paris, sauf avis contraire du procureur de la République antiterroriste et du procureur territorialement compétent, afin d'éviter toute interférence avec une éventuelle procédure judiciaire en cours ou à venir.

Ce double verrou, visant à garantir la subsidiarité des perquisitions judiciaires, n'a pas réduit le caractère complémentaire du dispositif, puisque sur les 424 projets de visites transmises au procureur de la République antiterroriste (PNAT) entre le 1er novembre 2017 et le 31 octobre 2020, 406 ont reçu son accord, huit ont été retenues par ce dernier pour déclencher une procédure judiciaire et dix ont fait l'objet d'un avis défavorable.

	Projets de visite domiciliaire	**Avis du procureur de la République**	
		Accord	*Prise en compte judiciaire*
1ère année d'application	**89**	86	3
2e année d'application	**111**	107	4
3e année d'application	**224**	213	1
Cumul depuis le 01/11/2017	**424**	406	8

En outre, la requête à des fins de visite domiciliaire doit établir que sont réunis les mêmes critères cumulatifs que ceux exigés pour fonder les mesures individuelles de contrôle administratif et de surveillance (art. L. 228-1 du CSI) :

- le comportement de la personne visée doit constituer une menace d'une particulière gravité pour la sécurité et l'ordre publics ;
- elle doit par ailleurs entrer en relation de manière habituelle avec des personnes incitant, facilitant ou participant à des actes de terrorisme et/ou soutenir, diffuser ou adhérer à des thèses incitant à la commission d'actes de terrorisme en France ou à l'étranger ou faisant l'apologie de tels actes.

Les dossiers présentés par les préfets ont dans leur grande majorité été considérés comme suffisamment solides pour donner lieu à une autorisation du juge des libertés et de la détention

[9] Article 11 de la loi du 3 avril 1955 relative à l'état d'urgence.

de Paris (depuis le 1er novembre 2017 et jusqu'au 30 octobre 2020, sur 406 requêtes, seules 49 ont fait l'objet d'une ordonnance de rejet, essentiellement pour absence de caractérisation de la menace d'une **particulière** gravité pour la sécurité et l'ordre publics, indépendamment des deux autres critères alternatifs (36 rejets sur 49) dont 12 ne remplissait également pas l'autre des critères.

	Requêtes préfectorales à des fins de visite domiciliaire	**Ordonnances du JLD**		**Visites effectuées**	**Saisies réalisées**
		Accord	*Refus*		
1ère année d'application	**86**	73	13	70	40
2e année d'application	**107**	83	23	74	40
3e année d'application	**213**	190	13	151	81
Cumul depuis le 01/11/2017	**406**	346	49	295	161

De même, rares sont les cas où l'exploitation des données saisies durant la visite a été refusée par le juge des libertés et de la détention.

	Demandes d'autorisation d'exploitation des données	Ordonnances du JLD		Contentieux
		Accord	*Refus*	
1ère année d'application	**41**	41	0	0
2e année d'application	**39**	36	3	1
3e année d'application	**66**	55	5	2
Cumul depuis le 1/11/2017	**146**	132	8	3

Dans la grande majorité des cas, le juge des libertés et de la détention a répondu aux requêtes préfectorales le jour de sa saisine (42 %) ou le lendemain de sa saisine (39 % des cas). Le délai de réponse le plus long observé au cours de cette troisième année d'application de la loi SILT est de 21 jours (cas exceptionnel).

1.4.1. Un régime validé dans son ensemble par le Conseil constitutionnel, à l'exception des modalités de saisie des documents et objets

Dans sa décision n° 2017-695 du 29 mars 2018, le Conseil constitutionnel a jugé que le législateur, qui a à la fois strictement borné le champ d'application de la mesure qu'il a instaurée et apporté les garanties nécessaires, a assuré une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et, d'autre part, le droit au respect de la vie privée, l'inviolabilité du domicile et la liberté d'aller et de venir.

Il a relevé notamment à cet égard que, en adoptant les dispositions contestées, le législateur a poursuivi l'objectif de lutte contre le terrorisme, qui participe de l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public.

Par ailleurs, le législateur a énoncé un ensemble de garanties propres à limiter l'atteinte, notamment :

- en définissant avec précision les conditions de recours aux visites et saisies et limité leur champ d'application à des personnes soupçonnées de présenter une menace d'une particulière gravité pour l'ordre public.

- en soumettant toute visite et saisie à l'autorisation préalable du juge des libertés et de la détention, qui doit être saisi par une requête motivée du préfet et statuer par une ordonnance écrite et motivée, après avis du procureur de la République.

- en introduisant une exemption de visites et de saisie dans les lieux affectés à l'exercice d'un mandat parlementaire ou à l'activité professionnelle des avocats, des magistrats ou des journalistes et les domiciles de ces personnes.

- en précisant que la visite doit être effectuée en présence de l'occupant des lieux ou de son représentant et lui permet de se faire assister d'un conseil de son choix. En l'absence de l'occupant, les agents ne peuvent procéder à la visite qu'en présence de deux témoins qui ne sont pas placés sous leur autorité.

Dans ces conditions, le Conseil constitutionnel a conclu que le législateur avait *« strictement borné le champ d'application de la mesure qu'il a instaurée »*, *« apporté les garanties nécessaires »* et *« assuré une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et, d'autre part, le droit au respect de la vie privée, l'inviolabilité du domicile, la liberté d'aller et venir » et « le droit à un recours juridictionnel effectif ».*

En revanche, examinant le régime de saisie des documents et objets au regard de l'article 17 de la Déclaration des droits de l'Homme et du citoyen de 1789, qui garantit le caractère inviolable et sacré du droit de propriété, le Conseil constitutionnel a rappelé que les atteintes portées à ce droit devaient être *« justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi »*. Il en a dès lors conclu que, *« le législateur [n'ayant] fixé aucune règle permettant d'encadrer l'exploitation, la conservation et la restitution des documents et objets saisis au cours de la visite »*, ce régime méconnaissait le droit de propriété et devait être déclaré contraire à la Constitution, avec effet immédiat. Les garanties ont en revanche été jugées suffisantes s'agissant des hypothèses de saisies de données contenues dans les supports de données informatiques (CC, 29 mars 2018, n° 2017-695, pts 58-70).

La disposition a donc été modifiée dans le cadre de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice pour étendre le régime de saisie des

données à celui des documents. En revanche, le Gouvernement n'a pas souhaité réintroduire la possibilité de saisir des objets, cette possibilité ayant été estimée peu pertinente :

- en effet, la présence d'objets en lien avec la menace et découverts lors de la visite peut être consignée dans le procès-verbal rédigé lors de la visite, lequel, signé par la personne concernée, son représentant ou deux témoins, fait foi ; de même, les objets peuvent être photographiés. En effet, contrairement aux exigences procédurales devant le juge pénal, ces modes de preuves sont suffisants devant le juge administratif pour caractériser les raisons sérieuses exigées par la loi et justifier ainsi les mesures de police administrative qui peuvent découler de la visite domiciliaire ;
- en revanche, dans l'hypothèse où la visite donnerait lieu à la découverte de documents ou d'objets illicites (en particulier armes, stupéfiants et écrits faisant l'apologie du terrorisme), ces derniers peuvent être saisis selon les règles de la procédure pénale, qui trouvent alors à s'appliquer.

1.4.2. Un recours très important à cet instrument lié au contexte sécuritaire

Entre le 1er novembre 2017 et le 31 octobre 2020, 406 requêtes préfectorales à des fins de visite domiciliaire ont été adressées au juge des libertés et de la détention près le tribunal judiciaire de Paris, avec un doublement la dernière année (203 contre 107 l'année précédente)

En revanche, l'attentat perpétré à Conflans-Sainte-Honorine (78) le 16 octobre 2020 a eu un impact très important sur le nombre de visites domiciliaires : le ministre de l'intérieur a en effet fait le choix d'une stratégie de multiplication des visites domiciliaires sur l'ensemble du territoire. Ainsi, au cours du mois d'octobre 2020, 176 requêtes préfectorales (contre 4 l'année précédente) ont été soumises au juge des libertés et de la détention et 119 visites ont été réalisées (contre 4 l'année précédente également). Ces visites domiciliaires se sont poursuivies au-delà du 31 octobre 2020, avec 94 requêtes préfectorales et 88 visites effectuées au cours du mois de novembre 2020.

Au total, cette opération massive et inédite de police administrative a permis d'effectuer à ce jour plus de 200 visites domiciliaires en quelques semaines seulement, confirmant, d'une part, l'appropriation de cet outil par les préfectures et, d'autre part, l'utilité de cette mesure, qui aurait permis la saisie de plus d'une centaine de supports de données et la judiciarisation de cinq personnes, dont une pour des faits en lien avec le terrorisme.

De manière générale, les préfectures et les services de renseignement reconnaissent l'utilité de cet outil en ce qu'il permet de comprendre l'environnement des individus suivis, d'affiner l'analyse sur leur degré de radicalisation, de lever un doute, voire de clôturer un suivi

Dans certains cas, la visite domiciliaire, dont la finalité est préventive, est le seul moyen de lever ce doute, avant même qu'un comportement puisse être judiciarisé.

. Ainsi, à titre d'exemple, on remarquera que le critère de *« soutien à des thèses incitant à la commission d'actes de terrorisme en France ou à l'étranger ou faisant l'apologie de tels actes* »

ne suppose pas de communication publique et n'entre pas nécessairement dans le champ du délit d'apologie du terrorisme, qui a trait à toute action de communication publique présentant sous un jour favorable des actes terroristes ou ceux qui les ont commis. C'est donc précisément lorsque le soutien ou l'adhésion ne revêtent pas un caractère public mais se manifestent lors de conversations privées, interceptées par la mise en œuvre de techniques de renseignement ou connues par des sources humaines, que la visite ou la saisie prendra tout son sens, là où l'autorité judiciaire n'aurait encore pas pu intervenir.

Afin de garantir cette subsidiarité, le procureur de la République antiterroriste (PNAT) est systématiquement informé de l'éventualité d'une visite et ce, avant même d'en demander l'autorisation au juge des libertés et de la détention. Cette information vise à ne pas interférer avec d'éventuelles procédures judiciaires en cours ou à permettre à l'autorité judiciaire d'ordonner elle-même une perquisition judiciaire au vu des éléments qui lui ont été transmis. De même, le procureur de la République territorialement compétent reçoit tous les éléments relatifs à ces opérations, lui permettant ainsi une appréciation fine du projet de l'autorité administrative.

Ces procédures se sont révélées globalement fructueuses : huit projets de visite ont ainsi été retenus par l'autorité judiciaire pour donner lieu à des procédures judiciaires, tandis que 10 ont reçu un avis défavorable, pour permettre à l'autorité judiciaire de continuer à instruire les dossiers.

En effet, lorsque la personne concernée par un projet de visite domiciliaire fait également l'objet d'une instruction ou d'une enquête, il est parfois contre-productif de lui signaler, par le biais d'une visite domiciliaire, qu'elle fait l'objet d'une surveillance, ce qui pourrait l'amener à modifier son comportement ou à dissimuler des preuves. Or, l'autorité judiciaire peut avoir intérêt à continuer son instruction ou son enquête sans dévoiler le fait que cette personne est mise en attention, des services de renseignements ou des services judiciaires.

C'est tout l'objet de la saisine des procureurs de la république, anti terroriste d'une part et territorialement compétent d'autre part, qui peuvent différer cette visite domiciliaire, pour ne pas contrecarrer les mesures d'instruction en cours, voire, exercer des poursuites contre la personne concernée lorsque les éléments dont ils disposent sont suffisants.

De même, l'information par l'officier de police judiciaire du procureur territorialement compétent, lors de la découverte d'une infraction à l'occasion d'une visite administrative, le met également en capacité de traiter des éventuelles suites pénales de cette mesure administrative.

1.4.3. Une saisie des données et des supports dans plus de la moitié des cas

Le I de l'article L. 229-5 du CSI prévoit que : « *Aux seules fins de prévenir la commission d'actes de terrorisme, si la visite révèle l'existence de données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée, il peut être procédé à leur saisie ainsi qu'à celle des données contenues*

dans tout système informatique ou équipement terminal présent sur les lieux de la visite soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la visite ».

Sur les 322 visites domiciliaires réalisées au cours des trois premières années, 172 ont donné lieu à la saisie de données ou de documents.

Le II de l'article L. 229-5 prévoit également que « *dès la fin de la visite, l'autorité administrative peut demander au juge des libertés et de la détention du tribunal judiciaire de Paris d'autoriser l'exploitation des données saisies. Au vu des éléments révélés par la visite, le juge statue dans un délai de quarante-huit heures à compter de sa saisine sur la régularité de la saisie et sur la demande de l'autorité administrative. Sont exclus de l'autorisation les éléments dépourvus de tout lien avec la finalité de prévention de la commission d'actes de terrorisme ayant justifié la visite. ».*

Lorsque les saisies ont été opérées au regard des éléments découverts lors des visites autorisées, de nature à confirmer l'existence d'une menace, le juge des libertés et de la détention a, dans chaque cas, autorisé leur exploitation.

Au 31 octobre 2020, 157 requêtes aux fins d'exploitation des supports de données saisis (contre 172 saisies) ont été introduites et huit ont été rejetées, essentiellement pour l'absence de découverte d'éléments en lien avec la menace, seuls de nature à permettre la saisie des documents ou données, les autres requêtes ayant donné lieu à un accord du JLD postérieurement à cette date.

- l'un des refus du JLD a été motivé par le fait que la visite n'avait donné lieu à aucun début d'exploitation sur place des outils saisis, et ce malgré le fait que l'intéressé avait communiqué le code de déverrouillage de l'un des téléphones portables. Le juge a donc conclu qu'il n'était pas justifié que la visite ait révélé l'existence de documents ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée (ordonnance du 27 mai 2020).

- par ailleurs, le JLD a refusé à quatre reprises l'exploitation des supports de données saisis au motif que les saisies avaient été opérées sans que les visites n'aient révélé l'existence de documents ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée (ordonnances du 20 octobre 2020, du 24 octobre 2020, du 26 octobre 2020, du 28 octobre 2020).

Enfin, dans le cadre des 172 saisies effectuées et des 149 autorisations d'exploitation, 32 demandes de prorogation du délai d'exploitation ont été formulées par les préfectures au 31 octobre 2020, afin de tenir compte à la fois de difficultés techniques et du volume des données saisies, qui ont toutes été accordées par le JLD. Toutes ont été autorisées par le JLD.

1.4.4. Des poursuites judiciaires pour des faits de terrorisme à la suite de visites domiciliaires

57 visites domiciliaires ont donné lieu à des poursuites pénales dont 30 pour des faits de terrorisme.

En 2018, la visite d'un domicile a donné lieu à la saisie puis à l'exploitation de 40 Go de données, lesquelles ont permis de mettre en évidence un projet visant à créer une filière de recrutement et d'acheminement de jeunes filles vers la zone irako-syrienne, des poursuites pénales ayant été engagées.

De même, l'exploitation de données saisies dans un téléphone portable et un ordinateur portable à l'occasion d'une visite domiciliaire effectuée le 14 septembre 2018 a permis de constater que l'intéressé relayait notamment des tweets pro-*djihadiste*s incitant à la commission d'actions violentes sur le territoire. Les faits ont été signalés au parquet, qui a dès lors ouvert une procédure pour apologie du terrorisme, toujours en cours d'instruction.

De même, la réalisation d'une visite domiciliaire a permis de mettre en exergue les velléités de départ sur zone de *djihad* d'un individu présent sur le territoire national, lequel entretenait par ailleurs des contacts avec un combattant sur zone, ayant pu être identifié. Ces éléments ont donné lieu à l'ouverture d'une enquête préliminaire du parquet antiterroriste, débouchant sur l'interpellation, le placement en garde à vue, la mise en examen pour association de malfaiteurs en relation avec une infraction à caractère terroriste et le placement en détention provisoire de l'individu.

D'autres transmissions à l'autorité judiciaire ont donné lieu à l'ouverture d'une enquête pénale pour recel d'apologie, certains dossiers ayant déjà abouti à la condamnation des individus concernés. En revanche, un signalement effectué suite à l'exploitation de supports informatiques saisis au cours d'une visite domiciliaire a débouché sur un classement sans suite, les faits d'apologie du terrorisme n'ayant pas été retenus.

En 2019, une visite domiciliaire a donnée lieu au placement en garde à vue de l'intéressé après la découverte d'une correspondance et de transferts d'argent en lien avec le terrorisme.

Six individus ont fait l'objet de poursuites judiciaires pour des faits de délit de recel d'apologie du terrorisme et apologie du terrorisme. Ont notamment été découvertes lors des visites, des vidéos de propagande ou de soutien à Daech, des images et vidéos de combattants et des vidéos sur le jihad.

En 2020, une visite domiciliaire a donné lieu à l'ouverture d'une procédure en flagrance pour détention et fabrication d'engins explosifs, à la suite de la découverte dans une cave de matériel pouvant servir à la fabrication de ces engins.

Quatre individus ont par ailleurs fait l'objet de poursuites judiciaires pour des faits de délit de recel d'apologie du terrorisme et apologie du terrorisme. Ont notamment été découvertes lors des visites, des vidéos de propagande ou de soutien à *Daech*, des images et vidéos de combattants et des vidéos sur le jihad.

1.4.5. Des infractions constatées dans le cadre d'une procédure incidente[10]

Parmi ces infractions ayant donné lieu à procédure judiciaire incidente, on peut citer les éléments suivants, à titre d'exemple :

- découverte d'armes détenues illégalement : 28 visites ont permis la découverte de plusieurs armes, engins explosifs, armes blanches et munitions ;
- découverte de produits stupéfiants ;
- découverte de faux documents d'identité et d'objets volés.

Ces chiffres démontrent qu'en facilitant la transmission d'informations entre les autorités administrative et judiciaire, cette procédure permet de porter à la connaissance de la justice des infractions qui ne l'auraient pas été en-dehors de la mise en œuvre de mesures de police administrative.

1.4.6. La mise en œuvre d'autres mesures de police administrative à la suite d'une visite domiciliaire

L'objet des visites domiciliaires est avant tout de lever le doute sur la dangerosité de certaines personnes et leur implication dans la préparation d'actions terroristes ou leur incitation.

Tirant les conséquences des découvertes réalisées lors des visites domiciliaires, et alors même que les personnes n'ont pu faire l'objet de poursuites pénales, l'autorité administrative a pu les prendre en compte pour exercer une surveillance.

– **MICAS :** durant les trois premières années d'application, 14 mesures individuelles de contrôle administratif et de surveillance ont été prises à l'issue d'une visite domiciliaire. Ces visites et l'exploitation des données saisies ont permis de confirmer l'adhésion des intéressés à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes et, le cas échéant, que leur comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics. A l'inverse, 39 visites domiciliaires ont été réalisées à l'égard de personnes déjà placées sous mesure individuelle de contrôle administratif et de surveillance.

  Ce faible nombre s'explique par la nécessité de démontrer, pour obtenir l'autorisation de mener une visite domiciliaire, que sont remplis les mêmes critères que ceux permettant de placer un individu sous mesure de surveillance. Contrairement à la situation qui prévalait durant l'état d'urgence, où la perquisition administrative était utilisée comme préalable à une assignation à résidence, pour caractériser la radicalisation d'une personne ou au contraire l'écarter, la mesure de visite domiciliaire ne peut être utilisée à cette fin, compte tenu de la rédaction de la loi.

  Dans certains cas néanmoins, les découvertes incidentes ont permis de démontrer que le comportement de personnes constituait une menace d'une particulière gravité pour la

[10] Procédure pénale sans lien avec un motif terroriste

sécurité et l'ordre publics et ont permis au ministre de l'intérieur de prononcer une mesure individuelle de contrôle administratif et de surveillance ou de la renouveler en caractérisant les éléments nouveaux ou complémentaires exigés après une durée cumulée de six mois d'application.

A contrario, celles qui n'ont débouché sur la découverte d'aucun élément en lien avec la menace terroriste ont permis de confirmer que ces personnes ne constituaient plus une menace d'une particulière gravité pour la sécurité et l'ordre publics. En conséquence, la mesure dont ils faisaient l'objet a été abandonnée.

- **Gel des avoirs :** il est courant que des personnes ayant fait l'objet d'une mesure individuelle de contrôle administratif et de surveillance (MICAS) ou d'une visite domiciliaire fasse également l'objet d'une mesure de gels des avoirs sur le fondement des articles L. 562-2 et suivants du code monétaire et financier.

- **Interdiction de sortie du territoire (IST) :** aucun arrêté portant interdiction de sortie du territoire pris sur le fondement de l'article L. 224-1 du CSI n'a été pris à l'issue d'une visite domiciliaire à l'encontre d'individus qui ont manifesté des velléités de départ contre 4 l'année précédente, cette diminution s'expliquant par le tarissement des intentions de départs sur un théâtre d'opérations de groupements terroristes.

1.5. DES OUTILS DE PREVENTION DU TERRORISME COMPLEMENTAIRES DE CEUX DEJA PRESENTS DANS L'ORDONNANCEMENT JURIDIQUE

Ces outils de police administrative s'ajoutent et s'articulent avec d'autres instruments de police administrative destinés à prévenir des actes de terrorisme, également mis en œuvre au niveau ministériel, afin d'apporter la réponse la plus pertinente et la plus complète à la menace présentée par un individu ou une personne morale. Il est précisé que ces mesures ne sont pas visées par la disposition du II de l'article 5 de la loi n° 2017-1510 du 30 octobre 2017 prévoyant que les dispositifs précités sont applicables jusqu'au 31 juillet 2021.

Ces mesures prises au niveau ministériel sont les suivantes.

1.5.1. L'interdiction de sortie du territoire (art. L. 224-1 du CSI)

Cette mesure, complémentaire de la mesure individuelle de contrôle administratif et de surveillance, vise à s'assurer qu'un individu de nationalité française ne quitte pas le territoire national pour rejoindre un théâtre d'opérations de groupements terroristes, « dans des conditions susceptibles de le conduire à porter atteinte à la sécurité publique lors de son retour sur le territoire français ».

L'interdiction de sortie du territoire est prononcée par le ministre de l'intérieur pour une durée de six mois et peut être renouvelée pour une durée identique par décision expresse et motivée.

Elle prend effet dès sa signature, et non dès sa notification comme c'est le cas de manière habituelle pour une mesure administrative individuelle, et entraîne immédiatement l'invalidation des titres de voyage de la personne (passeport et carte nationale d'identité) et son inscription au fichier des personnes recherchées, afin de bloquer sa sortie du territoire, notamment lors d'un contrôle à l'embarquement dans un aéroport.

Toutes les personnes placées sous contrôle administratif et surveillance ne sont pas pour autant susceptibles de faire l'objet d'une interdiction de sortie du territoire, l'autorité administrative devant démontrer spécifiquement les raisons sérieuses qu'elle a de penser que la personne projette un tel déplacement, ce qui suppose de caractériser une intention de départ (propos tenus, achat de billets, organisation d'un trajet, recherche d'itinéraires, liquidation des biens et fermeture des comptes, etc.).

Près de 40 % des mesures individuelles de contrôle administratif et de surveillance prononcées depuis le 1er novembre 2017 l'ont été à l'encontre de personnes faisant ou ayant déjà fait l'objet d'une interdiction de sortie du territoire. La coïncidence de ces deux mesures, comme ce fut le cas sous l'état d'urgence pour les assignations à résidence, s'explique par un engagement fréquent des intéressés dans la mouvance radicale et un lien avec des filières de recrutement, pouvant alors susciter des projets de départ à l'étranger.

Le nombre d'interdictions de sortie du territoire est aujourd'hui en net retrait (49 mesures, dont 21 initiales, ont ainsi été prononcées entre le 1er novembre 2017 et le 31 octobre 2018, contre 181 entre le 1er novembre 2016 et le 31 octobre 2017, 22 mesures ont été prononcées (dont 18 initiales) entre le 1er novembre 2018 et le 31 octobre 2019 et 14 mesures, dont 6 initiales, entre le 1er novembre 2019 et le 30 octobre 2020), cette diminution étant liée à la forte diminution des velléités de départ vers les théâtres d'opérations de groupements terroristes, elle-même vraisemblablement liée à l'évolution de la situation politique et militaire dans les pays abritant ces théâtres.

Symétriquement, les personnes sont revenues de ces théâtres dans un mouvement de flux qui s'est actuellement quasiment tari. Ces retours n'ont pour autant pas conduit l'autorité administrative à recourir au contrôle administratif des retours sur le territoire national prévu par les articles L. 225-1 à L. 225-8 du code de la sécurité intérieure, dans la mesure où ils ont systématiquement fait l'objet d'une prise en compte judiciaire, et alors que le dispositif de contrôle administratif des retours avait été conçu par le législateur comme subsidiaire par rapport à l'intervention de l'autorité judiciaire.

1.5.2. Le gel des fonds et des ressources économiques (art. L. 221-1 du CSI)[11]

Les personnes physiques ou morales, ou toute autre entité, qui commettent, tentent de commettre, facilitent ou financent des actes de terrorisme, y incitent ou y participent ainsi que les personnes morales ou autres entités détenues ou contrôlées par les premières ou agissant

[11] Article renvoyant aux obligations prévues par les chapitres Ier et II du titre VI du livre V du code monétaire et financier (art. L. 562-1 et suivants).

sciemment pour leur compte ou sur leurs instructions peuvent voir les fonds et ressources économiques qu'elles possèdent, détiennent ou contrôlent, gelés pour une durée de six mois renouvelable, par arrêté conjoint du ministre chargé de l'économie et du ministre de l'intérieur.

Des mesures de gel des fonds et ressources économiques peuvent également être décidées, par arrêté du ministre chargé de l'économie, pour une durée de six mois renouvelable, dans le cadre de régimes de sanctions financières internationales décidées par le Conseil de sécurité des Nations unies ou par l'Union européenne, en réaction à une violation du droit international ou dans le cadre de la lutte contre le terrorisme (article L. 562-3 du code monétaire et financier).

Une telle mesure vise à la fois les personnes détenant des ressources importantes mais également celles dont les ressources sont plus insignifiantes mais dont les comptes peuvent servir de réceptacles à des opérations de flux financiers à destination de groupes terroristes.

C'est ainsi que plus de 600 mesures nationales de gel des avoirs ont été prises depuis le 1er novembre 2017, avec en moyenne environ 200 mesures prises annuellement depuis 2018. 176 mesures de gel des avoirs ont été prises pendant la troisième année d'application de la loi SILT, soit un chiffre proche de celui constaté l'année précédente. 88 mesures étaient encore en vigueur au 31 octobre 2020, dont 95 concernent des personnes physiques et cinq concernent des personnes morales ou tout autre entité. Par ailleurs, entre le 1er novembre 2019 et le 31 octobre 2020, 20 individus ayant fait l'objet d'une MICAS et/ou d'une visite domiciliaire ont également fait l'objet d'une mesure nationale de gel des avoirs.

1.5.3. Les dissolutions d'associations (art. L. 212-1 du CSI)

L'article L. 227-1 du code de la sécurité intérieure prévoit que, aux seules fins de prévenir la commission d'actes de terrorisme, peuvent faire l'objet d'une décision de fermeture les lieux de culte dans lesquels les propos qui sont tenus, les idées ou théories qui sont diffusées ou les activités qui se déroulent provoquent à la violence, à la haine ou à la discrimination, provoquent à la commission d'actes de terrorisme ou font l'apologie de tels actes.

Lorsque ces agissements sont également provoqués, entretenus ou cautionnés par la personne morale gérant le lieu de culte, celle-ci peut, le cas échéant, faire l'objet d'une dissolution administrative sur le fondement des 6° ou 7° de l'article L. 212-1 du code de la sécurité intérieure, selon lequel *« Sont dissous, par décret en conseil des ministres, toutes les associations ou groupements de fait : (...) 6° Ou qui, soit provoquent à la discrimination, à la haine ou à la violence envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, soit propagent des idées ou théories tendant à justifier ou encourager cette discrimination, cette haine ou cette violence ; / 7° Ou qui se livrent, sur le territoire français ou à partir de ce territoire, à des agissements en vue de provoquer des actes de terrorisme en France ou à l'étranger* ».

De telles mesures de dissolution ont été prises à l'encontre d'associations gérant des lieux de culte, tels que la mosquée de Lagny-sur-Marne, la mosquée Rhama de Torcy, la mosquée Calendal d'Aix-en-Provence ou la mosquée Assouna de Marseille.

Par ailleurs, indépendamment des associations gestionnaires de lieux de culte dissoutes sur ce fondement, sept autres associations ou groupements de fait provocant à des actes de terrorisme ont, depuis le 1er novembre 2017, fait l'objet d'une mesure de dissolution sur les fondements des articles 6° et 7° de l'article L. 212-1 du code de la sécurité intérieure.

1.5.4. Les mesures d'éloignement des ressortissants étrangers non-européens (art. L. 521-1, L 521-2 et L. 521-3 du CESEDA)

Ont été également instruites des procédures d'expulsions (ministérielles ou préfectorales) dans les cas où il s'est avéré qu'un individu placé sous contrôle administratif et surveillance pouvait être éloigné, à raison de sa nationalité d'une part, et de son comportement d'autre part.

Cette instruction a été menée de concert avec la direction générale des étrangers en France (DGEF) et l'office français pour la protection des réfugiés et apatrides (OFPRA), lorsque la mesure d'éloignement exigeait, auparavant, un retrait de la protection dont l'individu pouvait éventuellement bénéficier, ce retrait étant possible si la présence de la personne concernée **constitue une menace grave** pour la sûreté de l'État (art. L. 711-6, 1° du code de l'entrée et du séjour des étrangers et du droit d'asile – CESEDA, pour la qualité de réfugié, et art. L. 712-2 et L. 712-3 du même code pour la protection subsidiaire).

Depuis l'entrée en vigueur, le 31 octobre 2017, de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, 118 arrêtés d'expulsion ont été prononcés à l'encontre d'individus liés à la mouvance terroriste et islamiste radicale.

Sur ces 118 arrêtés d'expulsion :

- 23 ont été pris à l'encontre d'individus se trouvant à l'étranger (pour l'essentiel, partis combattre en zone syro-irakienne) et ne nécessitent donc pas d'être mis à exécution par le renvoi forcé des intéressés dans leur pays d'origine (mais ces arrêtés font obstacle à leur retour en France) ;
- 59 ont été exécutés par renvoi forcé des intéressés dans leur pays d'origine ;
- 33 n'ont pas encore été exécutés : douze en raison de l'incarcération des individus concernés ou de leur placement en hospitalisation sans consentement, six parce que les intéressés sont actuellement bénéficiaires d'une protection internationale (statut de réfugié ou protection subsidiaire), le cas échéant en cours de réexamen par l'OFPRA ou la CNDA, deux en raison d'un recours avec effet suspensif, exercé auprès de la Cour européenne des droits de l'homme, deux en raison de recours internes à caractère suspensif pendants, sept sont en attente de la délivrance d'un laissez-passer consulaire ou d'un accord de réadmission par les autorités consulaires des pays d'origine des intéressés, un en raison du fait que l'état de santé de l'intéressé

est incompatible avec l'éloignement, un n'est actuellement pas localisé sur le territoire national et enfin, deux (pris très récemment) sont en attente de définition des modalités pratiques d'éloignement. Dans l'attente de leur éloignement, les intéressés non incarcérés sont soit placés en rétention administrative, soit assignés à résidence, sur le fondement des dispositions du code de l'entrée et du séjour des étrangers et du droit d'asile, dans l'attente de la levée des obstacles à leur éloignement.

- Trois arrêtes ont été annulés par la juridiction administrative.

Le taux d'exécution de ces mesures d'expulsion prononcées est donc de 69,5%. La mise en œuvre des expulsions peut se heurter à des obstacles juridiques ou opérationnels qui conduisent à ajourner ou différer l'éloignement effectif de la personne expulsée.

Dans ce cas, la personne fait l'objet d'une mesure d'assignation à résidence, sur le fondement des articles L. 561-1 à L. 561-3 du code de l'entrée et du séjour des étrangers et du droit d'asile *« jusqu'à ce qu'il existe une perspective raisonnable d'exécution de son obligation »*.

Cette assignation à résidence, qui prend alors le relais de la mesure de contrôle administratif et de surveillance, est plus contraignante pour la personne concernée et permet une surveillance accrue. En effet, l'autorité administrative peut choisir le lieu de l'assignation et préciser le périmètre en dehors duquel l'étranger ne peut se déplacer sans autorisation préalable (sauf-conduit écrit), en assortissant le cas échéant cette obligation de présentations quotidiennes et d'une obligation de demeurer dans les locaux durant une plage horaire qui ne peut dépasser dix heures consécutives par période de vingt-quatre heures. Pour des raisons de sécurité et d'ordre publics, le lieu d'assignation peut être distinct du lieu de résidence habituelle. Enfin, en cas de comportement lié à des activités à caractère terroriste ou en cas de condamnation à une peine d'interdiction de territoire pour des activités à caractère terroriste, il peut être fait interdiction à l'étranger faisant l'objet de la mesure d'entrer en relation directe ou indirecte avec certaines personnes nommément désignées dont le comportement est lié à des activités à caractère terroriste (art. L. 563-1 du CESEDA).

2. OBJECTIFS POURSUIVIS

L'examen de l'ensemble des décisions prises sur le fondement des articles 1 à 4 de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme pendant les trois premières années d'application de la mesure démontre qu'il a été fait de ces nouveaux instruments une utilisation mesurée et raisonnable dans l'objectif de protéger la population, en complément des outils déjà existants, sans remettre en cause l'exercice de leurs droits et libertés fondamentaux, ainsi que l'ont reconnu tant le Conseil constitutionnel que le juge administratif, pourtant régulièrement saisis de recours contre la loi ou contre les mesures individuelles prises par l'autorité administrative.

L'objectif poursuivi est la pérennisation des mesures de lutte contre le terrorisme instaurées par la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme pour doter durablement l'autorité administrative de moyens lui permettant de prévenir efficacement les actes de nature terroriste.

3. DISPOSITIF RETENU

Il a donc été fait le choix de pérenniser l'ensemble des mesures introduites par la loi n° 2017-1510 du 30 octobre 2017, sous réserve de modifications à la marge portées également par le présent projet de loi.

Les dispositions du Titre II du Livre II du CSI relatives aux périmètres de protection (L. 226-1 – chapitre VI), la fermeture des lieux de culte (L. 227-1 – chapitre VII), les mesures individuelles de contrôle administratif et de surveillance (L. 228-1 – chapitre VIII) et les visites domiciliaires et saisies (L. 229-1 – chapitre IX) ainsi que le chapitre X sur le contrôle parlementaire ne seront donc pas abrogés.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

L'article 1 supprime le II de l'article 5 de la loi n° 2017-1510 du 30 octobre 2017 aux termes duquel les chapitres VI à X du titre II du code de la sécurité intérieure, issus des quatre premiers articles de cette loi, ne sont applicables que jusqu'au 31 juillet 2021.

Lors de son examen de ces dispositions (décisions n° 2017-691 QPC du 16 février 2018 et n° 2017-695 QPC du 29 mars 2018), le Conseil constitutionnel n'a pas conditionné leur conformité à la Constitution, au droit de l'Union européenne ou aux normes internationales à leur caractère temporaire. Leur pérennisation ne saurait donc remettre en cause l'appréciation qu'il a faite de l'équilibre ménagé par le législateur entre l'objectif de sauvegarde de l'ordre public

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Supprimer la clause limitative de durée d'application de ces dispositions aura pour effet de faire entrer définitivement dans l'ordonnancement juridique ces mesures de police administrative, en conservant la réglementation existante moyennant quelques ajouts ou ajustements prévus aux articles suivants, sans conséquence juridique notable.

Les dispositions resteraient, à l'échelle locale, sous la responsabilité des représentants de l'État dans les départements et, à l'échelle nationale, de la compétence de la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur. Cette direction continuera

d'assurer une veille permanente, de piloter juridiquement l'action des préfets et de centraliser toutes les décisions prises afin d'informer régulièrement les commissions de suivi et de contrôle de l'Assemblée et du Sénat créées à cet effet.

Les services d'administration centrale (DLPAJ), les services de renseignement ainsi que leurs services déconcentrés continueront à être particulièrement mobilisés par la mise en œuvre de ces mesures, ainsi que le juge des libertés et de la détention du tribunal judiciaire de Paris, s'agissant de l'autorisation des visites domiciliaires et des saisies, sur le fondement des articles L. 229-1 et suivants du code de la sécurité intérieure.

Les services de police et de gendarmerie locaux seront compétents pour placer en garde à vue les individus se soustrayant à leurs obligations, comme c'est le cas aujourd'hui dans le cas d'une violation d'arrêté d'assignation à résidence.

Le placement sous surveillance électronique mobile fait l'objet d'une délégation de gestion au ministère de la justice (direction de l'administration pénitentiaire). Le coût du PSEM peut être établi à 36 €/personne/jour, sans compter les frais de détérioration, perte ou mise à niveau technique.

4.3. IMPACTS SUR LES PARTICULIERS

L'ensemble des mesures prévues aux articles 1 à 4 de la loi dite « SILT » constituent des mesures de police administrative qui, par essence, ont un impact sur les personnes qu'elles concernent et peuvent avoir pour effet de restreindre leurs libertés.

Toutefois, compte tenu de leur finalité strictement encadrée, aux seules fins de prévenir la commissions d'actes de terrorisme, des conditions exigeantes pour leur prononcé, de leur durée strictement limitée et de leur renouvellement encadré et du contrôle exigeant du juge administratif ou du juge des libertés et de la détention, lors de l'autorisation des visites, ces garanties assurent une conciliation équilibrée entre atteinte à la liberté d'aller et venir et au droit de mener une vie privée et familiale normale et finalité de prévention du terrorisme.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATIONS

5.2.1. Application dans le temps

Le présent article qui a pour conséquence de pérenniser les mesures introduites par la loi n° 2017-1510 du 30 octobre 2017 entrera en vigueur au lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 2 : Élargir le champ d'application des mesures de fermeture des lieux de culte aux lieux en dépendant

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Si la fermeture d'un lieu de culte[12], lieu servant à la célébration de cérémonies organisées en vue de l'accomplissement de certains rites ou pratiques dans le cadre d'une croyance religieuse, est susceptible de résulter du non-respect de la législation relative aux établissements recevant du public ou de facteurs privés (résiliation de bail ou expulsion locative), deux dispositions législatives autorisent l'autorité administrative à prononcer la fermeture d'un lieu de culte aux fins de prévention des actes de terrorisme :

- l'article 8 de la loi n° 55-385 du 3 avril 1955 modifiée relative à l'état d'urgence ;
- l'article L. 227-1 du code de la sécurité intérieure (CSI).

1.1.1. Les motifs de fermeture d'un lieu de culte liés à la prévention d'actes de terrorisme

A - L'état d'urgence

En période d'état d'urgence, en application de l'article 8 de la loi n° 55-385 du 3 avril 1955 modifiée relative à l'état d'urgence, le ministre de l'intérieur ou le préfet peuvent ordonner « *la fermeture provisoire des salles de spectacles, débits de boissons et lieux de réunion de toute nature, en particulier des lieux de culte au sein desquels sont tenus des propos constituant une provocation à la haine ou à la violence ou une provocation à la commission d'actes de terrorisme ou faisant l'apologie de tels actes* […] ».

Sur la dernière période d'application de l'état d'urgence (2015 à 2017), dix-neuf lieux de culte ont fait l'objet d'une fermeture en application de cette disposition. Parmi les fermetures réalisées initialement sous l'état d'urgence, deux ont ensuite fait l'objet d'une nouvelle mesure de fermeture sous le régime créé, lors de la sortie de l'état d'urgence, à l'article L. 227-1 du CSI.

[12] Les collectivités territoriales et le financement des lieux de culte. Rapport d'information de M. Hervé Maurey fait au nom de la délégation aux collectivités territoriales du Sénat, 2015. Le rapport dénombrait : 45 000 lieux de culte catholiques, 4 000 lieux de culte protestants (protestants historiques : 1 400, protestants évangéliques : 2 600), 800 lieux de culte juifs (relevant du Consistoire : 600, hors Consistoire : 200), 130 lieux de culte orthodoxes, 2 450 lieux de culte musulman, 380 lieux de culte bouddhistes, 1 040 lieux de culte des Témoins de Jéhovah et 110 lieux de culte de l'Eglise de Jésus-Christ des Saints des derniers jours. La seule différence notoire émane des orthodoxes car il est fait référence à un Annuaire de l'Eglise orthodoxe en France publié sous l'égide de l'Assemblée des évêques orthodoxes de France et dont la dernière version remonte à 2017

B - Les dispositions du code de la sécurité intérieure

La loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (SILT) a créé l'article L. 227-1 du CSI. Cet article dispose qu' « *aux seules fins de prévenir la commission d'actes de terrorisme, le représentant de l'État dans le département, ou à Paris, le préfet de police peut prononcer la fermeture des lieux de culte dans lesquels les propos qui sont tenus, les idées ou théories qui sont diffusés ou les activités qui se déroulent provoquent à la violence, à la haine ou à la discrimination, provoquent à la commission d'actes de terrorisme ou font l'apologie de tel actes* ».

En application de ces dispositions, la fermeture administrative d'un lieu de culte est soumise à une double condition :

- elle ne peut être prononcée qu'aux fins de prévenir la commission d'un acte de terrorisme ;

- les propos tenus au sein du lieu de culte concerné, les idées ou théories qui y sont diffusées ou les activités qui s'y déroulent doivent soit :

    - provoquer à la violence à la haine ou à la discrimination : le cas échéant, il appartient au préfet d'établir le lien entre cette provocation et le risque de commission d'actes de terrorisme ;

    - provoquer à la commission d'actes de terrorisme ou en faire l'apologie.

Le deuxième alinéa de l'article L. 227-1 du CSI prévoit, en outre, que la durée de fermeture du lieu de culte prévue par arrêté doit être proportionnée aux circonstances qui l'ont motivée et ne peut excéder six mois. En l'absence de dispositions en ce sens, la fermeture du lieu de culte ne peut pas être renouvelée à l'issue du délai ainsi fixé par l'arrêté préfectoral. Habituellement, une mesure de police peut être renouvelée, tant que les troubles à l'ordre public qu'elle vise à prévenir ou à faire cesser durent. Toutefois, compte tenu de ce que les troubles sont inhérents au fonctionnement du lieu, si le lieu est fermé, par définition, ces troubles ne peuvent plus être objectivés. Ainsi, une éventuelle nouvelle mesure de fermeture ne peut reposer que sur des faits intervenus après la réouverture du lieu de culte concerné.

La durée de fermeture de six mois permet au représentant de l'État dans le département, à la collectivité concernée et à la communauté religieuse locale de prendre les mesures nécessaires au retour à une pratique modérée du culte (changement de gestionnaire ou du ministre chargé du culte, renforcement des contrôles et de la vigilance des dirigeants, condamnation explicite des propos tenus et des thèses véhiculées dans le lieu de culte, etc.).

Par ailleurs, ce dispositif est assorti d'une sanction pénale, en application de l'article L. 227-2 du CSI qui dispose que « *la violation d'une mesure de fermeture d'un lieu de culte […] est punie d'une peine de six mois d'emprisonnement et de 7 500 euros d'amende* ».

Tel qu'indiqué précédemment à l'article 1er, le Parlement a souhaité initialement inscrire ces nouvelles dispositions dans un cadre juridique temporaire. Ainsi, le II de l'article 5 de la loi SILT a limité la durée d'application des dispositions des articles L. 227-1 et L. 227-2 du CSI au 31 décembre 2020 dans un premier temps puis au 31 juillet 2021.

1.1.2. Bilan des fermetures de lieu de culte prononcées sur le fondement de la loi SILT

L'article L. 227-1 du CSI s'accompagne de garanties nécessaires au maintien de l'équilibre entre la préservation de l'ordre public et la sauvegarde des libertés publiques, au rang desquels la liberté de conscience et le libre exercice des cultes.

Le champ d'application de la mesure est, tout d'abord, restreint, d'une part, dans sa finalité en visant uniquement à prévenir des actes de terrorisme, et d'autre part, dans son champ d'application en visant les seuls lieux de cultes, entendus au sens strict, soit les lieux où s'exerce concrètement le culte.

En outre, l'instruction et l'édiction d'une mesure de fermeture de lieu de culte nécessitent le rassemblement d'éléments précis et circonstanciés par les services du ministère de l'intérieur, afin de s'assurer que les critères permettant de prononcer la fermeture soient satisfaits.

Les éléments susceptibles de rentrer dans le champ de l'article L. 227-1 du CSI peuvent concerner :

- les messages véhiculés par le lieu de culte de manière active (prêches, organisation de conférences, diffusion d'écrits, invitation de personnalités connues pour leur soutien à des organisations terroristes, incitation au départ sur zones de combat, etc.) ou passive (renvoi à des idées ou théories par mise à disposition des fidèles d'ouvrages, de liens internet renvoyant à des sites prosélytes, etc.) ;

- les fréquentations du lieu de culte : implication des membres dirigeant le lieu de culte ou de fidèles dans des organisations terroristes ou liens entretenus avec des individus en lien avec ces organisations ;

- les activités organisées au sein du lieu de culte : enseignement coranique exaltant les valeurs du *djihad*, activités sportives constituant des lieux d'endoctrinement ou d'entraînement au *djihad* ; organisation d'une filière de combattants ; activités de soutien aux vétérans du *djihad* ou aux détenus pour des motifs en lien avec le terrorisme, etc.

Enfin, une mesure de fermeture d'un lieu de culte prise au titre de l'article L. 227-1 du CSI est subordonnée, d'une part, à la mise en œuvre d'une procédure contradictoire et, d'autre part, au respect d'un délai de 48 heures avant sa notification et son entrée en vigueur. Ce délai permet à toute personne y ayant un intérêt de saisir le juge du référé-liberté d'une requête aux fins de

suspension de la mesure. Placée sous le contrôle rigoureux du juge administratif, cette mesure doit être strictement adaptée, nécessaire et proportionnée aux raisons l'ayant motivée.

À ce jour et depuis l'entrée en vigueur de la loi SILT, huit lieux de culte ont été fermés sur ce fondement, sept étant arrivés à échéance, un seul est encore actuellement en vigueur.

Sur le plan contentieux, sept des huit décisions de fermeture de lieu de culte ont été contestées au fond comme en référé, leur bien-fondé systématiquement été confirmé par le juge administratif.

L'ensemble des mesures de fermetures prononcées ont concerné des mosquées en lien avec la mouvance islamiste radicale.

Dans le détail, il peut être rappelé que :

- trois lieux de culte ont été fermés en 2017 ;
- trois lieux de culte ont été fermés en 2018 ;
- un lieu de culte a été fermé en 2019. ;
- un lieu de culte a été fermé en 2020.

Sur le plan géographique, ont été concernés les départements du Nord (deux fermetures), des Bouches-du-Rhône (deux fermetures), de l'Hérault, de l'Isère et, des Yvelines et de la Seine-Saint-Denis (une fermeture pour chacun de ces départements).

Un seul des sept lieux de culte dont la durée de fermeture est arrivée à son terme a rouvert, après que l'imam responsable de la diffusion de propos et de messages entrant dans le champ de l'article L. 227-1 du CSI a été expulsé du territoire national. Dans deux cas, le bail a été résilié par le propriétaire ; dans deux cas, l'association gestionnaire du lieu de culte a été dissoute ; dans deux cas, l'imam a été expulsé ou a quitté le territoire (voir détail à l'article 1er).

Le nombre réduit de fermetures prononcées au cours des deux dernières années d'application de la loi SILT démontre la difficulté à établir les critères permettant de prononcer ce type de décision, les responsables des lieux de culte potentiellement concernés étant extrêmement prudents et évitant de tenir, en public et durant les prêches, des propos rentrant dans le champ d'application de la loi. Ce n'est donc qu'au prix d'un long travail de renseignement que peut être envisagée une mesure de fermeture de lieu de culte suffisamment étayée.

1.2. CADRE CONSTITUTIONNEL

Au plan constitutionnel, l'article 10 de la Déclaration des droits de l'Homme et du citoyen dispose que « *nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public* ».

Dans sa décision n° 2003-467 DC du 13 mars 2003 (*Loi pour la sécurité intérieure*), le Conseil constitutionnel (CC) a toutefois rappelé que les mesures de police administrative susceptibles

d'affecter l'exercice des libertés constitutionnellement garanties doivent être justifiées par la nécessité de sauvegarder l'ordre public. Par suite, une mesure dictée par un objectif de sauvegarde de l'ordre public, prise dans une stricte acception, à savoir la prévention du terrorisme, peut être justifiée à condition d'être nécessaire, adaptée et proportionnée.

L'article L. 227-1 du CSI a été déclaré conforme à la Constitution par le Conseil constitutionnel dans sa décision n° 2017-695 QPC du 29 mars 2018.

Dans cette décision, le Conseil constitutionnel a reconnu le caractère équilibré de cette disposition, qui permet d'opérer une conciliation entre l'objectif de valeur constitutionnel de prévention des atteintes à l'ordre public et la liberté de conscience et le libre exercice des cultes.

Participent en particulier de cette conciliation :

- le double encadrement des motifs d'une fermeture d'un lieu de culte ;
- la limitation à une durée de six mois d'une mesure de fermeture d'un lieu de culte ;
- la soumission préalable de la mesure de fermeture d'un lieu de culte au triple contrôle d'adaptation, de nécessité et de proportionnalité ;
- l'entrée en vigueur assortie d'un délai d'exécution qui ne peut être inférieur à 48h, afin de permettre à toute personne y ayant intérêt de saisir dans ce délai le juge des référés du tribunal administratif, d'un recours sur le fondement de l'article L. 521-2 du code de justice administrative

L'extension du dispositif aux lieux qui, en raison de leur configuration, dépendent du lieu de culte fermé s'inscrirait pleinement dans ce cadre constitutionnel. Plusieurs modalités d'encadrement sont également prévues s'agissant de ces locaux dépendant :

- un encadrement lié à leur nature : les lieux doivent dépendre, en raison de leur configuration, du lieu de culte dont la fermeture a été prononcée. Il s'agit ainsi de viser les seuls locaux en lien avec le lieu de culte, compte tenu de leur configuration (localisation, destination, modalités de gestion, etc.) ;
- un double encadrement lié à leur usage, puisqu'il doit exister des raisons sérieuses de penser que :
    - ces locaux connexes peuvent être utilisés aux mêmes fins que le lieu de culte dont la fermeture a été prononcée, soit l'application des mêmes critères que ceux permettant de motiver la fermeture des lieux de culte (propos qui sont tenus, idées ou théories qui sont diffusées ou activités qui se déroulent provoquent à la violence, à la haine, ou à la discrimination, provoquent à la commission d'actes de terrorisme ou font l'apologie de tels acte) ;
    - et que l'usage de ces locaux vise à faire échec à l'exécution de la mesure de fermeture du lieu de culte dont ils dépendent. Il est donc nécessaire de démontrer l'intention de contournement de la mesure de fermeture principale.

En outre, ce nouveau dispositif envisagé présente les mêmes garanties procédurales que celles validées par la jurisprudence constitutionnelle (procédure contradictoire, délai d'exécution qui ne peut être inférieur à 48 heures, saisine possible du juge des référés).

Enfin, la disposition envisagée prévoit que la fermeture des locaux dépendant du lieu de culte prend fin à l'expiration de la mesure relative au lieu de culte principal. Le prononcé de cette mesure se limite ainsi à la stricte durée nécessaire à la finalité poursuivie.

L'extension du dispositif aux lieux dépendant du lieu de culte garantit ainsi un strict équilibre entre, d'une part, l'objectif de valeur constitutionnel de prévention des atteintes à l'ordre public et, d'autre part, la liberté de conscience et le libre exercice des cultes.

1.3. CADRE CONVENTIONNEL

La liberté de pensée, de conscience et de religion constitue un droit fondamental, consacré non seulement par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (ci-après « la Convention ») mais par plusieurs textes internationaux et européens.

Aux termes de l'article 9 de la Convention :

« *1. Toute personne a droit à la liberté de pensée, de conscience et de religion ; ce droit implique la liberté de changer de religion ou de conviction, ainsi que la liberté de manifester sa religion ou sa conviction individuellement ou collectivement, en public ou en privé, par le culte, l'enseignement, les pratiques et l'accomplissement des rites.* »

« *2. La liberté de manifester sa religion ou ses convictions ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité publique, à la protection de l'ordre, de la santé ou de la morale publiques, ou à la protection des droits et libertés d'autrui.* »

L'article 9 § 1 de la Convention contient deux volets, relatifs, respectivement, au droit d'avoir une conviction et au droit de la manifester, seul et en privé mais aussi de la pratiquer en société avec autrui et en public.

L'article 10 de la Charte des droits fondamentaux de l'Union européenne protège aussi la liberté de pensée, de conscience et de religion dans les mêmes termes que la Convention.

Ces libertés ne sont pas absolues : puisque la manifestation par une personne de ses convictions religieuses peut avoir des conséquences pour autrui, les rédacteurs de la Convention ont assorti ce volet de la liberté de religion des réserves émises au second paragraphe de l'article 9. Ce dernier dispose que « *toutes restrictions à la liberté de manifester sa religion ou sa conviction doivent être prévues par la loi et constituer des mesures nécessaires dans une société démocratique, à la sécurité publique, à la protection de l'ordre, de la santé ou de la morale publiques, ou à la protection des droits et libertés d'autrui.* »

La jurisprudence de la Cour européenne des droits de l'Homme (CEDH) reprend avec constance cette circonstance que la restriction à la liberté de manifester sa religion ou sa conviction doit être prévue par la loi et nécessaire, dans une société démocratique, à la poursuite de l'un ou de plusieurs des buts légitimes qui y sont énoncés (CEDH, 2013, *Eweida et autres c. Royaume-Uni*, § 80 n° 48420/10, 59842/10, 51671/10 et 36516/10). En d'autres termes, les limitations prévues au second paragraphe de l'article 9 portent uniquement sur le droit de manifester une religion ou une conviction et non sur le droit d'en avoir (CEDH, 2007, *Ivanova c. Bulgarie*, § 79 n° 52435/99).

La CEDH a considéré que les ingérences suivantes étaient nécessaires à la préservation de la sécurité publique et ne constituaient pas une violation de l'article 9 de la Convention :

- la décision des autorités britanniques de fermer le site historique de Stonehenge au moment du solstice d'été et de ne pas autoriser un groupe d'adeptes du druidisme d'y célébrer leur cérémonie solsticiale. La Commission européenne des droits de l'Homme a estimé qu'à supposer même qu'il y avait eu ingérence dans l'exercice des droits au titre de l'article 9, celle-ci visait à préserver la sécurité publique et était justifiée au sens du second paragraphe du même article, considérant notamment le fait que les autorités avaient préalablement déployé des efforts sincères essayant de satisfaire les intérêts des particuliers et des organisations s'intéressant à Stonehenge (*Chappell c. Royaume-Uni* ; voir également *Pendragon c. Royaume-Uni*, décision de la Commission du 14 juillet 1987, n° 12587/86) ;
- la condamnation à une amende avec sursis pour « trouble à la paix » de plusieurs personnes opposées à l'avortement qui avaient pénétré dans les locaux d'une clinique pratiquant des d'avortements et tenu une prière collective à genoux dans le couloir de l'établissement. La Commission a reconnu que la manifestation litigieuse tombait dans le champ d'application de l'article 9, mais que l'ingérence dénoncée était clairement justifiée au regard du second paragraphe du même article (*Van Schijndel et autres c. Pays-Bas*, décision de la Commission du 10 septembre 1997 n° 30936/96) ;
- l'interdiction imposée à une paroisse catholique par la municipalité, de sonner la cloche de l'église avant 7h30 au-dessus d'un certain volume. La Cour a décidé que cette ingérence visait le but légitime de protection des droits d'autrui - en l'espèce, du repos nocturne des riverains et était proportionnée à ce but. En effet, entre 23 heures et 7 h 30, la cloche pouvait toujours être sonnée à condition d'en baisser le volume ; quant au reste de la journée, le volume du son n'était pas limité (CEDH, 16 octobre 2012, *Schilder c. Pays-Bas*, n° 2158/12) ;
- la saisie et la confiscation d'ayahuasca, une substance hallucinogène consommée lors des célébrations de la religion connue comme celle « *du Santo Daime* ». La Cour a décidé que la mesure litigieuse, relevant de la législation sur les stupéfiants, était « *nécessaire dans une société démocratique* » pour la protection de la santé. Dans la mesure où les requérantes se disaient victimes d'une discrimination par rapport aux Églises chrétiennes qui utilisent de l'alcool (du vin de communion) dans leurs célébrations, la Cour a estimé que ces deux situations n'étaient pas comparables : premièrement, le vin n'est pas soumis au régime juridique des stupéfiants, et,

deuxièmement, les rites des Églises chrétiennes ne comprennent pas l'usage de substances psychoactives (6 mai 2014, *FränklinBeentjes et CEFLU-Luz da Floresta c. Pays-Bas*, n° 28167/07).

Par suite, l'extension envisagée de la fermeture de lieux de culte aux lieux en dépendant, pour une durée strictement définie et avec de nombreuses modalités d'encadrement, doit être regardée comme une restriction proportionnée et nécessaire au but poursuivi des droits garantis par la Convention.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

➢ *La fermeture de lieux de culte constitue un instrument efficace de prévention des actes de terrorisme*

Ainsi qu'il a été dit à propos de l'article 1er visant à pérenniser les dispositions des articles 1er à 4 de la loi du 31 octobre 2017, donc l'article 2 a créé l'article L. 227-1 du CSI, cette disposition a prouvé son efficacité quant à son objectif de prévention des actes de terrorisme dans un cadre juridique respectueux des libertés publiques, il apparaît dès lors nécessaire de procéder à sa pérennisation dans l'ordonnancement juridique.

➢ *Les dispositions actuelles sont susceptibles d'offrir des voies de contournements pouvant priver d'effet la mesure de fermeture du lieu de culte*

L'article L. 227-1 du CSI, dans sa rédaction actuelle, ne prend pas en compte le fait que les lieux de culte prennent parfois place dans un ensemble immobilier plus vaste, comprenant par exemple une école ou des locaux techniques et dirigés par les mêmes individus.

En effet, un lieu de culte n'est pas toujours aisément identifiable comme peuvent l'être des cathédrales, des églises, des chapelles, des synagogues, des temples, des pagodes ou des mosquées (qu'on appelle usuellement « édifices du culte »). Un lieu de culte peut jouir ou non d'un accès direct sur la voie publique. Il peut se situer dans un immeuble à vocation d'habitation ou de commerce, sur un lieu de travail, dans une caserne, dans un établissement scolaire, dans un hôpital, dans une prison, dans un lieu public ouvert tel qu'un aéroport ou dans une résidence privée.

Un lieu de culte peut être la propriété d'une association cultuelle, d'une association simplement déclarée, d'une congrégation, d'une collectivité publique, d'un établissement public ou d'un particulier. Il peut être loué par bail à une entité publique ou une entité privée propriétaire. Il peut également être un local mis à disposition par une collectivité publique ou une société civile immobilière.

Par ailleurs, les associations gestionnaires de lieux de culte disposent, dans la plupart des cas, de lieux connexes au lieu de culte, qu'ils se situent au sein du même bâtiment ou à proximité de celui-ci. Ces locaux dépendant du lieu de culte ont généralement vocation, tant que ce dernier est ouvert, à accueillir diverses activités déclarées comme culturelles. Néanmoins, en cas de fermeture du lieu de culte, ces locaux sont susceptibles d'accueillir des activités cultuelles au cours desquelles peuvent se tenir les mêmes propos ou peuvent être diffusées les mêmes idées et par suite, de faire échec à l'exécution de cette mesure.

Ainsi, compte tenu de la diversité de ces situations, la définition restrictive du lieu de culte au seul lieu dans lequel se tient habituellement le culte, rend *de facto* sa fermeture relativement aisée à contourner et tend à priver celle-ci d'effet dès lors qu'il existe des espaces dépendants du lieu de culte au sein du bâtiment en question ou à proximité immédiate, vers lesquels peut être déportée la pratique du culte.

En outre, le dispositif actuel ne permet pas de prendre entièrement en compte la question du sort des fidèles pendant la durée de la fermeture : l'autorité administrative doit pouvoir réagir au risque de création d'un lieu de culte alternatif, non encadré (chapiteaux ou salles mis à disposition des fidèles) dans lesquels sont susceptibles de perdurer les troubles ayant justifié la fermeture.

À titre d'exemple, l'instruction de la mesure de fermeture d'une salle de prière située dans l'Isère, prise en 2019 en application de l'article L. 227-1 du code de la sécurité intérieure, a permis de révéler que l'association gestionnaire de la mosquée était propriétaire de deux locaux distincts dont l'un avait pour vocation l'accueil des fidèles musulmans, tandis que l'autre était alloué aux activités culturelles et mis à disposition en tant que « *prêt à usage* » pour une école coranique, les fidèles de la mosquée pouvant donc, durant la durée de la mesure de fermeture du lieu de culte, s'y réunir, dans les mêmes conditions et sous la conduite du même imam.

De même, l'instruction d'un dossier de fermeture d'un lieu de culte situé dans le Nord a permis de révéler que l'ensemble immobilier comprenait également un centre culturel dont une bibliothèque, ainsi qu'une salle annexe. Malgré la fermeture du lieu de culte sur le fondement de l'article L 227-1 du code de la sécurité intérieure, les notes de renseignement ont permis d'établir que les fidèles continuaient à se réunir dans l'enceinte immobilière et que l'imam continuait à tenir ses prêches dans une salle annexe au lieu effectivement fermé par la mesure initiale.

Par ailleurs, le maintien clandestin du culte dans des locaux proches d'une salle de prière fermée a été constaté dans le cadre d'un lieu de culte salafiste du sud de la France, fermé dans le cadre de l'état d'urgence, puis à nouveau en application de l'article L. 227-1 du code de la sécurité intérieure. Ainsi, malgré la résiliation par le propriétaire de la convention d'occupation à titre précaire de l'association gestionnaire de la salle de prière, un noyau dur de fidèles est venu prier clandestinement dans le local de l'immeuble. Une fermeture de ces locaux dépendant du lieu de culte aurait permis de faire cesser les troubles à l'ordre public résultant du maintien clandestin du culte dans les mêmes conditions de radicalité.

S'agissant d'une salle de prière située dans les Yvelines, fermée sous l'état d'urgence puis par nouvel arrêté en application de l'article L. 227-1 du code de la sécurité intérieure, une perquisition administrative menée dans un local voisin avait permis de constater que ce local constituait une extension de la salle de prière fermée. Il est apparu que les membres de la salle de prière l'utilisaient occasionnellement, que des cours d'arabe y étaient également dispensés et que ce local, réservé aux femmes, était également utilisé par la mosquée pour la prière du vendredi.

Enfin, pour faire échec à la fermeture d'une mosquée décidée pendant l'état d'urgence (mais le cas pourrait être transposable aujourd'hui), l'imam et les fidèles avaient installé un chapiteau face à ce lieu, pour y tenir des prêches et des prières, sans que les instruments administratifs à disposition du préfet permettent de faire cesser ce contournement.

Les cas précités illustrent le fait que les associations gestionnaires de lieux de culte utilisent, dans la plupart des cas, des lieux connexes au lieu de culte, qu'ils se situent au sein du même bâtiment ou à proximité de celui-ci, pour contourner la mesure de fermeture du lieu de culte qu'ils gèrent ou animent. Dans ce contexte, les actuelles dispositions de l'article L. 227-1 du CSI, si elles demeurent efficaces, ne permettent pas d'apporter une réponse satisfaisante aux stratégies de contournement de la mesure de fermeture du lieu de culte.

2.2. OBJECTIFS POURSUIVIS

En étendant la possibilité de fermeture administrative au lieu dépendant d'un lieu de culte, le dispositif proposé vise à empêcher la diffusion des propos, idées ou théories ou la tenue des activités visés par l'article L. 227-1 du CSI, à une échelle plus élargie et, ce faisant, à prévenir plus efficacement la commission d'actes de terrorisme. En effet, même s'il n'existe pas de définition précise du lieu de culte, qui pourrait être regardé comme tout lieu dans lequel se tient un culte, l'acception commune tend à limiter le lieu de culte au lieu « dédié au culte », rendant *de facto* sa fermeture relativement aisée à contourner et tend à priver celle-ci d'effet dès lors qu'il existe des espaces adjacents au lieu de culte et en dépendant ; au sein du bâtiment en question ou à proximité immédiate, vers lesquels peut être déportée la pratique du culte.

Dans ce contexte, il apparaît nécessaire de conférer à la disposition une dimension plus large, en adoptant une approche non pas centrée sur la délimitation physique du lieu de culte mais en considérant l'ensemble des espaces où, en raison de leur configuration, sont susceptibles de se tenir des propos ou activités visés à l'article L. 227-1 du CSI. Compte tenu de la persistance d'un risque terroriste élevé et des contournements aux mesures de fermeture de lieu de culte constatés sur le terrain, cette extension de l'article L. 227-1 du CSI apparaît nécessaire pour préserver sa pleine effectivité.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Une option initialement envisagée était d'étendre la possibilité de fermeture aux autres locaux détenus par les gestionnaires du lieu de culte fermé et pouvant également servir à l'exercice du culte. Ce critère aurait toutefois eu pour effet d'élargir potentiellement le nombre de lieux concernés, lesquels ne desservent pas nécessairement géographiquement les mêmes fidèles que ceux privés du lieu de culte fermé et ne leur offrent donc pas une possibilité de contournement de la mesure.

Par ailleurs, dans plusieurs cas rencontrés, les locaux de déport du lieu de culte n'étaient pas nécessairement gérés par la même personne physique ou morale que le lieu de culte fermé. Ainsi, le critère géographique (ensemble immobilier) ou fonctionnel (lieu annexe utilisé pour des fins cultuelles) doit également être pris en compte.

3.2. DISPOSITIF RETENU

L'option retenue s'appuie sur deux critères :

D'une part, le lieu doit constituer un lieu dépendant du lieu de culte fermé, cette dépendance n'étant pas précisée, ce qui permet de l'établir par tout moyen de preuve (à raison de sa proximité géographique, de la configuration des locaux, de son usage habituel, de sa disposition par la même association gestionnaire et de l'utilisation qui en est faite à titre habituel ou exceptionnel, selon la méthode du faisceau d'indices).

Toutefois, cette dépendance organique ou géographique ne suffit pas, à elle seule, à permettre de fermer le lieu. Il faut également qu'il existe des raisons sérieuses de penser que ces locaux seraient utilisés pour contourner la mesure de fermeture du lieu de culte.

Selon les cas, la mesure de fermeture du lieu dépendant du lieu de culte pourra donc être concomitante à celle prononçant le lieu de culte, s'il existe des raisons sérieuses de penser que le culte est susceptible de se tenir dans le lieu en dépendant (parce que tel a déjà été le cas par exemple ou parce qu'il existe une imbrication très forte entre les lieux...) ou différée, à raison de manœuvres postérieures de contournement de la mesure.

Enfin, la fermeture de ces locaux prend fin à l'expiration de la mesure de fermeture du lieu de culte.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La mesure proposée modifie la rédaction de l'article L. 227-1 du code de la sécurité intérieure

Les manquements aux mesures de fermeture des lieux dépendant du lieu de culte principal seront passibles des sanctions définies à l'article L. 227-2 du CSI (six mois d'emprisonnement et de 7 500 euros d'amende), déjà applicables aux manquements à la fermeture du lieu de culte.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

À l'instar du dispositif existant à l'article L. 227-1 du CSI, l'extension des possibilités de fermeture de locaux dépendant du lieu de culte s'inscrit pleinement dans le respect des dispositions en matière de libertés fondamentales issues du droit international et du droit de l'Union européenne. Dès lors, la mesure proposée n'entre en contradiction avec aucune norme internationale ou issue du droit de l'Union européenne.

4.2. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Dans la mesure où l'autorité préfectorale est seule compétente en matière de fermeture de lieux de culte, la disposition envisagée n'aurait aucun impact sur les collectivités territoriales.

4.3. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La surveillance de la bonne exécution de la mesure de fermeture devrait être assurée par les services de renseignement. Dans la mesure où ces derniers procèdent d'ores et déjà à la surveillance de l'activité des lieux de culte fermés et que les lieux en dépendant, en raison de leur configuration, sont ici entendus comme affectés en réalité au culte, appartenant à un même bâtiment ou à proximité immédiate du lieu fermé, l'impact sur les services administratifs de la mesure envisagée devrait, en tout état de cause, être extrêmement limité.

S'agissant des services de préfecture, l'impact doit également être considéré comme limité, compte tenu du suivi déjà réalisé des lieux concernés ainsi que de l'appui apporté par l'administration centrale du ministère de l'intérieur.

Tout au plus, lorsque la fermeture du lieu dépendant du lieu de culte ne sera pas concomitante à celle du lieu principal, les services des préfectures seront amenés à prendre deux arrêtés successifs, d'abord celui relatif à la fermeture du lieu de culte puis, après constat qu'un lieu dépendant de ce lieu de culte est utilisé à des fins de détournement de cette mesure, l'arrêté de fermeture de ce lieu.

4.4. IMPACTS SUR LES PARTICULIERS

La disposition proposée n'engendrerait aucun impact notable sur les particuliers, si ce n'est un renforcement du caractère effectif de la mesure de fermeture du lieu de culte.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATIONS

5.2.1. Application dans le temps

Les modifications envisagées entrent en vigueur dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

La mesure envisagée s'applique à l'échelle nationale y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 3 (1° a et 2°) : Imposer la fourniture d'un justificatif du lieu d'habitation ou de domicile

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 228-1 du code de la sécurité intérieure prévoit la possibilité pour le ministre de l'intérieur d'enjoindre un certain nombres d'obligations à une personne à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes. Ces obligations, qui ne peuvent être prononcées qu'aux seules fins de prévenir la commission d'actes de terrorisme, sont prévues aux articles L. 228-2 à L. 228-5 du même code.

Parmi les obligations pouvant être prononcées à l'encontre des personnes visées à l'article L. 228-1, au titre des régimes instaurés par les L. 228-2 et L. 228-4 du CSI, figure l'obligation de déclarer leur lieu d'habitation ou de domicile.

Toutefois, le cadre juridique actuel ne leur fait pas obligation de fournir un quelconque justificatif de ce domicile, de sorte que les intéressés peuvent utiliser le motif du changement de domicile pour se déplacer sur le territoire national en toute légalité, sans avoir à s'installer réellement à leur nouvelle adresse.

Enfin, pour les personnes n'ayant pas de domicile (sortants de prison par exemple), il est difficile d'anticiper leur placement sous MICAS à leur sortie de prison, sans réellement connaître le lieu de leur futur domicile.

Leur imposer de justifier de l'adresse de leur domicile ou de leur lieu d'habitation permettrait donc de faire échec à cette stratégie de contournement de la mesure de surveillance, utilisée par certaines personnes placées sous mesure individuelle de contrôle administratif et de surveillance.

La précision en ce sens de cette obligation permettrait également d'assurer un meilleur suivi des demandes d'aménagement de la mesure, notamment celles liées à des déménagements, ou celles liées à l'impossibilité de se présenter à tel ou tel service de police ou de gendarmerie, compte tenu de son éloignement du domicile.

1.2. CADRE CONSTITUTIONNEL

Dans ses décisions 2017-691 QPC du 16 février 2018 et 2017-695 QPC du 29 mars 2018, portant sur la mesure administrative d'assignation à résidence aux fins de lutte contre le terrorisme instaurée par les dispositions de l'article L.228-1 et suivants du code de la sécurité intérieure, le Conseil constitutionnel a constaté que cette mesure de police administrative était nécessaire en ce que le législateur a poursuivi l'objectif de lutte contre le terrorisme, qui participe de l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public, que les conditions de recours à cette mesure sont précises et son champ d'application limité à des personnes soupçonnées de présenter une menace d'une particulière gravité pour l'ordre public.

Par ailleurs, il a considéré que la mesure était proportionnée et n'excédait pas la rigueur nécessaire dès lors, notamment, que le périmètre géographique de l'assignation à résidence ne pouvant être inférieur au territoire de la commune doit permettre à l'intéressé de poursuivre une vie familiale et professionnelle.

L'autorité administrative doit donc, pour établir le périmètre de résidence de l'intéressé d'une part, puis aménager ce périmètre pour permettre la poursuite de sa vie privée et familiale d'autre part, connaître avec certitude son lieu de domicile.

Il n'est en effet pas rare que la personne faisant l'objet d'une telle mesure sollicite une modification de ce périmètre en excipant d'un déménagement, ou bien de contraintes administratives ou familiales justifiant cette modification et l'autorité administrative doit être en mesure d'apprécier, sous le contrôle du juge, le bien fondé de cette demande, au regard des justificatifs produits, dont au premier chef, celui du domicile.

Ainsi, lorsqu'un requérant conteste le périmètre au sein duquel il est assigné à résidence, le juge administratif se livre à un contrôle minutieux des arguments développés devant lui, accordant ainsi une importance cruciale aux éléments les plus probants produits par les parties (CE 26 juill. 2018, n° 422322, point 3).

Par suite, en ce qu'elle permet d'établir le caractère réellement pertinent de la mesure quant au périmètre choisi, l'exigence d'un justificatif de domicile concourt au caractère proportionné de la mesure.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Exiger un justificatif du lieu d'habitation permettra à l'autorité administrative de déterminer avec plus de précision le périmètre de résidence de la personne faisant l'objet d'une mesure individuelle de contrôle administratif et de surveillance et de s'assurer de la réalité des changements de domicile déclarés.

2.2. OBJECTIFS POURSUIVIS

En terme opérationnel, exiger un justificatif aura pour conséquence de connaître précisément le lieu d'habitation ou de domicile de l'individu faisant l'objet d'une mesure de police administrative et d'adapter au mieux les mesures de surveillance.

3. DISPOSITIF RETENU

Les personnes visées à l'article L. 228-1 du code de la sécurité intérieure et faisant l'objet d'une mesure individuelles de contrôle administratif et de surveillance prévue aux articles L. 228-2 et L. 228-4 du CSI ne devront plus seulement déclarer leur lieu d'habitation ou de domicile et tout changement de lieu d'habitation ou de domicile, mais également fournir un justificatif à cette occasion.

En la matière la justification du domicile étant libre à défaut de texte l'encadrant, il appartiendra à la personne concernée d'apporter tous éléments permettant d'en justifier, sous le contrôle de l'administration et des services de renseignement.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Le 3° de l'article L. 228-2 et le 1° de l'article L. 228-4 du CSI sont modifiés.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services administratifs du ministère de l'intérieur, qui édictent les mesures de MICAS et les modifient en cas de changement de domicile, seront destinataires de ce justificatif, afin d'instruire les mesures.

Les services de police et de gendarmerie, auxquels se présentent les personnes dans le cadre de leurs obligations, et les services de renseignement qui procèdent à la surveillance de ces personnes, seront également destinataires de cette information.

4.3. IMPACTS SUR LES PARTICULIERS

Les personnes concernées devront justifier de leur lieu de domicile ou de tout changement de ce lieu, à l'appui de la mesure initiale ou d'une demande d'aménagement de celle-ci.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATIONS

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 3 (1° b) : Faire obligation à certaines personnes placées sous surveillance, dans le cadre de l'article L. 228-2 du code de la sécurité intérieure, de ne pas paraître temporairement dans certains lieux dans lesquels se tiennent des évènements exposés, par leur ampleur ou leurs circonstances particulières, à une menace terroriste

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 228-1 du code de la sécurité intérieure prévoit la possibilité pour le ministre de l'intérieur d'enjoindre un certain nombre d'obligations à une personne à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes.

Ces obligations, qui ne peuvent être prononcées qu'aux seules fins de prévenir la commission d'actes de terrorisme, sont prévues aux articles L. 228-2 à L. 228-5 du même code et peuvent selon les cas, être prononcées pour une durée de trois mois ou de six mois, sans toutefois pouvoir excéder une durée cumulée de douze mois. Par ailleurs, au-delà de six mois, leur renouvellement est subordonné à l'existence d'éléments nouveaux ou complémentaires justifiant la pérennité des conditions exigées pour leur prononcé.

La personne placée sous une telle mesure peut faire l'objet de deux régimes d'obligations, alternatifs, dont la durée est variable au regard de leur intensité :

Celui prévu aux articles L. 228-2 et L. 228-3 du code de la sécurité intérieure, parmi lesquelles figurent l'obligation de ne pas se déplacer à l'extérieur d'un périmètre géographique déterminé, de se présenter périodiquement aux services de police ou aux unités de gendarmerie, dans la limite d'une fois par jour, ou à défaut de faire l'objet d'un placement sous surveillance électronique mobile, de déclarer son lieu d'habitation et tout changement de lieu d'habitation. Ces obligations peuvent être prononcées pour une durée maximale de trois mois, renouvelable dans la limite d'une durée cumulée de douze mois, leur renouvellement étant subordonné à la démonstration d'éléments nouveaux et complémentaires au-delà d'une durée de six mois.

Celui prévu à l'article L. 228-4 du même code, lorsque l'intéressé ne fait pas l'objet des obligations prévues aux articles L. 228-2 et L. 228-3, par lequel le ministre peut faire obligation à la personne concernée de déclarer son domicile et tout changement de domicile, de signaler ses déplacements à l'extérieur d'un périmètre déterminé ne pouvant être plus restreint que le

territoire de la commune de son domicile, de ne pas paraître dans un lieu déterminé, qui ne peut inclure le domicile de la personne intéressée, en tenant compte de la vie familiale et professionnelle de la personne intéressée. Ces obligations peuvent être prononcées pour une durée maximale de six mois, renouvelable dans la limite d'une durée cumulée de douze mois, leur renouvellement étant subordonné à la démonstration d'éléments nouveaux et complémentaires au-delà d'une durée de six mois.

Enfin, au titre de l'article L. 228-5, le ministre peut faire interdiction aux personnes soumises à l'un ou l'autre régime, de ne pas se trouver en relation directe ou indirecte avec certaines personnes, nommément désignées, dont il existe des raisons sérieuses de penser que leur comportement constitue une menace pour la sécurité publique. Cette interdiction peut être prononcée pour une durée maximale de six mois, renouvelable dans la limite d'une durée cumulée de douze mois, son renouvellement étant subordonné à la démonstration d'éléments nouveaux et complémentaires au-delà d'une durée de six mois.

Il résulte de ces dispositions qu'en l'état actuel du droit, une personne assujettie au régime d'obligations prévues aux articles L. 228-2 et L. 228-3 ne peut, en outre, faire l'objet d'une interdiction de paraître en certains lieux alors qu'opérationnellement, une telle possibilité serait utile.

1.2. CADRE CONSTITUTIONNEL

Il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et, d'autre part, le respect des droits et libertés reconnus à tous ceux qui résident sur le territoire de la République. Parmi ces droits et libertés figure la liberté d'aller et de venir garantie par les articles 2 et 4 de la Déclaration des droits de l'Homme et du citoyen (not. CC 13 mars 2003, n° 2003-467 DC). Ainsi, les mesures de police administrative susceptibles d'affecter la liberté d'aller et de venir doivent être justifiées par la nécessité de sauvegarder l'ordre public et proportionnées à cet objectif (CC 9 juillet 2010, n° 2010-13 QPC).

Le Conseil constitutionnel a déjà, à plusieurs reprises et hors contexte d'état d'urgence (sur les mesures de police administrative en présence de circonstances exceptionnelles, v. not. 22 décembre 2015, n° 2015-527 QPC), examiné la constitutionnalité de mesures de polices prises dans un objectif de sauvegarde de l'ordre public et, plus particulièrement de lutte contre le terrorisme, au prisme de la liberté d'aller et venir.

Il a notamment considéré, à propos de l'article L. 332-16-2 du code du sport autorisant les préfets de département à restreindre la liberté d'aller et de venir de supporters d'une équipe sur les lieux d'une manifestation sportive, que « *les dispositions contestées renforcent les pouvoirs de police administrative en cas de grands rassemblements de personnes, à l'occasion d'une manifestation sportive, qui sont susceptibles d'entraîner des troubles graves pour l'ordre public ; qu'il appartient à l'autorité administrative, sous le contrôle du juge, de définir, à partir de critères objectifs et avec précision, les personnes ou catégories de personnes faisant l'objet des mesures de restriction de déplacement ; que ces mesures doivent être justifiées par la*

nécessité de sauvegarder l'ordre public et ne pas porter une atteinte disproportionnée à la liberté d'aller et venir ; qu'elles peuvent être contestées par les intéressés devant le juge administratif, notamment dans le cadre d'un référé-liberté ; qu'eu égard aux objectifs que s'est assignés le législateur et à l'ensemble des garanties qu'il a prévues, les dispositions contestées sont propres à assurer, entre le respect de la liberté d'aller et venir et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée » (CC 10 mars 2011, n° 2011-625 DC).

Il a également jugé conforme à la Constitution, compte tenu des garanties qui encadrent l'édiction de cette mesure, l'interdiction de sortie du territoire (v. CC 14 octobre 2015, n° 2015-490 QPC) ou encore l'assignation à résidence d'étrangers faisant l'objet d'une mesure d'éloignement, en relevant que ces derniers ne disposaient pas d'un droit de séjour et de circulation comparable à celui des titulaires de la nationalité française (v. CC 9 juin 2011, n° 2011-631 DC ; 1er décembre 2017, n° 2017-674 QPC).

S'agissant des dispositions de l'article L. 226-1 du code de la sécurité intérieure, qui donnent aux préfets la possibilité d'instituer des périmètres de protection au sein desquels l'accès et la circulation des personnes sont réglementés, le Conseil constitutionnel, après avoir rappelé la nécessaire conciliation que le législateur doit opérer entre la liberté d'aller et venir et l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public, a examiné la finalité et les conditions de mise en œuvre des dispositions contestées, la portée de l'atteinte engendrée par leur application et, enfin, leur possible renouvellement. Pour, *in fine*, et au prix d'une réserve d'interprétation tenant à la démonstration de la persistance du risque en cas de renouvellement de la mesure, retenir la conformité à la Constitution du dispositif ainsi créé (CC 29 mars 2018, n° 2017-695 QPC).

S'agissant de mesure visant une personne physique en particulier, le Conseil analyse successivement les modalités de mise en œuvre de la mesure, la portée de l'atteinte engendrée par cette mesure, les conditions de son renouvellement et enfin la possibilité pour la personne visée de contester utilement cette mesure (not. CC 14 oct. 2015, n° 2015-490 QPC, s'agissant de l'interdiction de sortie du territoire).

C'est notamment à un tel examen que le Conseil constitutionnel s'est livré pour reconnaître (sous une réserve tenant à la durée maximale de la mesure) qu'en instaurant les mesures individuelles de contrôle administratif et de surveillance prises sur le fondement de l'article L. 228-2 du code de la sécurité intérieure, le législateur a assuré une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et, d'autre part, la liberté d'aller et de venir (CC, 19 février 2018, n° 2017-691 QPC). Là encore, le contrôle que le juge administratif pourra opérer sur une telle mesure a été particulièrement souligné par le juge constitutionnel (sur les modalités de ce contrôle dans le cadre d'un référé-liberté : CE, ord., 14 mars 2018, n° 418689).

Il suit de là qu'une disposition nouvelle visant à interdire à une personne assujettie au régime d'obligations prévues aux articles L. 228-2 et L. 228-3 de paraître en certains lieux ne sembleraient pas présenter de risque d'inconstitutionnalité.

1.3. CADRE CONVENTIONNEL

L'article 5 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales dispose que « *Toute personne a droit à la liberté et la sûreté. Nul ne peut être privé de sa liberté, sauf dans les cas suivants et selon les voies légales*. »

Pour déterminer si un individu se trouve « privé de sa liberté » au sens de l'article 5, il faut partir de sa situation concrète et prendre en compte un ensemble de critères comme le genre, la durée, les effets et les modalités d'exécution de la mesure considérée (CEDH, *Guzzardi c. Italie*, 6 novembre 1980, § 92).

S'agissant d'un régime de « liberté surveillée » (obligation de présentation à l'autorité de police, permanence du lieu de résidence, interdiction de s'éloigner de la commune, assignation à résidence dans un créneau horaire), la Cour estime qu'elle ne constitue pas une privation de liberté au sens de l'article 5 de la Convention, mais une simple restriction à la liberté de circuler (CEDH 20 avril 2010, *Villa c. Italie*, n° 19675/06).

De même, ne constitue pas une privation de liberté le « placement sous surveillance de la police » et l'« assignation à domicile », mesures préventives impliquant certaines restrictions à la liberté de circulation, ainsi que l'obligation de se plier régulièrement à certaines procédures de contrôle mais n'impliquant aucun confinement des intéressés dans un local délimité, ceux-ci restant en principe libres de se déplacer dans les limites géographiques de leur district (CEDH 9 février 2006, *Freimanis et Lidums c/ Lettonie,* n° 73443/01).

S'agissant de la proportionnalité de mesures faisant obstacle à la liberté d'aller et venir, celles-ci ne se justifient qu'aussi longtemps qu'elles tendent effectivement à la réalisation de l'objectif qu'elles sont censées poursuivre (CEDH 13 novembre 2003, *Napijalo c. Croatie*, n° 66485/01). Fût-elle initialement justifiée, une mesure restreignant la liberté de circulation d'une personne peut devenir disproportionnée et violer les droits de cette personne si elle se prolonge automatiquement pendant longtemps (CEDH 31 octobre 2006, *Földes et Földesné Hajlik c. Hongrie*, n° 41463/02).

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

L'article L. 228-1 du CSI implique deux séries d'obligations, les premières plus restrictives que les secondes : les premières impliquent l'interdiction de se déplacer à l'extérieur d'un périmètre géographique déterminé, la présentation périodique aux services de police ou aux unités de gendarmerie et la déclaration du lieu d'habitation ou tout changement de lieu d'habitation (L. 228-2) alors que les secondes imposent seulement la déclaration de domicile, le signalement des déplacements hors d'un périmètre et l'interdiction de paraître en un lieu déterminé (L. 228-4).

Par suite, un individu faisant l'objet d'une interdiction de déplacement en dehors d'un périmètre ne peut simultanément faire l'objet d'une interdiction de paraître au sein de ce périmètre, alors que les besoins de surveillance et de contrôle peuvent parfois commander de cumuler ces interdictions, notamment en cas d'évènement particulier, exposé par son ampleur ou ses circonstances particulières, à un risque élevé de menace à caractère terroriste.

C'est pourquoi il est proposé d'en faire une obligation pouvant être prononcée dans le cadre des obligations de l'article L. 228-2, tout en distinguant son contenu de celle pouvant être prononcée au titre de l'article L 228-4.

2.2. OBJECTIFS POURSUIVIS

Il apparait nécessaire de prévoir une interdiction de paraitre de manière cumulative aux obligations prévues à l'article L. 228-2. Celle-ci serait plus limitée dans sa durée que l'obligation de ne pas paraître dans un lieu déterminée prévue au titre du L. 228-4, qui peut être prononcée pour une durée de six mois. La nouvelle disposition viserait à écarter un individu, qui fait l'objet d'une surveillance et d'une astreinte à résider dans un périmètre déterminé, d'un lieu se trouvant précisément au sein de ce périmètre, pour autant qu'elle soit nécessaire. En d'autres termes, cette obligation ne serait pas systématiquement prononcée à l'égard de toutes les personnes placées dans le cadre de l'article L. 228-2 mais seulement à l'égard de celle astreintes à résider dans un périmètre au sein duquel doit se tenir un évènement exposé à risque élevé de menace à caractère terroriste, et pour la seule durée de cet évènement.

Ainsi, il se peut qu'au sein de ce périmètre, se tiennent des évènements ponctuels, exposés par leur ampleur ou leurs circonstances particulières, à une menace terroriste. Il serait alors paradoxal que la mesure de surveillance dont fait l'objet l'intéressé lui fasse obligation de se maintenir dans le périmètre où se tient l'évènement, et donc à proximité de cet évènement, au contraire de pouvoir l'en écarter.

Confrontée à de pareilles hypothèses, liées à la tenue d'un sommet international, d'une rencontre sportive internationale ou d'un évènement festif de grande ampleur, le ministre de l'intérieur a dû, par le passé, se résoudre à abroger les obligations découlant de l'article L. 228-2, et notamment l'obligation de résider dans le périmètre de l'évènement, pour pouvoir soumettre la personne concernée aux obligations de l'article L. 228-4, dont au premier chef l'interdiction du paraître dans le ou les lieux concernés.

Une telle solution n'est assurément pas adaptée à l'objectif poursuivi par la mesure qui vise, à la fois à surveiller la personne, de manière assez stricte s'agissant de celles placées sous le régime d'obligations prévues à l'article L. 228-2 mais également, à pouvoir l'écarter en tant que de besoin d'un lieu où elle est susceptible de mener à bien ses desseins à caractère terroriste.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Il avait d'abord été envisagé d'ajouter à l'article L. 228-5 du code de la sécurité intérieure, l'obligation de ne pas paraître dans un lieu déterminé, cette obligation étant, au même titre que l'obligation de ne pas entrer en relation avec certaines personnes déterminées, rendue commune aux deux régimes. Cet ajout avait donc pour conséquence de supprimer cette obligation du régime d'obligations prévues à l'article L. 228-4 du code de la sécurité intérieure.

Toutefois, un tel aménagement et surtout un alignement de la durée de l'obligation sur la durée maximale de six mois, renouvelable, applicable au titre de l'article L. 228-4, aurait alourdi les obligations pesant sur les personnes soumises aux obligations du L. 228-2, excédant ainsi la rigueur nécessaire au regard de l'objectif poursuivi.

3.2. DISPOSITIF RETENU

L'option finalement retenue consiste à ajouter au régime des obligations prévues à l'article L. 228-2, une interdiction de paraître dont les effets sont plus limités que celle pouvant être prononcée dans le cadre de l'article L. 228-4 afin d'atténuer la rigueur du cumul de cette obligation avec celle résultant de l'astreinte à demeurer dans un périmètre déterminé.

La mesure est nécessaire, pour permettre d'écarter d'un lieu dans lequel se tient un évènement exposé à la menace terroriste, une personne dont il existe des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité, tout en la maintenant sous surveillance étroite. Elle est adaptée en ce qu'elle permet d'atteindre ces deux objectifs.

Enfin, elle est proportionnée dès lors qu'elle est assortie de plusieurs garanties de nature à en atténuer la rigueur résultant du cumul avec une obligation de résider dans un périmètre déterminé.

Cette interdiction de paraître est **limitée dans ses finalités** : elle ne vise qu'à écarter une personne astreinte à résider dans un périmètre, d'un lieu se trouvant au sein de ce périmètre et dans lequel se tient un évènement exposé, par son ampleur ou ses circonstances particulières, à une menace terroriste. Le ou les lieux concernés doivent être précisément désignés, leur définition s'inspirant de celle prévue à l'article L. 211-11-1 du code de la sécurité intérieure relatif aux grands évènements désignés par décret, sans toutefois se réduire à cette seule catégorie. L'arrêté doit indiquer précisément les motifs qui permettent de qualifier le lieu ainsi que ceux qui justifient l'interdiction pour la personne de s'y rendre.

La durée de la mesure est strictement **limitée à la durée de l'évènement** dont il s'agit d'écarter la personne concernée. Il s'agit donc d'une mesure ponctuelle, pouvant aller d'une journée à quelques jours, selon l'évènement en cause. Dès lors que cette durée est connue à l'avance, compte tenu de la programmation de l'évènement, il n'est pas paru utile de limiter facticement la durée de l'interdiction à des périodes courtes, pouvant être renouvelée. En effet, en pareil cas, le renouvellement serait alors automatique et lié au seul constat objectif que l'évènement

est toujours en cours et non au comportement de l'intéressé ou au risque que fait peser sa présence aux abords ou au sein de l'évènement. Pour cette raison, il a donc été décidé d'aligner strictement, dès le prononcé de la mesure, la durée de l'interdiction sur la durée de l'évènement, dans la limite toutefois de trente jours au titre de chaque évènement.

Cette limitation est de nature à atténuer la rigueur de la mesure en la limitant à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi, la plupart des évènements se tenant dans une limite temporelle inférieure à trente jours ou comptant plusieurs manifestations distinctes, susceptibles de faire l'objet d'interdictions ponctuelles. Dans cette dernière hypothèse, la mesure d'interdiction n'aura vocation à être prononcée que pour les manifestations se déroulant dans le périmètre de résidence de l'intéressé.

Ainsi, les Jeux Olympiques par exemple se dérouleront du 26 juillet au 11 août 2024, puis seront suivis des jeux paralympiques du 28 août au 8 septembre, soit une durée totale inférieure à un mois dans les deux cas. Par ailleurs, les sites retenus pour les épreuves sont situés dans des communes et départements distincts et par définition, les épreuves n'y durent que quelques jours au plus. Par suite, l'interdiction de paraitre ne pourra concerner que les personnes faisant l'objet d'une obligation de résidence dans le périmètre de la commune ou du département simultanément à la tenue de l'épreuve et pour la seule durée de celle-ci.

Par ailleurs, **afin de garantir un droit au recours effectif, la disposition prévoit que la mesure d'obligation de ne pas paraître dans un lieu déterminé est notifiée au moins 48h à l'avance**, permettant ainsi au juge de statuer en urgence, notamment par la voie du référé-liberté, sur son bien fondé. Cette garantie s'inspire de celle exigée par le Conseil constitutionnel s'agissant de l'interdiction de prendre part à une manifestation revendicative (Décision n° 2019-780 DC du 4 avril 2019), le juge constitutionnel ayant estimé qu'en tant qu'elle prévoyait une possibilité de notification au cours de la manifestation avec exécution d'office, la mesure était disproportionnée en ce qu'elle portait une atteinte excessive à la possibilité d'exercer un recours effectif, même en référé-liberté, à son encontre.

Quand bien même les libertés en cause seraient-elles de nature différente : liberté d'aller et venir d'une part, et liberté d'expression, de réunion et de manifestation d'autre part, la mesure prend acte de la nécessité de garantir, dans toute la mesure du possible, un droit au recours effectif en permettant la saisine du juge et sa possible intervention avant son entrée en vigueur, afin d'éviter un non-lieu, notamment lorsque la mesure est de brève durée.

Toutefois, l'urgence, qui doit être motivée, peut empêcher une notification dans le délai de 48h, soit parce que la dangerosité de la personne concernée n'a été décelée que tardivement et moins de 48h avant l'évènement dont il convient de l'écarter, soit parce que la personne est sortie de détention également à moins de 48h de cet évènement. Dans ce cas, l'interdiction pourra être notifiée moins de 48h avant son entrée en vigueur, l'urgence devant alors être dûment justifiée.

Enfin, la mesure doit **tenir compte de la vie privée et familiale de la personne concernée**, ce qui, s'agissant d'interdiction de paraître dans des lieux abritant des évènements ponctuels, par

définition distincts d'un domicile ou d'un lieu de travail, devrait pouvoir s'aménager, sans réduire l'efficacité opérationnelle de la mesure

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Il est créé un nouvel alinéa après le 3° de l'article L. 228-2 du code de la sécurité intérieure.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services du ministère de l'intérieur devront ajouter cette obligation aux obligations figurant dans les arrêtés de MICAS (lorsque la date de l'évènement sera déjà connue et se situera dans le temps d'exécution de cette mesure, ou bien prendre un arrêté complémentaire si nécessaire.

4.3. IMPACTS SUR LES PARTICULIERS

Les personnes soumises à ces mesures devront ne pas se trouver dans le périmètre d'interdiction défini par la mesure, le fait de se soustraire aux obligations fixées en application des articles L. 228-2 étant, aux termes de l'article L. 228-7, puni de trois ans d'emprisonnement et de 45 000 € d'amende.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATIONS

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 3 (3°) : Prévoir la possibilité de prolonger la MICAS pendant une durée maximale de deux ans lorsque l'intéressé a été condamné pour des faits de terrorisme

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

1.1.1. Rappel du cadre juridique applicable aux mesures individuelles de contrôle administratif et de surveillance

L'article L. 228-1 du code de la sécurité intérieure prévoit la possibilité pour le ministre de l'intérieur d'enjoindre un certain nombres d'obligations à une personne à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes.

Ces obligations, qui ne peuvent être prononcées qu'aux seules fins de prévenir la commission d'actes de terrorisme, sont prévues aux articles L. 228-2 à L. 228-5 du même code et peuvent selon les cas, être prononcées pour une durée de trois mois ou de six mois, sans toutefois pouvoir excéder une durée cumulée de douze mois. Par ailleurs, au-delà de six mois, leur renouvellement est subordonné à l'existence d'éléments nouveaux ou complémentaires justifiant la pérennité des conditions exigées pour leur prononcé.

1.1.2. Une utilité opérationnelle confirmée, notamment à l'encontre des sortants de détention

Les mesures individuelles de contrôle administratif et de surveillance ont été, au cours des deux dernières années, majoritairement prononcées à l'encontre de personnes sortant de détention. Cette population représentait ainsi 57 % des mesures prononcées entre le 1er novembre 2018 et le 31 octobre 2019 (77 mesures sur un total de 134 mesures) et 71 % des mesures prises entre le 1er novembre 2020 (102 des 143 mesures prononcées, correspondant à 88 personnes). Parmi les 66 mesures en vigueur au 31 octobre 2020, 51 concernent des individus sortant de prison (soit 77 %).

L'augmentation importante de ce nombre sur les deux dernières années d'application de la loi s'explique par le fait que de nombreux individus condamnés pour association de malfaiteurs en lien avec le terrorisme, ou participation à des actes terroristes, dans les années 2014-2015 ont désormais purgé leur peine. Plusieurs détenus terroristes islamistes sunnites (TIS) incarcérés

dans les prisons françaises ont ainsi été ou seront prochainement libérés : 45 en 2020 ; 64 en 2021 ; 47 en 2022 ; 38 en 2023.

Ces individus présentent des enjeux sécuritaires multiples à la sortie de détention : prosélytisme, menace à court terme représentée par des profils impulsifs, menace à moyen et long terme relative à des projets d'attentats ou encore tentative de redéploiement vers des zones de jihad à l'étranger.

Afin de favoriser leur suivi, a donc été instauré, dès juillet 2018, un dispositif d'anticipation et de prise en compte, par les services, des sorties de ces individus. Une unité permanente a été créée au sein de l'unité de coordination de la lutte antiterroriste (UCLAT) et un comité de suivi rassemblant des représentants des services des ministères de l'intérieur et de la justice se réunit tous les mois afin de définir les modalités de suivi des personnes dont la libération est proche. Il s'agit ainsi d'éviter tout conflit négatif de compétence et de s'assurer d'un suivi effectif par un service à l'issue de l'incarcération.

Dans le cadre de ce dispositif, la MICAS est conçue comme une mesure de police administrative permettant de surveiller l'individu sortant de prison, lorsqu'en détention, il a manifesté la pérennité de son engagement radical, par le biais de ses fréquentations, des visites qu'il a reçues, de ses activités licites ou non. Ces mesures s'articulent le plus souvent avec celles résultant du contrôle post-peine, dont le service pénitentiaire d'insertion et de probation est en charge.

Y compris lorsqu'elles interviennent en complément d'une mesure de surveillance judiciaire, les mesures individuelles de contrôle administratif et de surveillance prises à l'égard de ces individus sortant de détention présentent un grand intérêt dans la mesure où il est difficile d'anticiper leur comportement, au regard de celui qu'ils ont adopté en prison. Cette surveillance permet alors d'observer leurs relations habituelles (volontaires et non pas imposées comme en détention), leur pratique religieuse (fréquentation de telle ou telle mosquée), leur activité sur les réseaux sociaux, leurs efforts de réinsertion, etc.

1.2. CADRE CONSTITUTIONNEL

Pour prévenir la commission d'actions violentes de la part de personnes radicalisées, présentant des indices de dangerosité et connues comme telles par les services de police, la loi distingue les mesures de police administrative et les mesures de sûreté.

1.2.1. S'agissant des mesures de police administrative

Les mesures de surveillance administrative des personnes à l'égard desquelles il existe des indices de dangerosité sont qualifiées de mesure de police administrative, au regard de la finalité de la mesure qui **vise à** préserver l'ordre public (décision n° 2015-527 QPC du 22 décembre 2015 relative à l'assignation à résidence sous l'état d'urgence) ou à prévenir la commission d'actes de terrorismes (décision n° 2015-691 QPC).

Dans ses décisions 2017-691 QPC et 2017-695 QPC, portant sur la mesure administrative d'assignation à résidence aux fins de lutte contre le terrorisme instaurée par les dispositions de l'article L.228-1 et suivants du code de la sécurité intérieure, le Conseil constitutionnel a constaté que cette mesure de police administrative était **nécessaire** en ce que le législateur a poursuivi l'objectif de lutte contre le terrorisme, qui participe de l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public, que les conditions de recours à cette mesure sont précises et son champ d'application limité à des personnes soupçonnées de présenter une menace d'une particulière gravité pour l'ordre public.

Par ailleurs, il a considéré que la mesure était **proportionnée** et n'excédait pas la rigueur nécessaire, le périmètre géographique de l'assignation à résidence ne pouvant être inférieur au territoire de la commune et devant permettre à l'intéressé de poursuivre une vie familiale et professionnelle, l'obligation de présentation périodique aux services de police ou aux unités de gendarmerie ne pouvant excéder une présentation par jour, la durée de la mesure ne pouvant excéder trois mois, son renouvellement au-delà d'une durée cumulée de six mois étant subordonné à la production par le ministre de l'intérieur d'éléments nouveaux ou complémentaires.

Enfin, le Conseil constitutionnel a, au nom du **droit au recours effectif** ouvert à la personne concernée, censuré les mécanismes de recours prévus par le législateur, en imposant un délai de jugement plus rapide au juge du fond, compte tenu de la durée limitée de chaque mesure, et en renforçant le contrôle du juge sur les mesures de renouvellement, lesquelles notifiées cinq jours avant leur entrée en vigueur, peuvent faire l'objet d'un recours sous 48h et d'un jugement sous 72h, le juge constitutionnel ayant exigé que l'office du juge soit étendu à celui de l'excès de pouvoir et non limité à celui de l'atteinte grave et manifestement illégale à une liberté fondamentale.

S'agissant de la **durée des obligations**, le Conseil constitutionnel a également jugé que compte tenu de sa rigueur, la mesure prévue à l'article L. 228-1 du code de la sécurité intérieure ne saurait, sans méconnaître les exigences constitutionnelles précitées, excéder, de manière continue ou non, une durée totale cumulée de douze mois (cons. 17) et à cet égard, les commentaires aux cahiers de la 2ème décision n° 2017-695 QPC du 29 mars 2018 relative à cette mesure, indiquant que : « *Le Conseil a souligné que, quelle que soit la gravité de la menace qui la justifie, une telle mesure de police administrative ne peut se prolonger aussi longtemps que dure cette menace. L'assignation à résidence n'est pas une mesure de surveillance et de contrôle à laquelle l'État est assuré de toujours pouvoir recourir* ».

Une telle appréciation fait écho à la décision qu'il avait rendue à propos des assignations à résidence prononcée sur le fondement de l'article 6 de la loi du 3 avril 1955 relative à l'état d'urgence (n° 2017-624 QPC du 16 mars 2017), selon laquelle au-delà de douze mois, une mesure d'assignation à résidence ne saurait, sans porter une atteinte excessive à la liberté d'aller et de venir, être renouvelée que sous réserve, du respect de trois conditions :

- le comportement de la personne en cause doit constituer une menace d'une particulière gravité pour la sécurité et l'ordre publics ;

- l'autorité administrative doit produire des éléments nouveaux ou complémentaires ;
- doivent être prises en compte dans l'examen de la situation de l'intéressé la durée totale de son placement sous assignation à résidence, les conditions de celle-ci et les obligations complémentaires dont cette mesure a été assortie.

Pour autant, le Conseil constitutionnel a jugé à cette occasion, et cette appréciation paraît transposable aux mesures prévues à l'article L. 228-1 précité, que la seule prolongation dans le temps d'une mesure d'assignation à résidence ordonnée dans les conditions prévues par l'article 6 de la loi du 3 avril 1955 n'a pas pour effet de modifier sa nature et de la rendre assimilable à une mesure privative de liberté. Dès lors, le grief tiré de la méconnaissance de l'article 66 de la Constitution doit être écarté (QPC 2017-624).

De même, s'agissant de la **mesure d'assignation à résidence de longue durée applicable à l'étranger** faisant l'objet d'une interdiction du territoire ou d'un arrêté d'expulsion qui ne connaît pas de durée maximale (L. 561-1 du code de l'entrée et du séjour des étrangers et du droit d'asile – CESEDA), le Conseil constitutionnel a relevé que « *le maintien d'un arrêté d'expulsion, en l'absence de son abrogation, atteste de la persistance de la menace à l'ordre public constituée par l'étranger. En revanche, si le placement sous assignation à résidence après la condamnation à l'interdiction du territoire français peut toujours être justifié par la volonté d'exécuter la condamnation dont l'étranger a fait l'objet, le législateur n'a pas prévu qu'au-delà d'une certaine durée, l'administration doive justifier de circonstances particulières imposant le maintien de l'assignation aux fins d'exécution de la décision d'interdiction du territoire* », conduisant à la censure partielle des dispositions (décision n° 2017-674 QPC).

Enfin, s'agissant d'une autre mesure de police administrative, **l'interdiction de sortie du territoire**, prononcée en application de l'article L. 224-1 du code de la sécurité intérieure, le Conseil constitutionnel a jugé que sa durée n'excédait pas la rigueur nécessaire à la poursuite de son objectif, dès lors que l'interdiction de sortie du territoire peut être prononcée pour une durée maximale de six mois à compter de sa notification, qu'elle doit être levée dès qu'il apparaît que les conditions prévues par le 1 ° ou le 2 ° de l'article L. 224-1 ne sont plus satisfaites, que si elle peut être renouvelée tous les six mois par décisions expresses et motivées, sa durée globale ne peut excéder deux années ; que, conformément aux dispositions du premier alinéa de l'article 24 de la loi du 12 avril 2000 susvisée, chaque renouvellement de l'interdiction ne peut intervenir « qu'après que la personne intéressée a été mise à même de présenter des observations écrites et, le cas échéant, sur sa demande, des observations orales (décision n° 2015-490 QPC, cons. 8).

1.2.2. S'agissant des mesures de sûreté

Les mesures de sûreté, qui restreignent certaines libertés, s'insèrent dans un cadre constitutionnel distinct de celui des peines. Dans sa décision n° 2008-562 DC, le juge constitutionnel est ainsi venu préciser les critères permettant de distinguer ces deux types de mesures, en indiquant que, « *si la mesure prévue à l'article 706-25-15 du code de procédure pénale est prononcée en considération d'une condamnation pénale et succède à*

l'accomplissement de la peine, elle n'est pas décidée lors de la condamnation par la juridiction de jugement mais à l'expiration de la peine, par la juridiction régionale de la rétention de sûreté. Elle repose non sur la culpabilité de la personne condamnée, mais sur sa particulière dangerosité appréciée par la juridiction régionale à la date de sa décision. Elle a pour but d'empêcher et de prévenir la récidive. Ainsi, cette mesure n'est ni une peine ni une sanction ayant le caractère d'une punition ».

➢ *Sur le caractère nécessaire de la mesure :*

Dans sa décision n° 2008-562 DC du 21 février 2008 concernant la loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental, le Conseil constitutionnel a validé le principe d'une rétention de sûreté, dès lors que le dispositif prévu répond à la spécificité de la dangerosité en cause par la liste des infractions pouvant donner lieu à cette rétention et par la nature appropriée des mesures d'évaluation et de prise en charge (décision n° 2008-562 DC).

Cette appréciation a été confirmée dans sa décision n° 2020-805 DC du 7 août 2020 relative à la loi instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine, en considérant que cet objectif justifie qu'un contrôle de la dangerosité supposée des personnes dont l'élargissement est imminent soit organisé par le législateur, eu égard au « *risque particulier de récidive que présente une personne qui persiste à adhérer, à l'issue de sa peine, à une idéologie ou à des thèses incitant à la commission d'actes de terrorisme* ».

De même, le Conseil relève que la rétention de sûreté n'est prévue qu'en ultime recours, au terme d'un examen de l'état de dangerosité de la personne, si aucune autre mesure n'est susceptible d'atteindre le même objectif. Et, en ce qui concerne la mesure de placement sous surveillance électronique mobile, le Conseil constitutionnel relève que « *le risque de récidive doit être constaté par une expertise médicale faisant apparaître la dangerosité du condamné* » (décision n° 2005-527 DC du 8 décembre 2005).

➢ *Sur le caractère adapté de la mesure :*

Le Conseil constitutionnel s'assure que le champ d'application de la mesure est en adéquation avec sa finalité. Par exemple, une mesure de rétention de sureté de personnes sortant de prison et souffrant de trouble grave de la personnalité est adaptée, eu égard à la gravité des crimes (assassinat ou meurtre, torture, actes de barbarie, viol, etc.) pouvant justifier le prononcé d'une telle mesure (décision n° 2008-562 DC). Adéquation d'autant plus retenue par le Conseil que le législateur a prévu des modalités pertinentes d'évaluation de la dangerosité des personnes.

S'agissant d'une mesure de placement sous surveillance électronique mobile ordonné au titre de la surveillance judiciaire, le Conseil en retient le caractère adapté dès lors qu'elle a « *pour objet de prévenir une récidive dont le risque est élevé* » et « *n'a vocation à s'appliquer qu'à des personnes condamnées à une peine privative de liberté d'une durée égale ou supérieure à dix ans, pour certaines infractions strictement définies et caractérisées par leur gravité*

particulière, tels les crimes de viol, d'homicide volontaire ou d'actes de torture ou de barbarie » (décision n° 2005-527 DC).

➢ *Sur le caractère proportionné :*

Le Conseil constitutionnel a estimé qu'un tel dispositif ne pourrait être établi par la loi, afin de prévenir la récidive par des individus encore radicalisés, que si ce dispositif comportait les mêmes garanties suivantes :

- cette rétention de sûreté ne pourrait concerner que les personnes radicalisées condamnées pour un crime constituant un acte de terrorisme et dont la personnalité en fin de peine présenterait encore une grande dangerosité ;
- la rétention de sûreté en matière de terrorisme ne pourrait être ordonnée que si la décision de condamnation a prévu le réexamen, à la fin de sa peine, de la situation de la personne condamnée en vue de l'éventualité d'une telle mesure ;
- des procédures offrant les mêmes garanties que celles prévues par les articles 706-53-13 et suivants du code de procédure pénale devraient être prévues pour vérifier la dangerosité de l'intéressé ;
- la rétention de sûreté ne pourrait être décidée à titre exceptionnel par une juridiction qu'à défaut d'autre mesure efficace moins attentatoire à la liberté individuelle et qu'après que cette juridiction aurait vérifié que la personne condamnée a été mise en mesure de bénéficier pendant l'exécution de sa peine d'une prise en charge adaptée ;
- la mise en place d'un dispositif adapté d'évaluation et de prise en charge de personnes radicalisées condamnées pour acte de terrorisme et dont la personnalité en fin de peine présenterait encore une grande dangerosité, la mesure initiale et ses renouvellements étant soumis à une appréciation juridictionnelle. Dans ce cas, une possibilité de renouvellement illimité n'a pas été jugé disproportionnée, eu égard au réexamen de la dangerosité de la personne lors de chaque renouvellement (décision n° 2008-562 DC, cons. 23).

  En revanche, amené à contrôler, *a priori*, la conformité à la Constitution de la proposition de loi instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine (décision n° 2020-805 DC), le Conseil constitutionnel a en revanche relevé, avant de censurer les dispositions en cause, que les renouvellements de la mesure de sûreté peuvent être décidés aux mêmes conditions que la décision initiale, sans qu'il soit exigé que la dangerosité de la personne soit corroborée par des éléments nouveaux ou complémentaires ;
- enfin, eu égard à sa nature privative de liberté, à la durée de cette privation, à son caractère renouvelable et au fait qu'elle serait prononcée après une condamnation par une juridiction, ne saurait être appliqué à des personnes condamnées avant la publication de la loi qui l'instituerait ou faisant l'objet d'une condamnation postérieure à cette date pour des faits commis antérieurement.

1.3. CADRE CONVENTIONNEL

L'article 5 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales dispose que « Toute personne a droit à la liberté et la sûreté. Nul ne peut être privé de sa liberté, sauf dans les cas suivants et selon les voies légales. »

Pour déterminer si un individu se trouve « privé de sa liberté » au sens de l'article 5, il faut partir de sa situation concrète et prendre en compte un ensemble de critères comme le genre, la durée, les effets et les modalités d'exécution de la mesure considérée (CEDH, *Guzzardi c. Italie*, 6 novembre 1980, § 92).

S'agissant d'un régime de « liberté surveillée » (obligation de présentation à l'autorité de police, permanence du lieu de résidence, interdiction de s'éloigner de la commune, assignation à résidence dans un créneau horaire), la Cour estime qu'elle ne constitue pas une privation de liberté au sens de l'article 5 de la Convention, mais une simple restriction à la liberté de circuler (CEDH 20 avril 2010, *Villa c. Italie*, n° 19675/06).

De même, ne constitue pas une privation de liberté le « placement sous surveillance de la police » et l'« assignation à domicile », mesures préventives impliquant certaines restrictions à la liberté de circulation, ainsi que l'obligation de se plier régulièrement à certaines procédures de contrôle mais n'impliquant aucun confinement des intéressés dans un local délimité, ceux-ci restant en principe libres de se déplacer dans les limites géographiques de leur district (CEDH 9 février 2006, *Freimanis et Lidums c/ Lettonie,* n° 73443/01).

S'agissant de la proportionnalité de mesures faisant obstacle à la liberté d'aller et venir, celles-ci ne se justifient qu'aussi longtemps qu'elles tendent effectivement à la réalisation de l'objectif qu'elles sont censées poursuivre (CEDH 13 novembre 2003, *Napijalo c. Croatie*, n° 66485/01). Fût-elle initialement justifiée, une mesure restreignant la liberté de circulation d'une personne peut devenir disproportionnée et violer les droits de cette personne si elle se prolonge automatiquement pendant longtemps (CEDH 31 octobre 2006, *Földes et Földesné Hajlik c. Hongrie*, n° 41463/02).

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La limite temporelle de douze mois actuellement prévue dans la loi constitue une difficulté importante pour la prise en charge des individus les plus dangereux, dont la radicalisation est identifiée comme relevant du haut du spectre.

Un certain nombre de MICAS arrivent en effet à leur terme et ne peuvent être poursuivies au-delà de douze mois, malgré la persistance avérée de la dangerosité des personnes qui en font l'objet et quelles que soient les circonstances nouvelles qui peuvent se présenter. Au cours de la troisième année d'application de la loi, soit entre le 1er novembre 2019 et le 31 octobre 2020,

15 mesures sont ainsi arrivées à échéance après avoir atteint la durée maximale cumulée des obligations de douze mois, et n'ont donc pu être renouvelées en dépit du niveau de dangerosité des individus en faisant l'objet.

Cette limite temporelle est fortement préjudiciable pour les condamnés TIS, dont certains ont été formés au combat en Syrie, et qui sont placés sous MICAS au terme de plusieurs années d'emprisonnement. Sont concernées, dans la très grande majorité d'entre eux, des personnes présentant un niveau de dangerosité élevée, condamnées soit pour avoir effectué un séjour sur zone avec des éléments étayés de leur engagement terroriste, voire des preuves de leur participation à des exactions, soit pour avoir été impliqué dans un projet d'action violente sur le territoire national, que ce soit dans le projet directement ou dans le soutien logistique.

Pour ce type de profils, qui nécessitent souvent un suivi au long court par les services de renseignement, la limitation temporelle représente un écueil important, dans la mesure où elle ne permet pas toujours de prendre en compte, s'agissant des profils les plus dangereux, les éléments actualisés pouvant survenir après plusieurs mois, voire plusieurs années de suivi, ni d'entraver efficacement une menace s'inscrivant dans le long terme.

La contrainte posée est d'autant plus forte qu'il n'est pas rare que ces profils aient développé des méthodes efficaces de dissimulation au cours de leur détention (notion de « *taqiya* ») et adaptent leur comportement à l'issue de leur élargissement, en se conformant aux obligations et en se tenant éloignés de leur relationnel. La MICAS est intégrée, au même titre que la prison, dans les épreuves auxquelles sont confrontés les militants jihadistes et qu'ils surmontent en faisant preuve de patience. Dans ces conditions, le renouvellement au-delà de six mois de la mesure dont ils font l'objet peut se révéler complexe, faute d'éléments nouveaux et complémentaires pour nourrir le dossier, et ce alors même que la menace présentée par l'individu peut être réelle. Il importe, pour ces profils, de conserver une possibilité de reprendre une mesure d'entrave suffisamment longue lorsque des éléments nouveaux surviennent après plusieurs mois, voire plusieurs années de suivi.

2.2. OBJECTIFS POURSUIVIS

Dans ce contexte, la disposition proposée vise à se doter, pour les sortants de détention condamnés à de lourdes peines pour des faits de terrorisme, d'une capacité d'entrave administrative au-delà d'un an, susceptible d'être activée en cas d'éléments nouveaux ou complémentaires.

L'allongement, pour ces profils considérés comme les plus dangereux, du délai maximum de la MICAS à vingt-quatre mois serait à même de contraindre les individus visés à adapter leur comportement sur le long terme, en permettant de reprendre plus fréquemment la mesure, et ainsi abaisser la menace dont ils sont porteurs. Cette mesure est cohérente avec le suivi exercé par les services sur ce type d'individus, qui s'inscrit nécessairement dans le long terme.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Trois options ont été envisagées :

Option 1 : le juge des libertés et de la détention (JLD) autorise le ministre à renouveler la mesure individuelle de contrôle administratif et de surveillance à chaque nouvelle période de trois mois au-delà d'une durée de douze mois – les décisions sont ensuite prises par le préfet et peuvent donc être contestées devant le juge administratif.

Option 2 : le juge des libertés et de la détention renouvelle lui-même la mesure individuelle de contrôle administratif et de surveillance à chaque nouvelle période de trois mois au-delà de douze mois

Option 3 : le ministre de l'intérieur renouvelle la mesure individuelle de contrôle administratif et de surveillance selon la procédure actuellement en vigueur offrant déjà des garanties exorbitantes du droit commune : notification cinq jours avant l'expiration de la mesure en cours, permettant à la personne concernée de saisir, sous 48h, le juge administratif d'un recours pour excès de pouvoir sur lequel le juge statue en 72h. En cas de saisine du juge selon cette procédure, la décision ne peut s'exécuter qu'après rejet de la requête.

Compte tenu de la rigueur de la mesure, telle que constatée par le Conseil constitutionnel, il était permis de s'interroger sur la nécessité de faire prononcer ou autoriser le renouvellement de la mesure, au-delà d'une période cumulée de douze mois, par le juge des libertés et de la détention.

Cette solution n'a pas été retenue.

En effet, en premier lieu, l'intervention de l'autorité judiciaire n'est pas justifiée constitutionnellement, le Conseil constitutionnel ayant clairement indiqué que la mesure individuelle de contrôle administratif et de surveillance porte atteinte à la liberté d'aller et venir, et non à la liberté individuelle et n'entre donc pas dans le champ de compétence réservée à l'autorité judiciaire par l'article 66 de la Constitution (décision n° 2017-691 QPC du 16 févr. 2018). En outre, il a indiqué que la prolongation de la mesure au-delà de douze mois, s'agissant de l'assignation à résidence prise dans le cadre de l'état d'urgence n'a pas pour effet de transformer l'atteinte à la liberté d'aller et venir en atteinte à la liberté individuelle (décision n° 2017-624 QPC du 16 mars 2017). Enfin, l'autorisation du juge judiciaire ne saurait suppléer l'absence d'éléments nouveaux ou complémentaires, qu'il conviendra dans tous les cas de démontrer.

En deuxième lieu, une telle autorisation du juge judiciaire au-delà d'un an, alors que pendant les douze premiers mois, le contentieux relèvera du juge administratif, pourrait constituer une source de divergence entre les deux ordres de juridiction, le juge judiciaire pouvant être amené à désavouer l'appréciation opérée par le juge administratif ou à statuer sur le bien fondé d'une

demande de renouvellement alors que la légalité d'une mesure antérieure est toujours pendante devant le juge administratif. L'écueil eut été encore plus important dans l'option 1, du fait de la coexistence, d'une décision d'autorisation de renouvellement prononcée par le juge des libertés et de la détention et d'une décision de renouvellement, prononcée ensuite par le ministre, sous le contrôle du juge administratif.

Par ailleurs, des aménagements de procédure ont été introduits au code de justice administrative afin de garantir la sécurité des signataires des décisions en lien avec la prévention d'actes de terrorisme (L. 773-9 : contradictoire asymétrique pour protéger l'identité du signataire de la décision) qu'il faudrait étendre au code de l'organisation judiciaire.

Enfin, subordonner l'action de l'autorité de police à l'autorisation du juge judiciaire, dans un domaine étranger à sa compétence d'attribution, risquerait de constituer un précédent dangereux, en méconnaissance de la règle du privilège du préalable qui veut que les décisions de l'administration soient exécutoires, tant qu'elles n'ont pas été annulées ou suspendues par le juge administratif.

De fait, il a été estimé que le contrôle exercé par le juge administratif était suffisant :

- c'est le juge naturel de l'administration et des mesures de police non privatives de liberté ;
- le code de justice administrative a aménagé la procédure pour tenir compte de la nature des mesures en lien avec la prévention du terrorisme de ce contentieux (aménagement du contradictoire asymétrique ; procédure de renouvellement) ;
- le contrôle du juge est un contrôle de légalité (entier) et non pas seulement du bien fondé de la mesure ; si le requérant n'en fait pas usage avant l'entrée en vigueur de la mesure, il dispose des voies de droit normale après entrée en vigueur de la mesure (référé liberté ou suspension, recours en annulation ou en indemnisation), y compris pour y faire mettre fin à tout moment ;
- le juge administratif s'est organisé pour statuer en 72 h, de sorte que la procédure de renouvellement sous cinq jours est efficace ;
- il n'y a pas de risque de contradiction du fait de l'intervention d'ordres de juridiction successifs selon le moment du renouvellement ;
- La procédure actuellement en vigueur, dès le premier renouvellement, est déjà très dérogatoire au principe du préalable et constitue en l'état un précédent qu'il n'est pas souhaitable d'accentuer.

Au total, le contrôle exercé par le juge administratif est apparu suffisant, étant observé que ce contrôle doit s'exercer, avant tout, sur la pérennité des critères permettant de prononcer des obligations, tels que prévus à l'article L. 228-1 du code de la sécurité intérieure, établie par l'existence, lors de chaque renouvellement, d'éléments nouveaux ou complémentaires.

3.2. DISPOSITIF RETENU

Il est inséré une disposition complémentaire aux articles L. 228-2, L. 228-4 et L. 228-5 du code de la sécurité intérieure, prévoyant que, sous certaines conditions, par dérogation à la durée totale cumulée de douze mois, lorsque la personne concernée a été condamnée à une peine privative de liberté non assortie du sursis ou de trois ans en cas de récidive, pour une infraction à caractère terroriste hors apologie, la durée totale cumulée de ces obligations peut atteindre vingt-quatre mois. Le renouvellement de chaque mesure, d'une durée maximale de trois mois, est subordonné à l'existence d'éléments nouveaux ou complémentaire.

➢ *Sur le caractère nécessaire et adapté :*

Outre les critères habituels de comportement caractérisant une menace d'une particulière gravité pour l'ordre et la sécurité publics et le critère alternatif de soutien, de diffusion ou d'adhésion à des thèses incitant à la commission d'actes de terrorisme d'une part ou de relation habituelle avec des personnes ou organisations incitant, facilitant ou participant à des actes de terrorisme d'autre part, qui devront être démontrés dans tous les cas de figure, et ne peuvent servir à justifier une dérogation à la durée cumulée maximale de douze mois, la possibilité de renouveler les obligations au-delà de cette durée et pour une nouvelle durée cumulée de douze mois, est conditionnée à deux critères cumulatifs tirés des motifs et du quantum de la condamnation :

- la nature de la condamnation : infractions *mentionnées aux articles 421-1 à 421-6 du code pénal, à l'exception de celles prévues aux articles 421-2-5 et 421-2-5-1 (provocation à un acte de terrorisme, apologie du terrorisme ou extraction, reproduction et transmission de données provocant à des actes de terrorisme ou en faisant l'apologie pour entraver une procédure de blocage d'un service de communication au public en ligne).*
- et au quantum de la condamnation, soit une peine privative de liberté non assortie du sursis d'une durée supérieure ou égale à cinq ans ou d'une durée supérieure ou égale à trois ans lorsque l'infraction a été commise en état de récidive légale

Ces deux éléments sont supposés caractériser un risque élevé de dangerosité, résultant d'un passage à l'acte antérieur qui distingue ces personnes de celles à l'égard desquelles il existe seulement des raisons sérieuses de penser que leur comportement constitue une menace pour l'ordre et la sécurité publics.

➢ *En outre, afin d'encadrer les conditions de l'allongement proposé et de garantir qu'il constitue un dispositif ciblé sur la prise en charge des sortants de détention, il est prévu que cet allongement ne puisse être appliqué que lorsque la mesure initiale est prescrite par l'autorité administrative dans les six mois sortants de la détention. Sur la rupture d'égalité :*

Si, classiquement, le principe d'égalité ne s'oppose ni à ce que le législateur règle de façon différente des situations différentes, ni à ce qu'il déroge à l'égalité pour des raisons d'intérêt

général pourvu que, dans l'un et l'autre cas, la différence de traitement qui en résulte soit en rapport direct avec l'objet de la loi qui l'établit (not. décision n° 2007-557 DC), ce principe doit permettre de faire varier l'intensité ou la durée maximale de la mesure au regard des circonstances motivant son prononcé.

Ainsi, le Conseil constitutionnel a déjà admis une telle variation, s'agissant précisément de régimes différents applicables aux sortants de prison, comme la possibilité de placer sous surveillance électronique les personnes condamnées à une peine de prison égale ou supérieure à dix ans pour des faits particulièrement graves (décision du Conseil constitutionnel n° 2005-527 DC du 15 novembre 2007). A contrario, une personne condamnée pour des faits d'une moindre gravité où à l'égard de laquelle n'existe que des soupçons de dangerosité ne pourra pas être concernée par une telle mesure. De même, le législateur peut prévoir qu'une mesure de rétention de sûreté ne pourra s'appliquer qu'aux sortants de prison condamnés pour des faits d'une particulière gravité, cette mesure étant « *réservée aux personnes qui présentent une particulière dangerosité caractérisée par une probabilité très élevée de récidive parce qu'elles souffrent d'un trouble grave de la personnalité* » (décision n° 2008-562 DC).

En l'espèce, s'agissant de la possibilité de prolonger une mesure individuelle de contrôle administratif et de surveillance au-delà d'un an au regard de l'ancrage plus important de la personne dans la radicalisation à caractère terroriste, révélé par un précédent passage à l'acte, et caractérisant une menace plus importante pour l'ordre et la sécurité publics, la distinction opérée en fonction de l'existence ou non d'une condamnation à une peine de prison suffisamment significative (cinq ans ou trois en cas de récidive) pour des faits à caractère terroriste constitue un critère objectif et pertinent permettant de justifier la différence de traitement.

Cette différence de traitement n'est que virtuelle, ces personnes n'ayant que vocation à être placée sous une telle mesure de surveillance au-delà d'une durée cumulée de douze mois et la prolongation de la mesure, pour une durée cumulée de douze mois supplémentaire étant, en tout état de cause, subordonnée à la démonstration, à compter du douzième mois et tous les trois mois ensuite, d'éléments nouveaux ou complémentaires de nature à démontrer la pérennité de la menace d'une part, et à la confirmation de la légalité de cette mesure, avant l'entrée en vigueur de chaque renouvellement, par le juge administratif, saisi dans les conditions prévues aux articles L. 228-2 et L. 228-4 du code de la sécurité intérieure.

- *Sur le caractère proportionné de la mesure :*

Le Conseil constitutionnel a jugé, s'agissant des assignations à résidence de l'état d'urgence, que, au-delà de la durée de douze mois, une telle mesure ne peut être renouvelée que par périodes de trois mois et ne saurait, sans porter une atteinte excessive à la liberté d'aller et de venir, être renouvelée que sous réserve, d'une part, que le comportement de la personne en cause constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics, d'autre part, que l'autorité administrative produise des éléments nouveaux ou complémentaires, et enfin que soient prises en compte dans l'examen de la situation de l'intéressé la durée totale de son

placement sous assignation à résidence, les conditions de celle-ci et les obligations complémentaires dont cette mesure a été assortie (QPC 2017-624).

La prolongation au-delà de 12 mois devrait donc s'accompagner, en tout logique, d'un assouplissement des conditions de surveillance à mesure que celle-ci est renouvelée. Si, en application de ce principe, il pourrait être envisagé de restreindre les obligations pouvant être prononcées au-delà de douze mois, un tel dispositif serait de nature à priver le dispositif de son intérêt opérationnel. En effet, supprimer, lors du renouvellement, l'une des obligations prévues à l'article L. 228-2 du CSI, ferait perdre à la mesure son utilité : de fait, l'interdiction de se déplacer hors d'un périmètre n'a ainsi d'intérêt que si elle est assortie d'une obligation de présentation quotidienne aux services de police et d'une obligation de déclaration de son domicile ou de tout changement de celui-ci.

En réalité, plus que la proportionnalité du dispositif, dont le législateur a déjà prévu qu'il pouvait varier, dans son intensité, au regard de la nécessité de permettre le maintien de la vie privée et familiale, c'est le contrôle du juge sur la nécessité et la proportionnalité des obligations ordonnées, au regard du profil de l'intéressé, qui est de nature à constituer une garantie effective, ce d'autant que, de manière très dérogatoire à la règle du préalable, un tel contrôle est susceptible d'intervenir, si la personne le souhaite, avant l'entrée en vigueur de la décision de renouvellement.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Un alinéa est inséré après le cinquième alinéa de l'article L. 228-2, le cinquième alinéa de l'article L. 228-4 et le deuxième alinéa de l'article L. 228-5 du code de la sécurité intérieure.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Le renouvellement possible de la mesure, de trois mois en trois mois, pendant une année supplémentaire génèrera du travail de renseignement supplémentaire (établir les éléments nouveaux ou complémentaires permettant le renouvellement) et des services du ministère, pour édicter la mesure.

Par ailleurs, la procédure de renouvellement pouvant donner lieu, indépendamment des voies de droit commun, à une procédure contentieuse spécifique dont le résultat conditionne l'entrée en vigueur de la mesure, elle est susceptible de générer du travail contentieux.

4.3. IMPACTS SUR LES PARTICULIERS

Les personnes concernées sont susceptibles de voir leur liberté d'aller et venir contrainte pendant un temps plus long.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATIONS

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 3 (4°) : Sécuriser la procédure juridictionnelle applicable au renouvellement des MICAS

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Le législateur avait initialement prévu que les décisions de renouvellement des mesures individuelles de contrôle administratif et de surveillance (MICAS) prise sur le fondement des articles L. 228-2 et L. 228-5 du code de la sécurité intérieure soit notifiées cinq jours au moins avant leur entrée en vigueur pour permettre à la personne concernée de saisir éventuellement le juge du référé, sur le fondement de l'article L. 521-2 du code de justice administrative, dans un délai de 48h à compter de la notification, le juge des référés disposant alors d'un délai de 72h pour statuer et l'entrée en vigueur étant différée jusqu'à l'intervention de la décision du juge.

Le Conseil constitutionnel a toutefois considéré, dans sa décision n° 2017-691 QPC du 16 février 2018, que l'office du juge fondé sur l'article L. 521-2 du CJA et limité au contrôle des seules atteintes graves et manifestement illégales à une liberté fondamentale était insuffisant et devait au contraire porter sur la régularité et le bien-fondé de la décision de renouvellement.

Afin de concilier un contrôle du juge de l'excès de pouvoir et un délai de jugement compatible avec les exigences de continuité entre la mesure initiale et son renouvellement, le législateur a, dans la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice (article 65) modifié les articles L. 228-2 et L. 228-5 du CSI en maintenant les mêmes délais (notification cinq jours avant l'entrée en vigueur du renouvellement, délai de recours de 48h et délai de jugement de 72h) en prévoyant toutefois que le juge statuait sur la légalité de la mesure, moyennant des aménagements de procédure (délai de recours de 48h, délai de jugement de 72h et dispense de rapporteur public).

Le décret n° 2019-1495 du 27 décembre 2019 portant application de l'article L. 773-10 du code de la justice administrative a tiré les conséquences de ces aménagements de procédure.

Toutefois, lorsque la personne concernée a saisi un tribunal territorialement incompétent, le délai de renvoi au bon tribunal risque de faire échec à l'intervention d'une décision dans le délai de 72 h, empêchant ainsi l'entrée en vigueur de la décision de renouvellement alors que la décision en cours arrivera à expiration.

Dans le but d'éviter toute rupture dans la surveillance d'une personne, il est donc nécessaire de prévoir qu'en cas de saisine d'une juridiction territorialement incompétente, le délai de 72 h ne court qu'à compter de l'enregistrement par le tribunal territorialement compétent auquel est renvoyée la requête, la mesure en cours étant prorogée, par voie de conséquence, pendant ce délai.

1.2. CADRE CONSTITUTIONNEL

Statuant sur un dispositif légal instaurant des mesures de police administrative, le Conseil constitutionnel veille particulièrement à ce que les conditions mises à leur prolongation ou leur renouvellement soient précisément définies.

Ainsi, s'agissant des périmètres de protection instaurés sur le fondement des dispositions de l'article L. 226-1 du code de la sécurité intérieure, le Conseil constitutionnel a émis une réserve d'interprétation tenant à ce que le renouvellement de ces mesures est subordonné à la démonstration de la persistance du risque (CC 29 mars 2018, n° 2017-695 QPC).

S'agissant de l'interdiction de sortie du territoire (CC 14 oct. 2015, n° 2015-490 QPC) et des mesures individuelles de contrôle administratif et de surveillance (CC 19 février 2018, n° 2017-691 QPC), le Conseil constitutionnel a porté la même attention particulière à ce que les conditions mises au renouvellement de ces mesures soient précisément définies par la loi.

Il convient donc de déterminer avec le plus de précision possible et en usant de critères objectifs, les conditions mises à la prolongation d'une telle mesure, prise dans un objectif de prévention des atteintes à l'ordre public.

1.3. CADRE CONVENTIONNEL

L'article 6 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, relatif au droit à un procès équitable, garantit un « droit d'accès au juge », un droit à ce que la cause de chacun soit entendue (not. CEDH 21 février 1975, Royaume-Uni, n° 4451/70).

Ce droit d'accès à un tribunal n'est pas absolu, et les Etats bénéficient d'une certaine marge d'appréciation pour l'encadrer (not. CEDH 23 octobre 1996, *Levage Prestations Services c. France*, n° 21920/93). Ces limitations doivent poursuivre un but légitime et les restrictions apportées doivent être proportionnées au but visé (CEDH 13 juill. 1995, *Tolstoy Miloslavsky c/ Royaume-Uni,* nº 18139/91).

Toutefois, s'il ne saurait être portée atteinte à la substance même du droit au recours, il y a lieu de concilier cet impératif avec l'objectif légitime de ne pas faire obstacle à l'exécution de mesures de police tendant à prévenir les atteintes à l'ordre public.

Si, comme en l'espèce, le bien-fondé de la mesure de police (et partant, sa prolongation) doit être appréciée au regard de la liberté conventionnelle d'aller et venir, il convient dès lors que cette atteinte constituée par la prolongation soit précisément encadrée par le législateur et poursuivre un objectif légitime.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

En cas de saisine d'une juridiction territorialement incompétente lors du recours spécifique prévu aux articles L. 228-2 et L. 228-5 du CSI, le renvoi de la requête à la juridiction compétente, avec nouveau délai de 72 heures, risque d'aboutir à une décision après expiration de la précédente.

2.2. OBJECTIFS POURSUIVIS

Cette disposition vise à éviter que la saisine d'un tribunal incompétent, par méconnaissance de la règle ou à dessein, dans un but dilatoire, aboutisse au prononcé d'une décision juridictionnelle après expiration de la précédente mesure, occasionnant ainsi une rupture dans la surveillance de la personne concernée puisque la mesure prend fin à l'issue du délai de cinq jours alors que la nouvelle mesure peut, du fait du renvoi nécessaire à la juridiction compétente, ne pas être encore entrée en vigueur, le recours étant suspensif.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Option n° 1 : prévoir que nonobstant son incompétence territoriale, le tribunal incompétemment saisi statue sur la demande. Cette solution, qui aurait le mérite de ne pas retarder la décision juridictionnelle et d'éviter une rupture dans la surveillance des personnes placées sous MICAS, aboutirait toutefois à distordre les règles normales de compétence au profit d'une logique opérationnelle, tout en réduisant l'accès au juge pour le requérant, alors que l'aménagement de compétence résultant de l'article R. 312-8 du CJA vise précisément à permettre que le juge territorialement compétent soit déterminé par le domicile du requérant, pour en faciliter son accès.

Option n° 2 : prévoir que le délai de jugement de 72h court à compter de son enregistrement par le tribunal auquel la requête a été renvoyée. La mesure en cours demeure alors en vigueur jusqu'à ce qu'il ait été statué sur sa légalité.

3.2. DISPOSITIF RETENU

Il est proposé qu'en cas de saisine d'un tribunal territorialement incompétent lors du recours spécifique prévu aux articles L. 228-2, L. 228-4 et L. 228-5 du CSI à l'encontre de la décision de renouvellement, le délai de jugement de 72 heures court à compter de son enregistrement

par le tribunal auquel la requête a été renvoyée et que la mesure en cours demeure alors en vigueur jusqu'à ce qu'il ait été statué sur sa légalité.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Après le sixième alinéa de l'article L. 228-2, le sixième alinéa de l'article L. 228-4 et le troisième alinéa de l'article L. 228-5 du code de la sécurité intérieure.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La modification proposée permettra de garantir aux services une surveillance, sans rupture, de l'individu faisant l'objet de la mesure individuelle de contrôle administratif et de surveillance.

4.3. IMPACTS SUR LES PARTICULIERS

En cas de saisine d'une juridiction territorialement incompétente, la mesure en cours de validité pourra être prolongée le temps que la juridiction compétente se prononce sur la décision de renouvellement, et, en tout état de cause, pour une durée qui ne pourra excéder 72 heures.

La garantie d'intervention d'un juge avant l'entrée en vigueur de la décision de renouvellement est maintenue.

Cette disposition fait donc échec aux manœuvres dilatoires consistant à saisir un tribunal territorialement incompétent afin d'empêcher l'intervention d'une décision juridictionnelle avant l'expiration de la précédente.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATIONS

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 3 (5°) : Prendre en compte les obligations déjà prescrites par l'autorité judiciaire lors de la définition des obligations imposées dans le cadre d'une MICAS

1. ETAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 228-1 du code de la sécurité intérieure prévoit la possibilité pour le ministre de l'intérieur d'enjoindre un certain nombres d'obligations à une personne à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes. Ces obligations, qui ne peuvent être prononcées qu'aux seules fins de prévenir la commission d'actes de terrorisme, sont prévues aux articles L. 228-2 à L. 228-5 du même code.

Ces mesures individuelles de contrôle administratif et de surveillance ont été, au cours des deux dernières années, majoritairement prononcées à l'encontre de personnes sortant de détention. Un dispositif d'anticipation et de prise en compte, par les services, des sorties de ces individus a été mis en place et permet de définir les modalités de suivi des personnes dont la libération est proche. La MICAS alors est conçue comme une mesure de police administrative permettant de surveiller l'individu sortant de prison, lorsqu'en détention, il a manifesté la pérennité de son engagement radical.

Aussi n'est-il pas rare que ces mesures se conjuguent, une MICAS pouvant coexister avec une mesure de contrôle judiciaire ou de suivi post peine. Il n'existe en effet, aucun obstacle de principe à ce qu'une personne placée sous contrôle judiciaire ou faisant l'objet d'un suivi post-peine fasse également l'objet d'une mesure de contrôle administratif et de surveillance, dès lors que chacune des deux mesures répond à un objectif propre. Ainsi, le contrôle judiciaire vise à s'assurer de la présence de la personne qui en fait l'objet lors de son procès pénal tout en protégeant les victimes et en préservant le bon déroulement de l'enquête, tandis que le suivi post-peine vise à favoriser la réinsertion de l'individu sortant de prison et que la mesure individuelle de contrôle administratif et de surveillance vise à prévenir la commission d'acte en lien avec le terrorisme.

C'est la raison pour laquelle, préalablement au prononcé d'une obligation sur le fondement des articles L. 228-2, L. 228-4 et L. 228-5 du CSI, le ministre de l'intérieur informe le procureur de la République territorialement compétent et le parquet national antiterroriste (PNAT), compétent en matière de terrorisme, cette information permettant à l'autorité judiciaire de s'assurer que cette mesure ne risque pas de compromettre une enquête en cours, que les

obligations qui en découlent n'entrent pas en contradiction avec des mesures de suivi judiciaire ou, dans cette hypothèse, de les contracter lorsqu'elles ont les mêmes effets.

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel a rappelé que les mesures de surveillance administrative des personnes à l'égard desquelles il existe des indices de dangerosité constituent des mesures de police administrative, au regard de leur finalité visant **à** préserver l'ordre public (décision n° 2015-527 QPC du 22 décembre 2015 relative à l'assignation à résidence sous l'état d'urgence) ou à prévenir la commission d'actes de terrorismes (décision n° 2015-691 QPC).

Dans ses décisions 2017-691 QPC et 2017-695 QPC, portant sur la mesure administrative d'assignation à résidence aux fins de lutte contre le terrorisme instaurée par les dispositions de l'article L.228-1 et suivants du code de la sécurité intérieure, le Conseil constitutionnel a constaté que cette mesure de police administrative était **nécessaire** en ce que le législateur a poursuivi l'objectif de lutte contre le terrorisme, qui participe de l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public, que les conditions de recours à cette mesure sont précises et son champ d'application limité à des personnes soupçonnées de présenter une menace d'une particulière gravité pour l'ordre public.

Par ailleurs, il a considéré qu'une telle mesure était **proportionnée** et n'excédait pas la rigueur nécessaire, le périmètre géographique de l'assignation à résidence ne pouvant être inférieur au territoire de la commune et devant permettre à l'intéressé de poursuivre une vie familiale et professionnelle, l'obligation de présentation périodique aux services de police ou aux unités de gendarmerie ne pouvant excéder une présentation par jour, la durée de la mesure ne pouvant excéder trois mois, son renouvellement au-delà d'une durée cumulée de six mois étant subordonné à la production par le ministre de l'intérieur d'éléments nouveaux ou complémentaires.

Cette rigueur nécessaire doit toutefois être appréciée au regard de l'ensemble des autres mesures dont peut faire l'objet la personne concernée, d'effet équivalent, quand bien même poursuivraient-elles des finalités différentes.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Si le Conseil d'État a pu admettre (CE 1er déc. 2017, n° 415740) le caractère adapté et proportionné d'une mesure de contrôle administratif et de surveillance nonobstant son cumul avec des mesures prescrites par l'autorité judiciaire, c'est à la condition que ces obligations, lorsqu'elles ont un effet similaire, se contractent avec les obligations du contrôle judiciaire de l'intéressé.

Une telle solution avait déjà été retenue s'agissant des mesures d'assignation à résidence prise sous le régime de l'état d'urgence, dont, là encore, les obligations se confondaient avec celle du contrôle judiciaire de l'intéressé (CE 25 avr. 2017, n° 409677 pour un cumul entre les obligations de présentation à l'autorité de police découlant d'une assignation à résidence d'une part et d'un contrôle judiciaire d'autre part).

Ce précédent ne règle toutefois pas l'hypothèse dans laquelle les obligations imposées, d'une part, par l'autorité de police administrative et, d'autre part, par l'autorité judiciaire, se cumuleraient de telle sorte que, mises bout à bout, elles revêtiraient un caractère disproportionné, empêchant, par exemple, l'intéressé de mener une vie professionnelle ou familiale normale.

Une telle hypothèse s'est ainsi présentée, s'agissant d'une mesure d'assignation à résidence prise sur le fondement de l'état d'urgence (CE 12 sept. 2016, n° 403256), conduisant le Conseil d'Etat à examiner si, en l'espèce, l'autorité administrative avait, pour apprécier le caractère proportionné de sa mesure, examiné si celle-ci était conciliable avec celles prescrites par l'autorité judiciaire, relevant en l'espèce que, si l'obligation de pointage résultant du contrôle judiciaire ne peut à elle seule suffire à remplir l'objectif que vise l'obligation quotidienne posée par l'arrêté d'assignation à résidence, en revanche, « *les obligations résultant de son assignation à résidence permettent de remplir également celles résultant de son contrôle judiciaire* ».

2.2. OBJECTIFS POURSUIVIS

Au final, s'est instaurée, dans la plupart des cas, une véritable complémentarité entre les mesures prises au titre du contrôle judiciaire et celles prises au titre de la surveillance administrative, les obligations étant contractées lorsqu'elles sont identiques.

Plusieurs interventions de l'autorité judiciaire ont permis de signaler des difficultés résultant d'incompatibilités entre ces deux régimes (suivi socio-judiciaire dans un lieu distinct du périmètre d'assignation ou horaires incompatibles, impossibilité d'occuper un emploi pourtant imposé dans ce cadre). A chaque fois, les modalités de la surveillance administrative ont été aménagées. Il est néanmoins nécessaire que les diverses obligations qui découlent de ces deux régimes soient à la fois conciliables et, lorsqu'elles sont identiques, contractées, de sorte que la contrainte qui en découle ne présente pas un caractère disproportionné au regard de l'obligation de tenir compte de la vie privée, familiale et professionnelle (cf. TA Toulouse, 7 novembre 2017, n° 1705075 : *« Considérant qu'il résulte de l'instruction que les obligations de son contrôle judiciaire se confondent avec l'obligation de présentation quotidienne prévue par la mesure individuelle de contrôle administratif et de surveillance ; dès lors que, par une ordonnance de modification du contrôle judiciaire en date du 18 janvier 2016, le magistrat instructeur du tribunal de grande instance de Paris s'est borné à imposer à l'intéressé de se présenter au commissariat de police de Toulouse deux fois par semaine, le mardi et le vendredi, sans précision d'horaire ; que ladite obligation de présentation quotidienne, une fois par jour, ne présente pas un caractère excessif, compte tenu de la menace pour la sécurité et l'ordre*

publics constituée par le comportement de M. X ; qu'eu égard à l'ensemble de ces éléments, il n'apparaît pas, en l'état de l'instruction, que les modalités de contrôle administratif et de surveillance de l'intéressé revêtiraient un caractère disproportionné. »).

L'exigence de proportionnalité, figurant déjà à l'article L. 228-6 du code de la sécurité intérieure s'agissant des MICAS, doit donc être renforcée dans le projet de loi, pour confirmer d'une part, que les obligations administratives et judiciaires peuvent être cumulées et d'autre part, que les obligations prescrites au titre des MICAS prennent en compte et s'adaptent à celles prescrites par l'autorité judiciaire.

3. OPTION ENVISAGEE ET DISPOSITIF RETENU

3.1. OPTION ENVISAGEE

La disposition peut apparaître superflue dans la mesure où l'actuel article L. 228-6 du CSI prévoit déjà le principe de nécessité et de proportionnalité des obligations prononcées au titre des MICAS, ce qui sous entend la nécessité de prendre en compte les diverses obligations imposées par ailleurs et notamment par l'autorité judiciaire, à la personne concernée.

3.2. DISPOSITIF RETENU

Il est néanmoins apparu nécessaire d'affirmer explicitement cette nécessité, ce qui permet, par voie de conséquence, de lever l'ambiguïté sur la possibilité de cumuler les obligations découlant des MICAS avec celles prescrites par l'autorité judiciaire, au titre du contrôle judiciaire, de suivi post peine, du suivi socio judiciaire ou des mesures de sureté.

Est donc inséré, à l'article L. 228-6 du code de la sécurité intérieure une disposition selon laquelle la définition des obligations prononcées sur le fondement des articles L. 228-2 à L. 228-5 du même code tient compte, dans le respect des principes de nécessité et de proportionnalité, des obligations déjà prescrites par l'autorité judiciaire lorsqu'elles sont de même nature ou poursuivent le même objectif.

Ainsi, par exemple, une personne condamnée pour une infraction à caractère terroriste sera *ipso facto* inscrite au fichier des auteurs d'infractions terroristes (FIJAIT), avec pour obligation de se présenter tous les trois mois aux autorités, de justifier leur adresse et de prévenir avant tout déplacement transfrontalier. De telles obligations pouvant se superposer avec celles pouvant être prononcées au titre des mesures individuelles de contrôle administratif et de surveillance, celles-ci seront alors contractées.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Une phrase est insérée de l'article L. 228-6 du code de la sécurité intérieure.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services du ministère de l'intérieur devront prendre en compte les obligations déjà prononcés par les autorités judiciaires lors de l'édiction de la mesure, la loi imposant d'ores et déjà à cette fin d'informer l'autorité judiciaire (PNAT et procureur de la République du lieu d'habitation de la personne) de la nature des obligations envisagées au titre de la MICAS, pour précisément permettre de les concilier avec celles prononcées par l'autorité judiciaire.

4.3. IMPACTS SUR LES PARTICULIERS

La disposition permettra une meilleure coordination des mesures.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATIONS

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 3 (6°) : Prolonger la validité des MICAS en cours à la date de promulgation de la présente loi pour permettre leur éventuel renouvellement selon la procédure prévue aux articles L. 228-2, L 228-4 et L. 228-5 du code de la sécurité intérieure

1. ETAT DES LIEUX

Les article L. 228-2, L. 228-4 et L. 228-5 du code de la sécurité intérieure subordonnent le renouvellement des mesures individuelles de contrôle administratif et de surveillance (MICAS) à une procédure d'entrée en vigueur différée, ce renouvellement devant intervenir au moins cinq jours avant l'expiration de la mesure en cours. La personne concernée dispose alors d'un délai de 48 h pour contester cette mesure devant le juge administratif, lequel dispose à son tour d'un délai de 72 h pour statuer sur sa légalité. Ce recours est suspensif, la nouvelle mesure ne pouvant entrer en vigueur avant que le juge en ait confirmé la légalité.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. Necessite de legiferer

La loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (dite loi « SILT ») avait autorisé la mise en œuvre des mesures prévues à ses articles 1er à 4, dont les MICAS (article 3) jusqu'au 31 octobre 2020, ce délai ayant ensuite été prolongé jusqu'au 31 juillet 2021, par la loi n° 2020-1671 du 24 décembre 2020 relative à la prolongation des chapitres VI à X du titre II de livre II du code de la sécurité intérieure et de l'article L. 851-3 du code de la sécurité intérieure.

Par suite, l'ensemble des mesures actuellement prononcées ne peuvent l'être que jusqu'au 31 juillet 2021 et ne pourront être renouvelées que pour autant que ces mesures auront été pérennisées par l'actuel projet de loi, comme le prévoit son article 1er.

Compte tenu du calendrier parlementaire très resserré qui ne permet pas d'envisager, dans tous les cas, une promulgation de la loi avant le délai de caducité de l'actuelle loi SILT, et compte tenu du délai incompressible de cinq jours exigé pour renouvellement les mesures qui viendront automatiquement à expiration le 31 juillet prochain, il est nécessaire de prévoir que les mesures en cours demeurent en vigueur pendant une durée de sept jours, pour permettre de les renouveler tout en respectant la procédure spécifique présidant à ce renouvellement.

2.2. Objectifs poursuivis

L'objectif poursuivi est d'éviter que le délai d'au moins cinq jours entre l'entrée en vigueur de la loi et l'entrée en vigueur du renouvellement des mesures qui seront venues à expiration, soit

mis à profit par les personnes surveillées pour se soustraire durablement au contrôle des services de renseignement.

3. DISPOSITIF RETENU

Le 6° de l'article 3 prévoit que les mesures prononcées sur le fondement des articles L. 228-1 et suivants du code de la sécurité intérieure en cours à la date de promulgation de la présente loi et dont le terme survient moins de sept jours après cette promulgation demeurent en vigueur sept jours à compter de ce terme, si le ministre de l'intérieur a procédé au plus tard au lendemain de la publication de la présente loi, à la notification de leur renouvellement selon la procédure prévue aux huitième et neuvième alinéas de l'article L. 228-2, aux septième et huitième alinéas de l'article L. 228-4 et aux 4ème et 5ème alinéas de l'article L. 228-5.

Si la durée de sept jours retenue par cette disposition excède la durée de cinq jours normalement prévue par les articles précités, cette durée tient compte de la nécessité de procéder au renouvellement des nombreuses décisions qui seront en cours à la date d'entrée en vigueur de la nouvelle loi, lesquelles sont ensuite susceptibles d'être déférées au juge qui pourra être amené, dans ces circonstances particulières et s'il est saisi de très nombreux recours concomitants, à excéder le délai de 72 h qui lui est normalement imparti par la loi.

En tout état de cause, la prolongation de la durée des MICAS en cours au 31 juillet 2021 ne saurait avoir d'effet sur leur durée totale cumulée, qui, dans tous les cas, ne pourra excéder un an. En outre, ce renouvellement ne pourra être prononcé que si les conditions ayant présidé au prononcé de la précédente mesure sont encore réunies, sans préjudice de la nécessité de démontrer l'existence d'éléments nouveaux ou complémentaires, si ce renouvellement devait aboutir à porter la durée de la mesure à plus de six mois.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Cette disposition transitoire n'a pas vocation à être codifiée.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services du ministère de l'intérieur devront renouveler l'ensemble des mesures en cours et venant à expiration le 31 juillet 2021, sauf à ce que ces mesures ne soient plus nécessaires.

4.3. IMPACTS SUR LES PARTICULIERS

Le projet de loi organisant un continuum avec les mesures de la loi SILT, ces mesures n'auront aucun impact sur les particuliers, dès lors qu'elles doivent en tout état de cause s'inscrire dans les conditions d'édiction de la mesure et dans une durée totale cumulée d'un an.

5. MODALITES D'APPLICATION

5.1. APPLICATION DANS LE TEMPS

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2. APPLICATION DANS L'ESPACE

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 4 : Permettre la saisie d'un support informatique présent sur les lieux de la visite domiciliaire lorsque la personne fait obstacle à l'accès aux données informatiques qu'il contient

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Aux termes de l'article L. 229-5 du code de la sécurité intérieure, « *Aux seules fins de prévenir la commission d'actes de terrorisme, si la visite révèle l'existence de documents ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée, il peut être procédé à leur saisie ainsi qu'à celle des données contenues dans tout système informatique ou équipement terminal présent sur les lieux de la visite soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la visite* ».

La copie des données ou la saisie des supports informatiques qui les contiennent ne sont possibles que pour autant que la visite a mis en évidence un lien avec la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée : il peut s'agir de documents ou données accessibles lors de la visite, en lien avec la menace, mais ne pouvant, eu égard à leur nombre, être exploités sur place et devant être copiées à cette fin. Il peut également s'agir de données non accessibles dans un terminal informatique (ordinateur ou téléphone) qui doit être par suite, saisi, alors que d'autres documents présents sur place (ouvrage, affiches…) corroborent cette menace.

Il ne peut être procédé à l'exploitation des données ou documents saisis lors de la visite qu'après une nouvelle autorisation du juge des libertés et de la détention, qui doit statuer dans un délai maximum de 48 heures à compter de sa saisine. L'autorisation d'exploitation ne peut porter, conformément au II de l'article L. 229-5 du code de la sécurité intérieure, sur des éléments dépourvus de tout lien avec la finalité de prévention de la commission d'actes de terrorisme.

1.2. CADRE CONSTITUTIONNEL

Ces dispositions s'inspirent fortement de dispositions comparables relatives aux saisies effectuées par les services fiscaux et les services douaniers, dans le cadre des perquisitions qu'ils sont autorisés à effectuer des visites domiciliaires sous le contrôle de l'autorité judiciaire (respectivement art. L. 16 B et L. 38 du LPF et 64 du code des douanes).

Les garanties que pour les saisies déjà autorisées par la loi SILT (saisies des données relatives à la menace que constitue le comportement de la personne concernée ou dont la copie n'a pu être achevée pendant le temps de la visite) sont les suivantes :

- la saisie est opérée en présence d'un officier de police judiciaire avec mention sur le procès-verbal des motifs l'ayant rendue nécessaire et de l'inventaire de ce qui est saisi ;
- l'accès aux données saisies par les agents de police administrative n'est possible qu'après autorisation du JLD, qui statue sous 48h et dont les décisions sont susceptibles d'appel ;
- les supports informatiques saisis doivent être restitués dans les quinze jours et les copies des données y figurant détruites dans les trois mois (le JLD pouvant néanmoins autoriser un renouvellement de ces délais en cas de difficulté pour y accéder ou pour exploiter lesdites données.

Il convient de rappeler que dans sa décision n° 2017-695 QPC du 29 mars 2018, le Conseil constitutionnel a validé dans son ensemble le régime des visites domiciliaires et des saisies mais a conclu que la procédure de saisie des documents et des objets méconnaissait le droit de propriété et devait être déclarée contraire à la Constitution, avec effet immédiat. Les garanties ont en revanche été jugées suffisantes s'agissant des hypothèses de saisies de données contenues dans les supports de données informatiques (CC, 29 mars 2018, n° 2017-695, pts 58-70).

La disposition a donc été modifiée dans le cadre de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice pour étendre les garanties entourant la saisie des données à celle des documents.

Ces garanties sont par ailleurs comparables à celles qui sont prévues pour les saisies effectuées par les services fiscaux et douaniers dans la même hypothèse où la personne concernée ferait obstacle à l'accès à ses supports informatiques, au sujet desquelles la cour d'appel de Versailles a refusé de renvoyer une QPC (CA Versailles, 7 mai 2015, n° 15/00002).

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Dans certains cas, les données contenues dans les supports informatiques ne sont pas directement accessibles, étant protégées par un mot de passe, dont il arrive que l'intéressé refuse de le communiquer, empêchant ainsi l'autorité administrative d'établir leur lien avec la menace alléguée, et donc de procéder à leur saisie.

2.2. OBJECTIFS POURSUIVIS

La disposition permet donc de dépasser l'impossibilité de saisie des données résultant du refus des personnes de donner l'accès aux données contenues dans le support informatique, notamment en communiquant le mot de passe, en créant un autre cas de saisie des supports informatiques, après constat de ce refus mentionné au procès-verbal.

3. DISPOSITIF RETENU

Il est proposé que lorsque les personnes, faisant l'objet d'une visite visant à révéler l'existence de documents ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée, font obstacle à l'accès aux données contenues dans tout système informatique ou équipement terminal présent sur les lieux de la visite, mention en est faite au procès-verbal avant de procéder à la saisie de ces supports.

Par leur insertion dans l'article L. 229-5 du CSI, ces nouvelles dispositions sont encadrées par les mêmes garanties que celles existant pour les saisies déjà autorisées par la loi SILT

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. Impacts juridiques

Il est inséré un alinéa après le premier alinéa du I de l'article L. 229-5 du code de la sécurité intérieure.

4.2. Impacts sur les services administratifs

Les opérations de saisie de données informatiques lors de visites domiciliaires seront facilitées pour les services du ministère de l'intérieur, qui pourront alors dépasser le refus de la personne concernée de permettre l'accès aux matériels informatiques.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. Consultations menees

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. Modalites d'application

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 5 : Création d'une mesure judiciaire de prévention de la récidive terroriste et de réinsertion

1. ETAT DES LIEUX

1.1. ETAT DES LIEUX

D'ici la fin de l'année 2023, plus d'une centaine actuellement détenues pour actes de terrorisme en lien avec la mouvance islamiste (TIS) devraient sortir de détention à l'issue de leur peine.

Certaines d'entre elles présentent des signes de radicalisation importants. Leur personnalité à la fin de leur peine révèle encore une grande dangerosité caractérisant une probabilité très élevée de récidive, qui nécessite le prononcé de mesures de contrôle adaptées.

Sur le plan judiciaire, ces personnes peuvent faire l'objet :

- D'un suivi socio-judiciaire prévu par les articles 131-36-1 et suivants du code pénal, qui constitue une peine complémentaire permettant de soumettre les personnes condamnées pour des infractions graves, à l'issue de leur incarcération, à des mesures de surveillance et d'assistance destinées à prévenir la récidive (notamment, lorsque certaines conditions sont réunies, un placement sous surveillance électronique mobile ou une assignation à domicile). Une telle peine peut être prononcée pour une durée de 10 ans, ou 20 ans par décision spécialement motivée, pour un délit, pour une durée de 20 à 30 ans pour les crimes, et sans limitation de durée pour les crimes punis de la réclusion criminelle à perpétuité.

  Néanmoins, la peine de suivi socio-judiciaire n'a été étendue à l'ensemble des infractions terroristes, et notamment à l'association de malfaiteurs terroriste, que par 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. Cette peine ne peut donc être appliquée qu'aux personnes condamnées pour des faits commis postérieurement à l'entrée en vigueur de cette loi et n'a donc pas pu être prononcée pour les personnes qui vont être prochainement libérées.

- D'une mesure de surveillance judiciaire prévue par les articles 723-29 et suivants du code de procédure pénale, qui permet de soumettre, après sa libération, un condamné considéré comme dangereux à des obligations déterminées (notamment le placement sous surveillance électronique mobile et, dans certaines conditions, l'assignation à domicile), aux seules fins de prévenir une récidive dont le risque paraît avéré. Cette mesure est prononcée par le tribunal de l'application des peines à l'issue de l'incarcération de personnes condamnées à une peine privative de liberté supérieure ou égale à sept ans ou cinq ans en cas de récidive. Lorsque les conditions tenant au quantum de la peine prononcée ne sont pas remplies, les personnes condamnées peuvent faire

l'objet d'un suivi post-libération prévu par l'article 721-2 du code de procédure pénale, qui permet d'imposer des mesures de contrôle destinées à favoriser leur réinsertion.

Toutefois, cette mesure ne survit pas à la fin de la peine et ne peut être prononcée que pour la durée des réductions de peine éventuellement octroyées.

- D'un suivi post libération prévu par l'article 721-2 du code de procédure pénale, lorsque les conditions de la surveillance judiciaire tenant au quantum de la peine prononcée ne sont pas remplies. Cette mesure permet d'imposer à la personne condamnée, à sa libération, des mesures de contrôle destinées à favoriser sa réinsertion (notamment établir sa résidence en un lieu déterminé et ne pas détenir des armes).

  Cette mesure ne survit pas non plus à la fin de la peine et ne peut être prononcée que pour la durée des réductions de peine éventuellement octroyées.

- D'un enregistrement au Fichier national automatisé des auteurs d'infractions terroristes (FIJAIT) en application des articles 706-25-3 et suivants du code de procédure pénale, qui emporte notamment l'obligation pour les personnes condamnées pour un acte de terrorisme de justifier pendant dix ans de leur adresse tous les trois mois et de déclarer tout déplacement transfrontalier au moins quinze jours avant celui-ci.

- A l'issue de leur peine, d'une rétention de sûreté prévue par les articles 706-53-13 et suivants du code de procédure pénale, qui consiste dans le placement, à la fin de l'exécution de la peine, d'une personne condamnée dans un centre socio-médico-judiciaire de sûreté dans lequel lui est proposée, de façon permanente, une prise en charge médicale, sociale et psychologique.

  Cette mesure ne peut être prononcée qu'à l'égard des personnes condamnées à une peine de réclusion criminelle d'au moins 15 ans pour les actes de terrorisme les plus graves, notamment les crimes d'assassinat ou de meurtre aggravé commis dans un but terroriste, dès lors qu'elles présentent notamment un trouble grave de la personnalité. Elle n'est par conséquent pas applicable pour l'ensemble des actes de terrorisme : sont en particulier exclues de ce dispositif les personnes condamnées pour les infractions d'association de malfaiteurs terroriste qui vont être prochainement libérés. En outre, elle n'apparaît pas forcément la plus adaptée pour l'ensemble des profils des terroristes qui ne présentent pas tous des troubles graves de la personnalité.

- A l'issue de leur peine, d'une surveillance de sûreté prévue par l'article 723-37 du code de procédure pénale, qui permet de prolonger à l'issue de la peine pour deux ans renouvelables tant que perdure la dangerosité, les obligations de la surveillance judiciaire, du suivi socio-judiciaire ou de la libération conditionnelle avec injonction de soins, en imposant notamment le placement de la personne concernée sous surveillance électronique mobile. La surveillance de sûreté est soumise aux mêmes conditions que la rétention de sûreté, s'agissant des crimes commis, de la peine prononcée et de l'existence d'un trouble grave de la personnalité.

Sur le plan administratif, ces personnes peuvent être soumises à des mesures individuelles de contrôle administratif et de surveillance (MICAS) prévues par les articles L. 228-1 et suivants du code de la sécurité intérieure. Ces mesures permettent, aux seules fins de prévenir la commission d'actes de terrorisme, d'imposer aux personnes pour lesquelles il existe des raisons sérieuses de penser que leur comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics des interdictions de se déplacer à l'extérieur d'un périmètre déterminé ainsi que des obligations de pointage ou, le cas échéant, de placement sous surveillance électronique. Ces mesures peuvent être prononcées pour une durée totale cumulée de douze mois (décisions n° 2017-691 du 16 février 2018 et n° 2017-695 QPC du 29 mars 2018).

1.2. CADRE CONVENTIONNEL

Les mesures de sûreté ne se heurtent, par principe, à un obstacle conventionnel (Gardel c. France, n° 16428/05, CEDH, 17 décembre 2009).

La Cour européenne des droits de l'homme considère que la notion de « peine » prévue par l'article 7 de la Convention européenne des droits de l'homme revêt une portée autonome. Elle rappelle qu'elle demeure libre d'aller au-delà des apparences et apprécie elle-même si une mesure particulière s'analyse au fond en une « peine » au sens de cette clause, ou en une mesure de sûreté.

A cet égard, la CEDH apprécie les mesures selon leur nature, leur but, leur qualification en droit interne, les procédures associées à leur adoption et à leur exécution et leur gravité (CEDH, 9 févr. 1995, *Welch c/ Royaume-Uni*, n° 17440/90, § 28).

Si la qualification de mesure de sûreté doit être retenue, la CEDH rappelle que celle-ci constitue une mesure préventive et non punitive pour laquelle il ne peut être fait application du principe de non-rétroactivité énoncé par l'article 7 § 1 la de Convention européenne des droits de l'homme (CEDH, 3 septembre 2015, Berland c. France, n° 42975/10).

Ainsi, dans son arrêt Berland c. France précité, la Cour a considéré que la déclaration d'irresponsabilité pénale et les mesures de sureté qui l'accompagnaient[13] ne constituaient pas une « peine » au sens de l'article 7 § 1 de la Convention, et qu'elles devaient être analysées comme des mesures préventives auxquelles le principe de non rétroactivité n'a pas vocation à s'appliquer.

En revanche, la Cour a jugé que la détention de sûreté allemande était une peine, en retenant notamment qu'elle avait été ordonnée après une condamnation pour tentative de meurtre et vol qualifié et qu'elle visait davantage un but punitif que préventif, ainsi qu'en attestent son exécution dans une prison ordinaire, l'absence de soins spécialisés pour réduire la dangerosité de la personne concernée, la durée illimitée de la détention, son prononcé par les tribunaux et

[13] Il s'agissait en l'espèce de l'interdiction pendant 20 ans d'entrer en contact avec les parties civiles et de détenir une arme.

son exécution déterminée par les tribunaux de l'application des peines qui font partie du système de la justice pénale (arrêt du 17 décembre 2009, n° 19359/04, M. c. Allemagne)

1.3. CADRE CONSTITUTIONNEL

Sans s'estimer lié par la qualification donnée par le législateur, le Conseil constitutionnel opère une distinction entre, d'une part, le régime des peines et de certaines mesures dont elles peuvent être assorties et, d'autre part, le régime des mesures qui peuvent être appliquées, selon les cas, à une personne mise en cause ou condamnée pénalement ou en dehors de toute affaire pénale et qui n'ont pas de caractère punitif, parmi lesquelles figurent traditionnellement les mesures de sûreté[14].

Seules les peines sont soumises aux exigences résultant de l'article 8 de la Déclaration de 1789[15], qui s'applique à *« toute sanction ayant le caractère d'une punition »* et aux termes duquel : *« La loi ne doit établir que des peines strictement et évidemment nécessaires, et nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit, et légalement appliquée »*. Les mesures de sûreté ne sauraient méconnaître les exigences de cet article.

Ainsi, dans sa décision n° 2004-492 DC du 2 mars 2004, saisi de dispositions prévoyant l'inscription de l'identité d'une personne dans le fichier judiciaire national automatisé des auteurs d'infractions sexuelles, le Conseil a jugé que cette inscription *« a pour objet […] de prévenir le renouvellement des infractions et de faciliter l'identification des auteurs ; qu'il en résulte que cette inscription ne constitue pas une sanction mais une mesure de police ; que les auteurs des saisines ne sauraient dès lors utilement soutenir qu'elle méconnaîtrait le principe de nécessité des peines qui résulte de l'article 8 de la Déclaration de 1789 »*[16].

Le Conseil a également jugé, dans sa décision n° 2008-562 DC du 21 février 2008, que « *la rétention de sûreté n'est ni une peine, ni une sanction ayant le caractère d'une punition ; que la surveillance de sûreté ne l'est pas davantage ; que, dès lors, les griefs tirés de la méconnaissance de l'article 8 de la Déclaration de 1789 sont inopérants »*[17]. En dépit de l'inopérante de l'article 8 de la Déclaration de 1789 qu'il venait de constater, le Conseil a jugé, *« toutefois, que la rétention de sûreté, eu égard à sa nature privative de liberté, à la durée de*

[14] Dans l'ouvrage Vocabulaire juridique de Gérard Cornu, la notion de mesure de sûreté est définie comme une « Mesure de précaution destinée à compléter ou suppléer la peine encourue par un délinquant qui, relevant en principe, comme la peine, de l'autorité judiciaire ne constitue pas un châtiment, mais une mesure de défense sociale imposée à un individu dangereux afin de prévenir les infractions futures qu'il pourrait commettre et que son état rend probables, l'aider ou le soumettre à un traitement ».

[15] Ces exigences recouvrent le principe de légalité des délits et des peines, de non-rétroactivité des peines, de nécessité, de proportionnalité et d'individualisation des peines

[16] Décision n° 2004-492 DC du 2 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité, cons. 74.

[17] Décision n° 2008-562 DC du 21 février 2008, Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental, cons. 9.

cette privation, à son caractère renouvelable sans limite et au fait qu'elle est prononcée après une condamnation par une juridiction, ne saurait être appliquée à des personnes condamnées avant la publication de la loi ou faisant l'objet d'une condamnation postérieure à cette date pour des faits commis antérieurement »[18]

Il résulte de cet exposé jurisprudentiel que, pour distinguer une peine d'une mesure de sûreté, le Conseil s'appuie sur la nature du critère retenu pour y recourir (culpabilité ou dangerosité de la personne), l'objectif poursuivi (punir ou prévenir), le moment de sa mise en œuvre (lors de la peine ou à son issue) ainsi que l'autorité compétente pour la prononcer (juridiction de jugement ou autre juridiction).

Par ailleurs, si les mesures de sûreté ne sont pas soumises aux exigences de l'article 8 de la Déclaration de 1789, elles restent soumises aux autres exigences constitutionnelles qu'elles mettent en cause.

S'applique en effet le principe qui, en matière de restrictions apportées à la liberté individuelle, à la liberté personnelle ou au respect de la vie privée, prohibe la rigueur non nécessaire[19], en application des articles 4 et 9 de la Déclaration de 1789. Le Conseil s'assure que les atteintes portées à ces libertés sont *« adaptées, nécessaires et proportionnées à l'objectif de prévention poursuivi »*[20].

Ainsi, dans sa décision n° 2008-562 DC du 21 février 2008 précitée, le Conseil a, après avoir écarté le grief tiré de la méconnaissance de l'article 8 de la Déclaration de 1789, examiné la conformité de la rétention et de la surveillance de sûreté à la liberté d'aller et venir, au respect de la vie privée et à la liberté individuelle. Le Conseil a alors vérifié :

- L'adéquation du champ d'application de la mesure à la finalité poursuivie (contrôle du caractère adapté de la mesure) ;

- Que les dispositions adoptées ne permettaient de prononcer la rétention de sûreté qu'en l'absence d'autres solutions moins attentatoires à la liberté (contrôle de la nécessité). Il a, à cet égard, formulé une réserve d'interprétation selon laquelle il appartient à la juridiction régionale de la rétention de sûreté de vérifier que la personne condamnée a effectivement été mise en mesure de bénéficier, pendant l'exécution de sa peine, de la prise en charge et des soins adaptés au trouble de la personnalité dont elle souffre ;

- Que les garanties procédurales énoncées par le législateur (mesure prononcée par une juridiction indépendante, débat contradictoire, voies de recours) étaient de nature à assurer le respect du droit à un procès équitable (caractère proportionné de la mesure) ;

---

[18] *Ibid.* cons. 10.

[19] par exemple : n° 2002-461 DC du 29 août 2002, loi d'orientation et de programmation pour la justice, cons. 85 ; n° 2003-467 DC du 13 mars 2003, loi pour la sécurité intérieure, notamment cons. 49

[20] Décision n° 2008-562 DC du 21 février 2008, précitée, cons. 13.

Par ailleurs, dans sa décision n° 2004-492 DC du 2 mars 2004 précitée, après avoir considéré que l'inscription de l'identité d'une personne dans le fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS) ne constitue pas une sanction, le Conseil a examiné sa conformité à la Constitution au regard du droit au respect de la vie privée[21].

Le Conseil constitutionnel a également été amené à contrôler des mesures ordonnées par l'administration, qui visent à soumettre une personne à certaines obligations ou interdictions afin de prévenir la menace qu'elle présente, par son comportement, pour la sécurité et l'ordre publics.

S'agissant des mesures individuelles de contrôle administratif et de surveillance (MICAS), le Conseil constitutionnel a limité à douze mois la durée totale cumulée de ces mesures « compte tenu de leur rigueur » (décisions n° 2017-691 du 16 février 2018 et n° 2017-695 QPC du 29 mars 2018). Comme l'indique le commentaire, *« cette réserve d'interprétation rend compte de plusieurs éléments. D'une part, la mesure d'assignation à résidence est une mesure de droit commun, hors état d'urgence, ce qui justifie l'édiction de garanties supplémentaires. D'autre part, cette mesure présente, pour ceux auxquels elle s'applique, qui disposent d'une liberté complète d'aller et venir sur le territoire et ne sont pas mis en cause pour une infraction, une contrainte forte, ce que traduit l'expression* "compte tenu de sa rigueur". *Enfin, la nécessité de fixer un terme à la mesure, indépendamment de la persistance de la menace, avait elle-même été reconnue par le législateur, qui avait prévu une telle durée totale maximale de douze mois ».*

Enfin, dans sa décision n° 2020-805 DC du 7 août 2020, *Loi n° 2020-1023 du 10 août 2020 instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine,* le Conseil constitutionnel a censuré l'article 1er de la loi précitée qui instituait une nouvelle mesure de sûreté applicable aux personnes condamnées pour un acte de terrorisme, et présentant, à la fin de l'exécution de leur peine, une particulière dangerosité caractérisée par une probabilité très élevée de récidive et par une adhésion persistante à une idéologie ou à des thèses incitant à la commission d'actes de terrorisme.

Cette mesure de sûreté ne pouvait être prononcée que si la personne avait été condamnée à une peine privative de liberté d'une durée d'au moins cinq ans ou, en cas de récidive légale, d'au moins trois ans. Prise après un avis motivé de la commission pluridisciplinaire des mesures de sûreté chargée d'évaluer la dangerosité la personne, cette mesure était ordonnée par la juridiction régionale de la rétention de sûreté de Paris. Elle permettait d'imposer à la personne de respecter certaines obligations ou interdictions. La méconnaissance de ces obligations ou interdictions était punie de trois ans d'emprisonnement et de 45 000 euros d'amende. Cette mesure pouvait être ordonnée pour une durée maximale d'un an, renouvelable pour la même durée dans la limite de dix ans au maximum, ou cinq ans s'il s'agit d'un mineur.

[21] Décision n° 2004-492 DC du 2 mars 2004 précitée, cons. 75-76.

Le Conseil constitutionnel a jugé que ces dispositions méconnaissaient le principe de rigueur nécessaire et qu'elles n'étaient pas nécessaires, adaptées et proportionnées au regard de l'objectif poursuivi au regard des éléments suivants :

- en premier lieu, la mesure permettait d'imposer de nombreuses interdictions et obligations, éventuellement cumulatives, portant atteintes à la liberté d'aller et venir, au respect de la vie privée et à la vie familiale. Il a mis en exergue les plus attentatoires d'entre elles (paragr. 15)[22] ;
- en deuxième lieu, la durée de la mesure en accroissait la rigueur (période initiale d'un an, mais pouvant être renouvelée à 5 ou 10 ans et 3 ou 5 ans pour les mineurs). Il a relevé que ces durées maximales s'appliquaient seulement en considération de la peine encourue, quel que soit le quantum de la peine prononcée (paragr. 16) ;
- en troisième lieu, une personne condamnée à une peine d'emprisonnement dont la partie ferme était d'une durée très limitée pouvait être soumise à la mesure de sûreté contestée. Cette mesure pouvait également être décidée peu de temps après le prononcé de la condamnation alors que, s'agissant d'une peine assortie en partie du sursis, la juridiction de jugement pouvait décider de soumettre la personne dans le cadre d'une mise à l'épreuve à des obligations proches de celles de la mesure de sûreté (paragr. 17) ;
- en quatrième lieu, la mesure pouvait être prononcée sans que l'on exige que la personne ait pu bénéficier, pendant l'exécution de sa peine, de mesures de nature à favoriser sa réinsertion (paragr. 18) ;
- en cinquième lieu, le renouvellement de la mesure pouvait être décidé sans qu'il soit exigé que la dangerosité soit corroborée par des éléments nouveaux ou complémentaires (paragr. 19).

Toutefois, dans sa décision du 7 août 2020 précitée, le Conseil constitutionnel n'a pas écarté toute possibilité pour le législateur de prévoir des mesures de sûreté fondées sur la particulière dangerosité, évaluée à partir d'éléments objectifs, de l'auteur d'un acte terroriste et visant à prévenir la récidive de telles infractions (paragr. 14).

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

La mesure de sûreté créée par le projet de loi a pour objectif d'assurer le suivi des personnes actuellement détenues pour actes de terrorisme en lien avec la mouvance islamiste dont la peine arrive à échéance dans les prochains mois ou prochaines années.

[22] Paragr. 15. Il s'agit des mesures suivantes : obligation d'établir sa résidence dans un lieu déterminé, obligation de se présenter périodiquement aux services de police ou aux unités de gendarmerie, interdiction de se livrer à certaines activités, interdiction d'entrer en relation avec certaines personnes ou de paraître dans certains lieux, obligation de respecter les conditions d'une prise en charge sanitaire, sociale, éducative ou psychologique.

Au 11 août 2020, environ 500 personnes prévenues et condamnées sont détenues pour des actes de terrorisme en lien avec la mouvance islamiste[23]. Ils sont dénommés TIS pour terroristes islamistes sunnites.

A cette même date, 163 TIS définitivement condamnés pour crime ou délit qualifiés d'acte de terrorisme doivent être libérés dans les 3 ans qui viennent (18 en procédure criminelle et 145 en procédure correctionnelle).

TIS sortant à 3 ans	**163**
fin 2020	17
fin 2021	66
fin 2022	47
fin 2023	33

Comme exposé ci-dessus (1.1.), les mesures existantes n'apparaissent pas toujours adaptées en raison :

- du caractère non rétroactif de certaines d'entre elles ;
- du fait qu'elles ne survivent pas nécessairement à la fin de la peine et ne peuvent être prononcées que pour la durée des réductions de peine éventuellement octroyées ;
- du profil des personnes concernées, qui ne présentent pas toutes des troubles graves de la personnalité permettant le prononcé de mesures de suivi sur ce fondement au-delà de la fin de la peine.

La mesure judiciaire de réinsertion sociale antiterroriste a donc pour objectif d'assurer la réinsertion des détenus TIS par un accompagnement resserré et adapté à leur profil, au moyen d'obligations ou d'interdictions à vocation essentiellement sociale.

Cette mesure est complémentaire des mesures individuelles de contrôle administratif et de surveillance (MICAS), dont le prolongement est également envisagé dans le projet de loi pour les personnes condamnées à des peines supérieures à cinq ans d'emprisonnement ferme, ou trois ans en cas de récidive.

La MICAS a pour finalité le contrôle et la surveillance des personnes, tandis que la mesure judiciaire de sûreté poursuit une finalité de réadaptation sociale.

[23] Chiffres fournis par le Service national du Renseignement pénitentiaire (SNRP)

Ainsi, s'agissant de dispositions relatives à la procédure pénale, dont la modification relève du domaine de la loi en application de l'article 34 de la Constitution, un vecteur législatif est nécessaire.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ECARTEES

A été envisagée la création d'une mesure de sûreté comprenant des obligations de contrôle et de surveillance, à l'instar de celle prévue par la loi n° 2020-1023 du 10 août 2020 précitée, en adaptant ses modalités à l'aune des cinq griefs retenus par le Conseil constitutionnel.

Cette option a toutefois été écartée au bénéfice d'un dispositif global plus adapté au suivi des sortants de prison condamnés pour acte de terrorisme présentant deux volets distincts. La MJRSA a pour objectif de favoriser leur réinsertion, tandis que la prolongation de la durée des MICAS jusqu'à deux ans pour un certain public vise à assurer un contrôle et une surveillance de ces personnes. Il s'agit d'éviter une superposition de mesures susceptibles d'être appliquées aux mêmes fins et comprenant des prescriptions, sinon identiques, au moins comparables.

3.2. DISPOSITIF RETENU

La mesure judiciaire de réinsertion sociale antiterroriste (MJRSA) est une mesure de sûreté visant à assurer la réinsertion des personnes condamnées pour acte de terrorisme en les soumettant à des obligations et interdictions présentant une finalité de réadaptation sociale.

Cette mesure s'applique aux personnes condamnées à une peine privative de liberté non assortie du sursis d'une durée supérieure ou égale à 5 ans pour un acte de terrorisme, ou 3 ans en cas de récidive, s'il est établi, à l'issue d'un réexamen de leur situation intervenant à la fin de l'exécution de sa peine, qu'ils présentent une particulière dangerosité caractérisée par une probabilité très élevée de récidive et par une adhésion persistante à une idéologie ou à des thèses incitant à la commission d'actes de terrorisme (I de l'article 706-25-16 du code de procédure pénale).

Elle ne peut être ordonnée que si cette mesure apparaît strictement nécessaire (IV de l'article 706-25-16 du code de procédure pénale) pour prévenir la récidive. Elle n'est pas applicable si la personne a été condamnée à un suivi socio-judiciaire en application de l'article 421-8 du code pénal ou si elle fait l'objet d'une mesure de surveillance judiciaire prévue à l'article 723-29 du code de procédure pénale, d'une mesure de surveillance de sûreté prévue à l'article 706-53-19 ou d'une rétention de sûreté prévue à l'article 706-53-13 du même code.

La MJRSA est prononcée par le tribunal de l'application des peines de Paris, sur réquisitions du procureur de la République antiterroriste et après avis de la commission pluridisciplinaire des mesures de sûreté (article 706-25-16 du code de procédure pénale) pour une durée maximale d'un an. Elle peut être renouvelée pour la même durée dans la limite de cinq ans ou, lorsque le

condamné est mineur, dans la limite de trois ans (III de l'article 706-25-16 du code de procédure pénale).

La situation des personnes détenues susceptibles de faire l'objet d'une telle mesure est examinée, sur réquisitions du procureur de la République antiterroriste, au moins trois mois avant la date prévue pour leur libération par la commission pluridisciplinaire des mesures de sûreté prévue à l'article 763-10 du code de procédure pénale, afin d'évaluer leur dangerosité (article 706-25-17 du code de procédure pénale). À cette fin, la commission demande le placement de la personne concernée, pour une durée d'au moins six semaines, dans un service spécialisé chargé de l'observation des personnes détenues aux fins d'une évaluation pluridisciplinaire de dangerosité. À l'issue de cette période, la commission adresse au tribunal de l'application des peines de Paris et à la personne concernée un avis motivé sur la pertinence de prononcer la mesure de sûreté.

La décision est prise, avant la date prévue pour la libération du condamné, par un jugement rendu après un débat contradictoire et, si le condamné le demande, public, au cours duquel le condamné est assisté par un avocat choisi ou commis d'office. Elle doit être spécialement motivée au regard des conclusions de l'évaluation et de l'avis de la commission, ainsi que du caractère strictement nécessaire de la mesure pour prévenir la récidive. Le jugement précise les obligations auxquelles le condamné est tenu ainsi que la durée de celles-ci. La décision est exécutoire immédiatement à l'issue de la libération (article 706-25-18 du code de procédure pénale).

Le tribunal de l'application des peines de Paris peut, sur réquisitions du procureur de la République antiterroriste ou à la demande de la personne concernée, le cas échéant, après avis du procureur de la République antiterroriste, modifier les mesures de sûreté ou ordonner leur mainlevée. Cette compétence s'exerce sans préjudice de la possibilité, pour le juge de l'application des peines, d'adapter à tout moment les obligations de la mesure de sûreté (article 706-25-18 du code de procédure pénale). Les décisions peuvent être attaquées par la voie de l'appel devant la chambre de l'application des peines de la cour d'appel, (article 706-25-19 du code de procédure pénale).

Les obligations sont suspendues par toute détention intervenue au cours de leur exécution. Si la détention excède une durée de six mois, la reprise d'une ou de plusieurs des obligations doit être confirmée par le tribunal de l'application des peines de Paris au plus tard dans un délai de trois mois après la cessation de la détention, à défaut de quoi il est mis fin d'office à la mesure (article 706-25-20 du code de procédure pénale).

La décision définit (I de l'article 706-25-16 du code de procédure pénale) les conditions d'une prise en charge sanitaire, sociale, éducative ou psychologique, destinée à permettre la réinsertion et l'acquisition des valeurs de la citoyenneté. Cette prise en charge peut, le cas échéant, intervenir au sein d'un établissement d'accueil adapté. Elle peut imposer à l'intéressé d'exercer une activité professionnelle, de suivre un enseignement ou une formation professionnelle ; elle peut également lui interdire de se livrer à l'activité dans l'exercice ou à l'occasion de laquelle l'infraction a été commise. La décision précise les conditions dans

lesquelles l'intéressé doit communiquer au service pénitentiaire d'insertion et de probation les renseignements ou documents de nature à permettre le contrôle de ses moyens d'existence et de l'exécution de ses obligations, et répondre aux convocations du juge de l'application des peines ou du service pénitentiaire d'insertion et de probation. Elle peut aussi l'astreindre à établir sa résidence en un lieu déterminé.

Les obligations auxquelles la personne concernée est astreinte sont mises en œuvre par le juge de l'application des peines du tribunal judiciaire de Paris assisté du service pénitentiaire d'insertion et de probation et, le cas échéant, avec le concours des organismes habilités à cet effet.

La sanction prévue en cas de non-respect de ces obligations et interdictions est fixée à un an d'emprisonnement et 15 000 euros d'amende (article 706-25-21 CPP).

S'agissant plus précisément de l'obligation de respecter les conditions d'une prise en charge sanitaire, sociale, éducative ou psychologique, celle-ci est susceptible d'intervenir au sein des centres PAIRS (centres de prise en charge individualisée des personnes radicalisées).

Ces structures, initialement envisagée à titre expérimental en décembre 2016[24], ont été pérennisées par le plan national de prévention de la radicalisation présenté par le Gouvernement le 23 février 2018[25]. Les centres de Paris et de Marseille ont été ouverts en 2018, celui de Lyon le 10 juillet 2019 et celui de Lille le 7 octobre 2019.

Au sein des centres, la prise en charge est effectuée par une équipe pluridisciplinaire, composée *à minima* de 7 travailleurs sociaux expérimentés, d'un spécialiste de l'islam contemporain, d'un psychiatre et d'un psychologue. Elle peut être étayée par un conseiller pénitentiaire d'insertion et de probation, un spécialiste de la géopolitique ou des universitaires.

Un hébergement individualisé au sein d'un réseau de partenaires des services pénitentiaires d'insertion et de probation (SPIP) peut être proposé pour garantir une distance géographique suffisante par rapport à un environnement considéré comme défavorable, favoriser l'insertion, ou permettre l'accès des personnes éloignées. Hors les cas où un hébergement sera proposé, les bénéficiaires doivent être domiciliés dans un rayon de 100 km ou 1h30 de transport, avec prise en charge partielle des frais.

Une première phase de diagnostic intervient au maximum dans les trois premiers mois de prise en charge et permet au référent en charge du suivi de la personne au sein de la structure de proposer un programme adapté de prise en charge.

---

[24] Dispositif de prise en charge individuelle et pluridisciplinaire de personnes placées sous main de justice baptisé RIVE (recherche et intervention sur les violences extrémistes)

[25] Le plan prévoit ainsi, dans sa mesure 58, la création de « trois nouveaux centres de prise en charge individualisée pour des personnes radicalisées ou en voie de radicalisation, placées sous-main de justice à Lille, Lyon et Marseille, pilotés par le ministère de la Justice, pour mettre en œuvre une prise en charge individualisée éducative, psychologique et sociale efficiente, avec un référent cultuel

Trois niveaux de prise en charge sont possibles en fonction des besoins repérés dans chacune des dimensions du suivi (psychosociale, psychologique, culturelle, socio-professionnelle…) :

- le niveau 1 dit milieu ouvert renforcé, consistant en une prise en charge de 3 heures par semaine ;
- le niveau 2 dit intermédiaire permettant une prise en charge jusqu'à 10 heures par semaine pour les personnes dont le niveau de radicalité et d'intégration sociale demande un accompagnement important ;
- le niveau 3 dit intensif correspondant à une prise en charge jusqu'à 20 heures par semaine, et visant les personnes ayant un niveau de radicalité élevé et nécessitant par ailleurs un accompagnement intensif en vue de leur réinsertion sociale.

Le niveau de prise en charge proposé par le centre à l'issue du diagnostic est soumis à la validation du SPIP et peut être modifié tout au long du suivi. Le magistrat mandant est destinataire de ce projet via le SPIP et peut solliciter un renforcement ou un allègement du suivi à tout moment du déroulement de la mesure. Une fois validé, ce programme fait l'objet d'un écrit (document individuel de prise en charge) communiqué à la personne concernée.

Un comité de suivi du dispositif, composé des représentants des centres, de l'autorité judiciaire, du SPIP, de la direction des affaires criminelles et des grâces, de la direction de l'administration pénitentiaire, se réunira au minimum deux fois par an pour faire le bilan de l'activité des centres.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Les modifications législatives concernent exclusivement des dispositions du code de procédure pénale. Il est ainsi créé une section 5 au titre XV du livre IV intitulé « De la mesure judiciaire de réinsertion sociale antiterroriste » et comportant les articles 706-25-16 à 706-25-22.

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES

Au regard du faible nombre du public concerné par la nouvelle mesure de sûreté, son impact sur les services judiciaires apparaît limité.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application de la loi dans le temps

S'agissant d'une mesure de sûreté, celle-ci s'appliquera, dès son entrée en vigueur, à l'ensemble des faits commis avant son entrée en vigueur.

5.2.2. Application de la loi dans l'espace

Cet article a vocation à s'appliquer dans l'ensemble des collectivités ultra-marines où l'Etat est compétent en matière pénale.

Dans les collectivités régies par le principe de l'identité législative (Guadeloupe, Guyane, Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin, Saint-Pierre-et-Miquelon), les dispositions pénales sont applicables de plein droit. Aucune adaptation n'apparaît nécessaire.

Dans les collectivités régies par le principe de spécialité législative (Nouvelle-Calédonie, Polynésie française, Wallis-et-Futuna), aucune adaptation n'apparaît nécessaire et ces dispositions sont expressément étendues à ces collectivités.

5.2.3. Textes d'application

Les nouvelles dispositions appellent l'adoption d'un décret en Conseil d'Etat précisant les conditions et les modalités d'application de la nouvelle mesure, en application du nouvel article 706-25-21 du code de procédure pénale.

Article 6 : Droit de communication aux préfets et services de renseignement des informations relatives aux soins psychiatrique sans consentement

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Depuis 2017, le passage à l'action terroriste de profils présentant des parcours personnels complexes au plan psychiatrique ou psychologique a conduit le ministère de l'Intérieur à considérablement œuvrer à l'amélioration des dispositifs de suivi de ces individus, en lien étroit avec le ministère de la Santé.

Une instruction commune des ministres de l'intérieur et de la santé du 2 février 2018 a notamment permis de renforcer la coopération entre les préfectures et les Agences régionales de santé (ARS) en matière de prévention de la radicalisation, prévoyant en particulier la signature d'une convention entre la préfecture de département et l'ARS compétente fixant la nature et les modalités de leurs échanges.

En outre, la prise en charge des publics en voie de radicalisation et présentant cumulativement des fragilités diverses, dont des troubles du comportement, a été au centre de la création des cellules départementales de suivi pour la prévention de la radicalisation et l'accompagnement des familles (CPRAF). L'apport de la CPRAF est, de par sa composition même, essentiel, là où un seul suivi en groupe d'évaluation départemental (GED) par un service de renseignement démontre ses limites dans la prise en compte de ce type de profils. Alors que les GED ne permettent qu'un suivi sécuritaire, les CPRAF offrent des possibilités d'accompagnements sociaux, éducatifs, médicaux et psychologiques, voire psychiatriques, adaptés à la situation de chaque individu ainsi que de sa famille.

Les actions terroristes commises en 2019 et 2020 ont cependant mis en avant la nécessité de renforcer encore davantage les interactions entre le milieu de la santé et l'autorité administrative, aux fins d'accroître la prévention d'éventuels actes terroristes et d'assurer une prise en charge plus adaptée des profils présentant des troubles du comportement altérant le discernement.

C'est dans ce contexte qu'a été acté, entre les ministères de l'intérieur et de la santé, le besoin de rapprocher le fichier HOPSYWEB[26], qui recense et assure le suivi des personnes faisant l'objet de soins psychiatriques sans consentement, et le Fichier de traitement des signalements

[26] Créé par le décret n° 2018-383 du 23 mai 2018, le fichier HOPSYWEB est un traitement de données à caractère personnel réalisé à l'échelle départementale, placé sous la responsabilité de chaque agence régionale de santé, relatif au suivi des personnes en soins psychiatriques sans consentement prises en charge en application des dispositions des articles L. 3212-1, L. 3213-1, L. 3213-7, L. 3214-3 du code de la santé publique et 706-135 du code de procédure pénale.

pour la prévention de la radicalisation à caractère terroriste (FSPRT), relevant du ministère de l'intérieur, qui recense et permet d'assurer le suivi des personnes, qui engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste. Il ressort du rapport d'information sur les services publics face à la radicalisation, enregistré à la Présidence de l'Assemblée nationale le 27 juin 2019, que 12% des personnes enregistrées dans le FSPRT présenteraient des troubles psychiatriques.

Autorisé par le décret n° 2019-412 du 6 mai 2019[27] et effectif, sur le plan technique, depuis le 15 juillet 2020, ce rapprochement vise à informer les autorités préfectorales de la présence conjointe dans HOPSYWEB (sur une profondeur de trois ans) et FSPRT d'une même personne.

Parmi les finalités listées à l'article 1er du décret n° 2018-383 du 23 mai 2018, du décret précité, figure désormais au 6° « *L'information du représentant de l'Etat sur l'admission des personnes en soins psychiatriques sans consentement nécessaire aux fins de prévention de la radicalisation à caractère terroriste dans les conditions prévues au livre II de la troisième partie du code de la santé publique et à l'article 706-135 du code de procédure pénale* ».

Pour cette seule finalité, l'article 2-1 dudit décret (créé par le décret n° 2019-412 du 6 mai 2019) permet désormais la mise en relation des noms, prénoms et dates de naissance des personnes figurant dans ce traitement avec le fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT).

Lorsque cette mise en relation des traitements révèle une correspondance, le représentant de l'État dans le département où les soins sont délivrés et, le cas échéant, les agents qu'il désigne à cette fin, en sont informés. Cette information permet au représentant de l'État d'adapter le suivi de l'individu connu à raison de sa radicalisation, pour adapter sa prise en charge au regard des troubles psychiatriques révélés.

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel considère que la liberté proclamée par l'article 2 de la Déclaration des droits de l'Homme et du citoyen de 1789 implique le droit au respect de la vie privée, lequel requiert que soit observée une particulière vigilance dans la collecte et le traitement de données à caractère personnel de nature médicale (décision n° 2004-504 DC du 12 août 2004).

Toutefois, il appartient au législateur d'assurer la conciliation entre, d'une part, la protection de la santé des personnes souffrant de troubles mentaux ainsi que la prévention des atteintes à l'ordre public, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle et, d'autre part, la protection des droits et libertés constitutionnellement garantis au nombre desquels figurent la liberté d'aller et venir et le respect de la vie privée, protégés par les articles

[27] Décret n° 2019-412 du 6 mai 2019 modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement.

2 et 4 de la Déclaration des droits de l'Homme et du citoyen de 1789 (CE 28 déc. 2018, *Assoc. Cercle de réflexion et de proposition d'actions sur la psychiatrie*, n° 421329).

Le Conseil constitutionnel a déjà été amené à se prononcer sur la conformité à la Constitution de dispositions législatives organisant un partage, entre différentes autorités, d'informations à caractère confidentiel et en a confronté le principe et les modalités à l'objectif d'intérêt général poursuivi.

Si le législateur peut prévoir un droit de communication entre autorités publiques de données à caractère confidentiel, ce n'est qu'au nom d'un motif d'intérêt général, les atteintes au caractère confidentiel de ces données personnelles devant être adéquates et proportionnées à l'objectif poursuivi (CC 22 mars 2012, *Loi relative à la protection de l'identité*, n° 2012-652 DC ; 9 octobre 2013, *Loi relative à la transparence de la vie publique*, n° 2013-676 DC).

Le législateur doit alors définir avec suffisamment de précision les conditions des atteintes portées à la vie privée des personnes concernées, la nature des finalités poursuivies par l'atteinte portée à ce droit, ainsi que les garanties encadrant cette atteinte.

Ont ainsi été considérées comme ne méconnaissant pas le droit au respect de la vie privée, notamment, **une dérogation au secret fiscal**, dès lors qu'elle ne profite qu'à certaines personnes, dans des conditions clairement définies (CC 29 déc. 1983, *Loi de finances pour 1984*, n° 86-164 DC).

De même, a été jugé conforme à la Constitution, une disposition déliant un professionnel de l'action sociale de son secret professionnel pour **communiquer au maire ou au président du conseil général**, des informations confidentielles sur une personne ou une famille, dont l'aggravation des difficultés sociales, éducatives ou matérielles appelait l'intervention de plusieurs professionnel, dès lors que cette transmission d'informations est strictement nécessaire à l'accomplissement de la mission d'action sociale (CC 3 mars 2007, *Loi relative à la prévention de la délinquance*, n° 2007-553 DC).

Dans cette décision, le Conseil constitutionnel a considéré que le législateur a ainsi assorti les échanges d'informations qu'il a autorisés de limitations et précautions propres à assurer la conciliation qui lui incombe entre, d'une part, le droit au respect de la vie privée et, d'autre part, les exigences de solidarité découlant des dixième et onzième alinéas du Préambule de 1946.

En revanche, dans une décision relative aux dispositions de l'article L. 132-10-1 du code de la sécurité intérieure qui prévoyaient que les autorités judiciaires et les services pénitentiaires d'insertion et de probation peuvent transmettre aux états-majors de sécurité et aux cellules de coordination opérationnelle toute information qu'ils jugeraient utile de leur confier pour l'organisation du suivi des personnes condamnées qu'ils leur auraient désignées, le Conseil constitutionnel (23 sept. 2016, décision n° 2016-569 DC, cons. 25 s.) a certes reconnu que le législateur poursuivait un but d'intérêt général (favoriser l'exécution des peines et prévenir la récidive), mais a considéré qu'en se bornant à prévoir que la transmission pouvait concerner

« *toute information (...) sans définir la nature des informations concernées ni limiter leur champ* », le législateur a porté une atteinte disproportionnée au droit au respect de la vie privée. En effet, aucune indication n'était donnée sur la nature ou les catégories d'informations susceptibles d'être transmises, en dehors du fait qu'elles devaient être utiles au suivi de la mesure en milieu ouvert.

Enfin, dans une décision n° 2019-789 QPC du 14 juin 2019, relative au droit de communication des organismes de sécurité sociale, prévu à l'article L. 114-20 du code de la sécurité sociale, le Conseil constitutionnel a fait application des critères dégagés par sa jurisprudence en matière d'échanges, tenant aux finalités qui le justifient, aux éléments sur lesquels ils portent (leur « domaine d'application », selon les termes du Conseil constitutionnel) et notamment sur leur caractère délimité et sur les garanties entourant leur mise en œuvre. Il a jugé conforme à la Constitution le fait que les agents compétents des organismes de sécurité sociale puissent exercer leur droit de communication à des fins de recueil de données bancaires auprès des établissements de crédit et des établissements assimilés, qui, notamment, présentent un lien direct avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation. Il a en revanche censuré l'exercice du droit de réquisition aux fins d'obtenir auprès des opérateurs de communications électroniques les données de connexion conservées par ceux-ci, en se fondant sur le caractère à la fois sensible et non circonscrit de ces données, et donc sur la difficulté à les mettre directement en relation avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation.

1.3. CADRE CONVENTIONNEL

La protection des données à caractère personnel, dont celles relatives à la santé, est capitale non seulement pour protéger la vie privée des malades, mais également pour préserver leur confiance dans le corps médical et les services de santé en général. Les législations internes doivent donc ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'art. 8 de la Convention (CEDH 25 févr. 1997, Z. c. Finlande, n° 22009/93).

Cette divulgation doit tout d'abord être **nécessaire** et conformément au paragraphe 2 de l'article 8, une telle ingérence peut être motivée par la défense de l'ordre public.

La communication des seules informations médicales pertinentes à un service administratif peut répondre à un besoin légitime d'un État. Ce besoin peut, par exemple, être celui de vérifier les informations fournies par une personne qui demande à bénéficier de prestations sociales en raison de son état de santé (CEDH 27 août 1997, *M. S. c/ Suède,* n° 20837/92). En revanche, la Cour conclut à la violation de l'article 8 s'agissant de la divulgation de dossiers médicaux de témoins de Jéhovah aux autorités de poursuite russes à la suite de leur refus de subir des transfusions sanguines durant leur séjour dans des hôpitaux publics (dans le cadre d'une enquête sur la légalité des activités de cette organisation). La Cour considère en effet que les autorités n'ont pas ménagé un juste équilibre entre, d'une part, le droit des requérants au respect de leur vie privée et, d'autre part, l'objectif de protection

de la santé publique poursuivi par le procureur. (CEDH 6 juin 2013, *Avilkina et a. c. Russie*, n° 1585/09).

De même, la Cour relève que le recueil de données à caractère personnel relative à la localisation en temps réel du requérant ne méconnaît pas son droit au respect à la vie privée dès lors que cette ingérence poursuit un but légitime, à savoir la protection de la sécurité nationale, de la sûreté publique et des droits des victimes, ainsi que la prévention des infractions pénales. En outre, cette collecte de donnée est proportionnée dès lors qu'elle a été opérée après que d'autres mesures d'investigation moins attentatoires à la vie privée se sont révélées inefficaces (CEDH 2 sept. 2010, *Uzun c/ Allemagne*, n° 35623/05).

En revanche, la Cour conclut à une violation de l'article 8 s'agissant de la divulgation, lors d'une procédure judiciaire, d'informations confidentielles concernant la santé mentale d'un requérant ainsi que de son traitement psychiatrique, alors qu'en l'espèce, les informations ainsi transmises étaient sans influence sur l'issue du litige et que la demande de l'autorité judiciaire était superflue, la santé mentale du requérant ne constituant pas un élément important pour l'enquête, l'instruction ou le procès. (CEDH 29 juin 2006, *Panteleyenko c/ Ukraine*, n° 11901/02).

La communication doit ensuite être **encadrée et proportionnée**

Ainsi, l'article 8 est méconnu si les modalités de cette communication ne sont pas suffisamment encadrées (CEDH 8 février 2018, *Ben Faiza c/ France*, n° 31446/12). En effet, si le droit interne doit assurer que les données collectées sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, il doit également contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres ou abusifs (CEDH 4 déc. 2008, *S. et Marper c/ Royaume-Uni*, n° 30562/04).

Ainsi, l'utilisation, au cours d'une procédure judiciaire de divorce et sans le consentement de l'intéressé, de données à caractère médical le concernant est contraire aux stipulations de l'article 8 précité, la Cour relevant que la législation française n'assortit pas dans ce type de procédure, l'utilisation de telles données relevant la vie privée des personnes de garanties suffisantes (CEDH 10 oct. 2006, *L.L. c/ France*, n° 7508/02).

En revanche, le maintien, dans les archives d'un hôpital psychiatrique, de données relatives à l'internement d'office d'une patiente, qui ne sont pas accessibles au public mais à des catégories limitativement énumérées de personnes extérieures à l'établissement, ne constitue pas une ingérence disproportionnée au but légitime poursuivi, à savoir la protection de la santé (CEDH 9 juill. 1991, *Chave c. France*, n° 14032/88)

De même, ne viole pas l'article 8 le dispositif prévoyant une inscription au sein du Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS) dès lors que, outre la finalité légitime du traitement et le caractère proportionné au but poursuivi de la durée de conservation des données, la consultation des données personnelles par les autorités judiciaires

et administratives était régie par une obligation de confidentialités et des circonstances précisément déterminées (CEDH 17 déc. 2009, *B.B. c/ France*, n° 5335/06).

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Aux termes de l'article L. 1110-4 du code de la santé publique, toute personne prise en charge par un professionnel ou un organisme de soin régi par ce code « *a droit au respect de sa vie privée et du secret des informations la concernant. Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé.* »

Par suite, seul le législateur peut autoriser des personnes qui ne sont pas des professionnels de santé à avoir accès à des données protégées par le secret médical.

Tel est le cas s'agissant des informations en matière d'admission en soins psychiatriques sans consentement, à la demande d'un tiers ou en cas de péril imminent, sur décision du directeur de l'établissement (articles L. 3212-1 et suivants du code de la santé publique), sur décision du représentant de l'Etat dans le département (articles L. 3213-1 et suivants du code de la santé publique) ou dans le cadre d'une déclaration d'irresponsabilité pénale pour cause de trouble mental sur décision de la chambre d'instruction ou de la juridiction de jugement en application de l'article 705-135 du code de procédure pénale.

Ces trois dispositions prévoient en effet que le représentant de l'État dans le département du lieu d'hospitalisation est informé des principales décisions prises à l'encontre d'un patient admis en soins psychiatriques.

Toutefois, seul le représentant de l'État dans le département du lieu d'hospitalisation est destinataire de ces informations. Ceci explique que seul celui-ci soit informé des données issues de la mise en relation des fichiers HOPSYWEB et FSPRT. Or, certains individus, suivis pour radicalisation à caractère terroriste, peuvent faire l'objet d'une admission en soin psychiatrique dans un département différent de celui dans lequel ils résident, notamment en cas d'admission sur le fondement de l'article L. 3113-1 du code de la santé publique ou en cas d'admission pour péril imminent (2° du II de l'article L. 3212-1 du même code), dès lors que les troubles conduisant à cette admission ont été constatés dans ce département.

Il en résulte une déperdition de l'information pour l'autorité administrative en charge du suivi de la radicalisation à caractère terroriste de l'individu, laquelle peut être départementale ou nationale.

Une modification législative s'impose, dès lors, pour permettre, par dérogation aux dispositions de l'article L. 1110-4 précité, l'information des autorités en charge de ce suivi.

2.2. OBJECTIFS POURSUIVIS

Aux fins de permettre un meilleur suivi des personnes radicalisées présentant des troubles psychiatriques et de prévenir ainsi un éventuel passage à l'acte de nature terroriste, le Gouvernement souhaite autoriser l'information du préfet lorsqu'une personne signalée comme radicalisée fait l'objet d'une mesure de soins sans consentement.

La disposition ainsi ajoutée au code de la santé publique, par l'article L 3211-12-7, permet donc aux autorités administratives chargées du suivi des personnes figurant dans le fichier FSPRT (préfet du département ou services de renseignement) mais différentes du représentant de l'État du département du lieu d'hospitalisation de pouvoir figurer parmi les destinataires de cette mise en relation.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

L'exception au principe posé à l'article L. 1110-4 du code de la santé publique pourrait trouver sa place au sein de ce code ou du code de la sécurité intérieure, eu égard à la finalité de prévention de la radicalisation ainsi poursuivie.

Au sein du code de la sécurité intérieure, il pourrait être envisagé de modifier l'article L. 222-2, qui prévoit l'accès, à des fins de prévention et de répression des atteintes aux intérêts fondamentaux de la nation, de certains agents habilités à des fichiers de traitement de données à caractère personnel.

Toutefois, pour une meilleure lisibilité, il a été considéré que ces dispositions avaient davantage leur place au sein du code de la santé publique qui, d'une part, pose le principe du secret médical et en prévoit les exceptions et d'autre part, encadre le régime des soins psychiatriques sans consentement et les modalités d'information de l'autorité administrative.

C'est d'ailleurs aujourd'hui sur la base des transmissions d'informations prévues par le code de la santé publique qu'est instaurée la mise en relation des fichiers FSPRT et HOPSYWEB.

3.2. DISPOSITIF RETENU

Dans le code de la santé publique, est créé un article L. 3211-12-7 qui prévoit que, aux seules fins d'assurer le suivi d'une personne qui présente une menace grave pour l'ordre public à raison de sa radicalisation à caractère terroriste, le représentant de l'État dans le département et, à

Paris, le préfet de police, ainsi que les services de renseignement (visés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure) peuvent se voir communiquer les informations strictement nécessaires à l'accomplissement de leurs missions portées à la connaissance du représentant de l'État dans le département d'hospitalisation en application des articles L. 3212-5, L. 3212-8, L. 3213-9 du code de la santé publique et 706-135 du code de procédure pénale, qui prévoient les différentes voies d'accès à des soins sans consentement.

Ainsi, cette mise en relation des fichiers HOPSYWEB et FSPRT répond à un motif d'intérêt général, comme l'exige le Conseil constitutionnel (CC 22 mars 2012, *Loi relative à la protection de l'identité*, n° 2012-652 DC) et comme l'a reconnu le Conseil d'État (CE 27 mars 2020, *Cercle de réflexion et de proposition d'actions sur la psychiatrie et a*., n° 431350), à savoir « *prévenir le passage à l'acte terroriste des personnes radicalisées qui présentent des troubles psychiatriques* ».

La nécessité de cette mise en relation a été reconnue par le Conseil d'État dans la même décision, dès lors que ne sont mises en relation que les données strictement nécessaires à l'identification des personnes qui, à la fois, sont suivies pour radicalisation et font l'objet de soin psychiatriques sans consentement.

La finalité qui vise donc à partager les informations relatives au suivi des ces personnes entre les deux institutions est donc légitime, afin de mieux prévenir les risques de passage à l'acte des personnes faisant l'objet d'un suivi au titre de la radicalisation terroriste. A cet égard, l'autorité de police administrative en charge de ce suivi doit en particulier être à même de savoir si la personne inscrite dans le fichier de signalement pour la prévention de la radicalisation à caractère terroriste fait à ou a fait l'objet d'une prise en charge psychiatrique, pour adapter son suivi.

Cette mise en relation est également adaptée et proportionnée dès lors, tout d'abord, que les données mises en relations sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie. En effet, seules deux données, pertinentes au regard du but poursuivi, peuvent être potentiellement mises en relation : le suivi d'une personne pour radicalisation et le fait qu'elle fasse ou non l'objet de soin psychiatrique sans consentement (CC 3 mars 2007, *Loi relative à la prévention de la délinquance*, n° 2007-553 DC). Ne sont rapprochées que des données très limitées, à savoir le nom, le prénom et la date de naissance des personnes concernées, sans aucune autre information plus précise.

D'autre part, les modalités de cette mise en relation sont proportionnées à l'objectif poursuivi de prévenir le passage à l'acte terroriste des personnes radicalisées qui présentent des troubles psychiatriques dès lors que sont seuls destinataires les personnes ayant besoin d'en connaître pour contribuer à atteindre cet objectif (CC 29 déc. 1983, *Loi de finances pour 1984*, n° 86-164 DC), à savoir le préfet en charge du suivi pour radicalisation à caractère terroriste et les services de renseignement en charge de la prévention des atteintes aux intérêts fondamentaux de la Nation, au nombre desquelles figure la prévention du terrorisme (4° de l'article L. 811-3 du code de la sécurité intérieure).

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. Impacts juridiques

Il est créé un nouvel article L. 3211-12-7 au code de la sécurité intérieure.

La mise en relation entre ces deux fichiers, est déjà autorisée par le décret n° 2019-412 du 6 mai 2019 modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement La disposition nouvelle ne vise qu'à permettre à d'autres représentant de l'État que celui dans le département du lieu d'hospitalisation, d'utiliser cette plateforme de mise en relation.

4.2. Impacts sur les services administratifs

L'information du préfet chargé du suivi de l'individu au titre de sa radicalisation permettra à l'autorité administrative de mieux adapter son suivi et l'accompagnement qui lui est offert.

4.3. Impacts sur les particuliers

Le champ des autorités informées de l'admission en soins sans consentement d'une personne également suivie au titre de sa radicalisation sera étendu, tout en restant circonscrit aux autorités préfectorales de deux départements. Cette information permettra aux personnes concernées de bénéficier d'un accompagnement plus adapté à leurs troubles psychiatriques.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. Consultations menees

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. Modalites d'application

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi SILT, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

5.2.3. Textes d'application

Le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement devra être modifié pour permettre d'élargir la liste des accédants à l'information en cas de correspondance entre HOPSYWEB et FSPRT et les protocoles entre ARS et préfectures seront à modifier pour préciser les conditions de la levée de doute intervenant en cas d'identification d'une correspondance.

CHAPITRE II – DISPOSITIONS RELATIVES AU RENSEIGNEMENT

Article 7 : Transmission de renseignements entre services – Communication d'information aux services de renseignement

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Les conditions d'exploitation des renseignements collectés par le biais d'une technique de renseignement sont précisées par l'article L. 822-3 du code de la sécurité intérieure. Celui-ci précise que « *les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3* », « *ces opérations [étant] soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement* ».

Les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités. Conformément à l'article L. 822-4 du même code, ces opérations de destruction, comme celles de destructions des renseignements bruts collectés, font l'objet d'une information à la CNCTR.

Plusieurs dispositions législatives encadrent par ailleurs les modalités d'échanges de renseignements entre services, ainsi que de communications d'informations à ces services par d'autres administrations et entités publiques.

L'article L. 863-2 du code de la sécurité intérieure prévoit ainsi que « *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 partager toutes les informations utiles à l'accomplissement de leurs missions* ».

En outre, le même article L. 863-2 prévoit, à son deuxième alinéa, que « *les autorités administratives mentionnées à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 [État, collectivités territoriales, organismes gérant des régimes de protection sociale, etc.] peuvent transmettre aux services de renseignement, de leur propre initiative ou sur requête de ces derniers, des informations utiles à l'accomplissement de leurs missions* ».

Enfin, l'article L. 135 S du livre des procédures fiscales prévoit que les services spécialisés de renseignement peuvent, aux fins de recherche et de prévention des atteintes aux intérêts fondamentaux de la nation en matière de sécurité publique et de sûreté de l'État, « *demander aux administrations chargées de l'assiette, du recouvrement ou du contrôle des impôts et des*

recettes douanières de toutes sortes, sans qu'elles puissent leur opposer le secret professionnel, de leur communiquer tout document utile à l'exercice de leurs missions ».

1.2. CADRE CONSTITUTIONNEL

La transmission d'informations, lorsque celles-ci ont la nature de données à caractère personnel, doit être appréciée au prisme du droit au respect de la vie privée, principe à valeur constitutionnelle que le Conseil constitutionnel tire des articles 2 et 4 de la Déclaration de 1789.

Si le législateur peut y porter des atteintes au nom d'un motif d'intérêt général, celles-ci doivent être adéquates et proportionnées à l'objectif poursuivi (CC 22 mars 2012, *Loi relative à la protection de l'identité*, n° 2012-652 DC ; 9 octobre 2013, *Loi relative à la transparence de la vie publique*, n° 2013-676 DC).

À ce titre, le Conseil constitutionnel exige du législateur qu'il définisse avec suffisamment de précision les conditions des atteintes portées à la vie privée des personnes concernées, la nature des finalités poursuivies par l'atteinte portée à ce droit, ainsi que les garanties encadrant cette atteinte.

A ainsi été considérée comme ne méconnaissant pas le droit au respect de la vie privée, une dérogation au secret fiscal, dès lors qu'elle ne profite qu'à certaines personnes, dans des conditions clairement définies (CC 29 déc. 1983, *Loi de finances pour 1984*, n° 86-164 DC).

De même, a été jugé conforme à la Constitution, une disposition déliant un professionnel de l'action sociale de son secret professionnel pour communiquer au maire ou au président du conseil général, des informations confidentielles sur une personne ou une famille, dont l'aggravation des difficultés sociales, éducatives ou matérielles appelait l'intervention de plusieurs professionnels, dès lors que cette transmission d'informations est strictement nécessaire à l'accomplissement de la mission d'action sociale (CC 3 mars 2007, *Loi relative à la prévention de la délinquance*, n° 2007-553 DC).

Dans cette décision, le Conseil constitutionnel a considéré que le législateur a assorti les échanges d'informations qu'il a autorisés de limitations et précautions propres à assurer la conciliation qui lui incombe entre, d'une part, le droit au respect de la vie privée et, d'autre part, les exigences de solidarité découlant des dixième et onzième alinéas du Préambule de 1946.

En revanche, dans une décision relative aux dispositions de l'article L. 132-10-1 du code de la sécurité intérieure qui prévoyaient que les autorités judiciaires et les services pénitentiaires d'insertion et de probation peuvent transmettre aux états-majors de sécurité et aux cellules de coordination opérationnelle toute information qu'ils jugeraient utile de leur confier pour l'organisation du suivi des personnes condamnées qu'ils leur auraient désignées, le Conseil constitutionnel (23 sept. 2016, n° 2016-569 DC, cons. 25 s.) a certes reconnu que le législateur poursuivait un but d'intérêt général (favoriser l'exécution des peines et prévenir la récidive), mais a considéré qu'en se bornant à prévoir que la transmission pouvait concerner « *toute*

information (...) sans définir la nature des informations concernées ni limiter leur champ », le législateur a porté une atteinte disproportionnée au droit au respect de la vie privée.

En effet, aucune indication n'était donnée sur la nature ou les catégories d'informations susceptibles d'être transmises, en dehors du fait qu'elles devaient être utiles au suivi de la mesure en milieu ouvert.

Enfin, dans une décision n° 2019-789 QPC du 14 juin 2019, Mme Hanen S., relative au droit de communication des organismes de sécurité sociale, prévu à l'article L. 114-20 du code de la sécurité sociale, le Conseil constitutionnel a fait application des critères dégagés par sa jurisprudence en matière d'échanges, tenant aux finalités qui le justifient, aux éléments sur lesquels ils portent (leur « domaine d'application, selon les termes du Conseil constitutionnel) et notamment sur leur caractère délimité et sur les garanties entourant leur mise en œuvre. Il a jugé conforme à la Constitution le fait que les agents compétents des organismes de sécurité sociale puissent exercer leur droit de communication à des fins de recueil de données bancaires auprès des établissements de crédit et des établissements assimilés, qui, notamment, présentent un lien direct avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation. Il a en revanche censuré l'exercice du droit de réquisition aux fins d'obtenir auprès des opérateurs de communications électroniques les données de connexion conservées par ceux-ci, en se fondant sur le caractère à la fois sensible et non circonscrit de ces données, et donc sur la difficulté à les mettre directement en relation avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation.

1.3. CADRE CONVENTIONNEL

S'agissant de la transmission entre différentes autorités, d'informations revêtant le caractère de données personnelles protégées par l'article 8 de la CEDH, la Cour européenne des droits de l'Homme a notamment pu juger que la communication par un service médical à un organisme de sécurité sociale du dossier médical d'une patiente ne méconnaissait pas le droit au respect de la vie privée. Pour conclure ainsi, la Cour relève que le service médical a eu des raisons pertinentes et suffisantes de communiquer à l'organisme de sécurité sociale le dossier médical de la requérante et que la mesure n'avait pas été disproportionnée au but légitime poursuivi, à savoir, en permettant à l'organisme de vérifier si se trouvaient réunies les conditions auxquelles la requérante pouvait bénéficier d'une indemnité pour invalidité professionnelle, de protéger le bien-être économique du pays. En outre, s'agissant de la condition tenant à ce que les restrictions au droit au respect de la vie privée doivent être « prévues par la loi », la Cour relève que la communication de telles informations est soumise à des limitations importantes et assortie de garanties effectives et satisfaisantes contre les abus (CEDH 27 août 1997, n° 20837/92).

En revanche, la Cour conclut à la violation de l'article 8 s'agissant de la divulgation de dossiers médicaux de témoins de Jéhovah aux autorités de poursuite à la suite de leur refus de subir des transfusions sanguines durant leur séjour dans des hôpitaux publics (dans le cadre d'une enquête sur la légalité des activités de cette organisation).

La Cour considère en effet que les autorités n'ont pas ménagé un juste équilibre entre, d'une part, le droit des requérants au respect de leur vie privée et, d'autre part, l'objectif de protection de la santé publique poursuivi par le procureur (CEDH 6 juin 2013, *Avilkina et a. c. Russie*, n° 1585/09).

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

En l'état du droit, l'autorisation de mise en œuvre des techniques de recueil de renseignement, telle qu'encadrée par les articles L. 821-2 et suivants du code de la sécurité intérieure, est délivrée à un service de renseignement donné, au titre d'une ou plusieurs finalités figurant dans les missions de ce service, pour une ou plusieurs techniques dont la mise en œuvre est autorisée par la loi pour la finalité poursuivie, et pour des motifs expressément précisés.

Le recueil de renseignements sur le fondement de l'une des techniques du livre VIII est donc subordonné à un triple encadrement destiné à garantir la proportionnalité de l'atteinte à la vie privée : l'autorisation de mise en œuvre délivrée par le Premier ministre désigne la ou les finalités poursuivies, la technique autorisée et le service chargé de la mettre en œuvre.

Une fois collectés, si les renseignements s'avèrent utiles à d'autres finalités et à d'autres services, les intérêts fondamentaux de la Nation peuvent justifier voire commander la transmission de ces renseignements, ce qui suppose nécessairement de sortir du cadre initialement fixé pour la mise en œuvre de la technique ayant permis leur recueil.

Ainsi, par exemple, si la mise en œuvre d'une technique de recueil de renseignement au titre de la finalité de prévention de la criminalité organisée (6° du L. 811-3) aboutit au recueil de renseignements pertinents au regard de la finalité de prévention du terrorisme (4° du L. 811-3), il appartient au service qui a recueilli ces renseignements de les transmettre aux services de renseignement qui concourent à la lutte contre le terrorisme.

Une telle possibilité est déjà induite par la loi. En effet, en posant un principe d'interdiction des extractions ou des transcriptions sans rapport avec l'une des finalités de l'article L. 811-3 (et non avec la finalité ayant justifié l'autorisation de mettre en œuvre la technique de renseignement), le premier alinéa de l'article L. 822-3 permet déjà de transcrire et d'exploiter des renseignements recueillis au titre d'une finalité mais s'avérant ensuite correspondre à d'autres finalités énumérées à l'article L 811-3 ; d'autre part, l'article L. 863-2 permet que les services de renseignement partagent entre eux ces renseignements, comme toute autre information utile à leurs missions.

Ceci étant, les dispositions du premier alinéa de l'article L. 863-2 apparaissent superfétatoires dans la mesure où le simple dialogue entre services de renseignements n'a pas à être spécifiquement encadré, alors qu'elles n'apportent en revanche, par elles-mêmes, aucune précision s'agissant de l'encadrement des échanges de renseignements collectés par la mise en œuvre d'une technique de recueil de renseignement.

En effet, ces dispositions visent le partage « *d'informations* » entre services de renseignement, notion plus large que celle de « *renseignements* » recueillis par la mise en œuvre d'une technique de recueil de renseignement et qui peut concerner des informations recueillies par d'autres moyens (par exemple auprès d'une source humaine ou en source ouverte).

On rappellera que cette disposition est issue d'un amendement du rapporteur du projet de loi relatif au renseignement devant l'Assemblée nationale, qui relevait que le Gouvernement envisageait de déposer un amendement aux fins d'autoriser les échanges d'informations entre l'administration pénitentiaire et les différents services concourant aux activités de renseignement alors qu'il était muet sur le possible échange d'informations entre les autres services, pour lesquels les dispositions de la loi sur le renseignement trouvaient déjà à jouer et offraient un certain nombre de garanties. Craignant de créer un *a contrario*, cet amendement avait donc pour seul objet, par parallélisme des formes, de « *maintenir les capacités de dialogue entre les administrations publiques sur les thématiques décisives pour la sécurité de[s] concitoyens* ».

Le partage des renseignements nécessaires à l'exercice des missions de chacun des services de la communauté du renseignement est une condition essentielle de l'efficacité de l'action qu'ils mènent pour la défense et la promotion des intérêts fondamentaux de la Nation.

Il apparaît donc nécessaire, pour les favoriser et rendre plus lisible leur encadrement, d'expliciter les conditions de transmission de renseignements collectés entre services de renseignement, afin que des données recueillies par la mise en œuvre d'une technique de renseignement sollicitée par un service et qui pourraient s'avérer utiles à un autre puissent être partagées avec lui, pour l'accomplissement de ses missions.

Par ailleurs, le deuxième alinéa de l'article L. 863-2 prévoit la possibilité pour les autorités administratives mentionnées à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 (État, collectivités territoriales, organismes gérant des régimes de protection sociale, *etc.*) de transmettre aux services de renseignement, de leur propre initiative ou sur requête de ces derniers, des informations utiles à l'accomplissement de leurs missions.

Là encore, si ces transmissions s'avèrent souvent indispensables pour permettre aux services de renseignement de mener à bien leurs missions, il convient de mieux les encadrer, en précisant les informations concernées, les finalités au titre desquelles cette transmission est possible au regard des exigences du Conseil constitutionnel en la matière et du cadre conventionnel, les garanties qui l'entourent et notamment les obligations de traçabilité qui en découlent, plus spécifiquement lorsque les informations transmises sont susceptibles de faire l'objet, de la part des services de renseignement, d'un traitement de données à caractère personnel

Pour rappel, les traitements automatisés de données à caractère personnel mis en œuvre par les services de renseignement font l'objet, en application de la loi du 6 janvier 1978 susmentionnée, d'un encadrement rigoureux. En application de l'article 31 de cette loi, dans la mesure où ils sont mis œuvre par l'État et intéressent la sûreté de l'État, la défense ou la sécurité publique, ces traitements doivent préalablement être autorisés par un acte réglementaire – selon la

sensibilité des données, un arrêté ministériel ou un décret en Conseil d'État – après avis de la Commission nationale de l'informatique et des libertés (CNIL). En outre, l'article 33 de la même loi prévoit que dans ces cas, la demande d'avis adressée à la CNIL précise obligatoirement les finalités poursuivies par le traitement concerné, les catégories de données collectées, la durée de conservation des informations ou encore les services qui peuvent en être rendus destinataires. La plupart de ces éléments figurent par ailleurs dans l'acte réglementaire autorisant le traitement, en application de l'article 35 de la loi du 6 janvier 1978.

Ainsi, le renvoi opéré par l'article L. 863-2 aux conditions applicables au fichier de destination permet de s'assurer du strict respect de ces conditions de traitement des données personnelles, fixées par des dispositions législatives et réglementaires, dont le contrôle est assuré par la CNIL.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

S'agissant des transmissions de renseignements entre services de renseignements, il aurait pu être envisagé de compléter, voire de remplacer, les dispositions sur le partage **d'informations** entre services du premier alinéa de l'article L. 863-2 du code de la sécurité intérieure par une explicitation des modalités du partage de **renseignements** entre services de renseignement.

Il a toutefois été considéré que cette disposition se référait à des notions étrangères à celles que le législateur de 2015 a retenues, puisqu'il a encadré le recueil par les services de données au moyen de techniques de renseignement, de sorte que le terme d'informations n'est pas adéquat. En outre, il est apparu plus cohérent de traiter de cette question en explicitant certaines dispositions-cadres du livre VIII régissant le recueil de données brutes, leur extraction et leur transcription ou les obligations de traçabilité des services de renseignement.

L'article L. 822-3 mentionné *infra*, qui régit la collecte, l'extraction et la transcription des renseignements et autorise déjà un décloisonnement entre la finalité ayant justifié le recueil et celles permettant l'extraction et la transcription (« *Les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3* ») apparaît ainsi offrir le cadre le plus adapté pour préciser le régime de transmission des renseignements ainsi collectés, transcrits et extraits.

En revanche, l'alinéa 2 de l'article L. 863-2 est encadré et précisé pour concilier davantage l'atteinte portée à la vie privée par les transmissions qu'il prévoit, avec des finalités mieux délimitées et des garanties plus étendues.

3.2. DISPOSITIF RETENU

3.2.1. S'agissant des transmissions de renseignements entre services (I à V)

Le I de l'article 7 explicite deux possibilités déjà induites par la loi, mais qui ne font aujourd'hui l'objet d'aucun encadrement : d'une part, il prévoit à l'article L. 822-3 que si un service de renseignement obtient des renseignements utiles à la poursuite d'une finalité différente de celle qui en a justifié le recueil, il peut les transcrire ou les extraire pour le seul exercice de ses missions ; d'autre part, il explicite les conditions dans lesquelles les renseignements recueillis par un service de renseignement peuvent être transmis à un autre service lorsque cette transmission est strictement nécessaire à l'exercice des missions du service destinataire.

Ces échanges d'informations n'ont en principe pas à faire l'objet d'une procédure spécifique d'autorisation, sauf à alourdir inutilement et à freiner les échanges entre services, alors que leurs missions et leurs méthodes de travail supposent une coopération étroite.

L'article 7 prévoit toutefois deux tempéraments à ce principe.

D'une part, lorsqu'un service de renseignement découvre, dans le cadre de l'exploitation des renseignements recueillis, qu'ils intéressent une autre finalité que celle ayant justifié le recueil, les renseignements bruts (*i.e.,* dans l'état dans lequel ils ont été recueillis, renseignements que la loi désigne par les termes de « renseignements collectés ») ne pourront être transmis à un autre service qu'après autorisation du Premier ministre donnée après avis de la Commission nationale de contrôle des techniques de renseignement dans les conditions de forme et de procédure prévues aux articles L. 821-1 et L. 821-5. Les renseignements extraits ou transcrits pourront en revanche être transmis sans autorisation.

D'autre part, et en toute hypothèse, la transmission de renseignements bruts comme de renseignements extraits ou transcrits est subordonnée à une autorisation du Premier ministre après avis de la CNCTR lorsqu'ils sont issus de la mise en œuvre d'une technique de recueil de renseignement à laquelle le service destinataire n'aurait pu recourir au titre de la finalité motivant la transmission.

Il convient en effet de rappeler :

- d'une part, que la possibilité de mettre en œuvre certaines techniques de renseignements est limitée à certaines des finalités prévues à l'article L. 811-3 (en particulier la prévention du terrorisme : tel est le cas de la détection en temps réel prévue à l'article L. 851-2 et de la mise en œuvre de traitements automatisés sur les réseaux des opérateurs prévue à l'article L. 851-3) ;

- d'autre part, que les services de renseignement du second cercle, à la différence des services spécialisés de renseignement, ne peuvent pas mettre en œuvre la totalité des techniques de renseignement prévues par la loi, mais seulement celles auxquelles un décret en Conseil d'Etat leur donne accès et qui peuvent varier suivant les finalités poursuivies.

Pour autant, certaines situations opérationnelles peuvent justifier qu'un service de renseignement transmette à un autre service les renseignements recueillis alors même que ce

dernier n'aurait pu mettre en œuvre lui-même, pour la finalité justifiant que le renseignement lui soit transmis, la technique de recueil qui en a permis la collecte. Cette transmission, qui devra être dûment motivée, sera soumise à une autorisation du Premier ministre prise après avis de la CNCTR dans les conditions de forme et de procédure prévues aux articles L. 821-1 et L. 821-5.

Plusieurs autres garanties sont prévues pour garantir la nécessité et la proportionnalité des transmissions prévues par l'article 7 :

- la transmission d'un renseignement à un autre service est sans incidence sur sa durée de conservation, qui commence à courir à la date de son recueil, conformément aux dispositions de l'article L. 822-2. Chaque service, qu'il transmette ou qu'il soit destinataire d'un renseignement, devra veiller au respect de ces durées maximales de conservation et veiller à la destruction des renseignements qui lui ont été transmis ;

- chaque service de renseignement, qu'il transmette ou soit destinataire de renseignement, étant « responsable » de la destruction des renseignements au terme de leur durée légale de conservation, il est imposé un système de contrôle interne à chaque service, chargé de veiller au respect de ces règles. Ainsi, le projet prévoit la désignation par le responsable de chaque service de renseignement, pour assurer le respect de ces durées de conservation par les services destinataires, d'un agent chargé de veiller à ce que les renseignements recueillis par son service et transmis à un autre aient bien été détruits dans les conditions définies à l'article L. 822-4. Cet agent qui assure une traçabilité des transmissions, est informé de la destruction des renseignements ainsi transmis et peut rendre compte de toute difficulté dans l'application de cette disposition ;

- outre qu'elle est consultée pour avis avant que ne puisse être délivrée l'autorisation requise pour la transmission de certains renseignements, conformément au 2° du II de l'article L. 822-3, la CNCTR exerce un contrôle renforcé sur ces transmissions.

Ce contrôle comporte un volet « permanent » et un volet « en temps réel », explicités à l'article L. 822-4 :

- les opérations de destruction des renseignements collectés, leurs transcription et leurs extractions font l'objet de relevés tenus à la disposition de la CNCTR. Afin de garantir la traçabilité des échanges et les moyens de contrôle de la commission, il est proposé d'inclure parmi les opérations donnant lieu à de tels relevés, les transmissions de renseignements entre services, ces relevés devant préciser la nature, la date et la finalité des transmissions réalisées ainsi que le service destinataire. Par son accès permanent à ces relevés, la CNCTR sera ainsi informée sur les transmissions de renseignement entre services. Elle disposera également, dans les conditions fixées à l'article L. 854-9 du code de la sécurité intérieure, d'un accès permanent, complet et direct aux transmissions, comme pour les renseignements collectés, les transmissions et les extractions ;

- afin de permettre à la CNCTR d'exercer un contrôle en temps réel sur les opérations qui pourraient, le cas échéant, requérir son intervention rapide, l'article L. 822-4 est également modifié pour prévoir que, lorsque les transcriptions, extractions ou les transmissions poursuivent une finalité différentes de celle au titre de laquelle les renseignements ont été recueillis, les relevés qui font état de ces opérations sont immédiatement transmis à cette Commission.
- Le IV de l'article 7 prévoit, en modifiant à ce titre l'article L. 854-6, que les opérations de destruction des renseignements collectés par le biais de mesures de surveillance des communications internationales, leurs transcriptions, leurs extractions et leurs transmissions sont également soumises au même régime, fixé à l'article L. 822-4 du CSI.
- Enfin, est également modifié l'article L. 833-6, au V de l'article 7, permettant à la CNCTR d'adresser à tout moment au Premier ministre, au ministre responsable de son exécution et au service concerné une recommandation tendant à ce que les renseignements transmis soient détruits lorsqu'elle estime que leur transmission entre services a été effectuée en méconnaissance de l'article L. 822-3. La commission pourra tirer toutes les conséquences qui résulteraient de l'absence de suite donnée à ses recommandations en ce domaine, en saisissant la formation spécialisée du Conseil d'Etat afin que le juge des techniques de renseignements ordonne, s'il y a lieu, au service à l'origine d'une transmission irrégulière d'y mettre fin ou au service destinataire de supprimer les renseignements qu'il aurait irrégulièrement reçus.

3.2.2. S'agissant des transmissions d'informations par les autorités administratives aux services de renseignement (VI et VII)

Ces informations sont précieuses pour les services de renseignement qui peuvent solliciter les autorités administratives mentionnées à l'article L. 863-2 sur un dossier ponctuel ou bénéficier d'une transmission dont celles-ci auraient l'initiative. En effet, les services de renseignement sont en partie dépendants des informations qui leur sont transmises par d'autres administrations qui détectent des signaux faibles dans le cadre de leur activité. Il est possible de citer, à titre d'exemple, les signalements de radicalisation qui sont faits aux numéros verts dédiés, par les services sociaux, l'éducation nationale *etc.*

Les services de renseignement doivent en outre pouvoir solliciter les administrations pour accéder à des informations disponibles. *A contrario*, priver les services de renseignement de la possibilité de solliciter ou de recevoir des informations des autorités administratives reviendrait à les priver d'une partie des informations qui leur sont nécessaires pour l'accomplissement de leurs misions ou à les inciter à recourir à des techniques de renseignement non nécessaires. Cette possibilité s'articule donc avec le principe de nécessité et de proportionnalité du recours à la mise en œuvre d'une technique de renseignement.

Le VI de l'article 7 encadre davantage les conditions de ces transmissions :

- les informations sont adressées aux seuls services de renseignements ;

- les personnes destinataires de ces informations sont tenues au secret professionnel dans les conditions et sous les peines prévues aux articles 226-13 et 226-14 du code pénal ;
- les informations en cause peuvent, le cas échéant, être couvertes par l'un des secrets protégés par la loi ;
- elles doivent toutefois être strictement nécessaires à l'accomplissement des missions desdits services et la transmission doit concourir à la défense et la promotion des intérêts fondamentaux de la Nation, mentionnés à l'article L. 811-3 ;
- lorsque ces informations sont versées dans un traitement de données à caractère personnel, elles sont conservées dans les conditions applicables à ce traitement ;
- Les informations sont détruites dès lors qu'elles ne sont plus nécessaires à l'accomplissement des missions pour lesquelles elles ont été transmises ;
- une traçabilité des transmissions est organisée par chaque service destinataire, assurée par l'agent chargé de veiller au respect des durées de conservation des renseignements transmis entre services de renseignement, tel que prévu à l'article L. 822-3.

Il s'agira, *a priori*, du même agent qui devra, pour assurer la traçabilité sus-évoquée, mettre en place une organisation garantissant également la confidentialité des informations et l'habilitation des personnes permettant de les réceptionner.

Par voie de conséquence de la création de ce dispositif, le VII de l'article 7 supprime les dispositions de l'article 135 S du livre des procédures fiscales, qui fixent les modalités de transmission d'informations aux services de renseignement par l'administration fiscale, dont l'objet est, de facto, couverte par la nouvelle disposition créée.

Enfin, le VIII de l'article 7 prévoit la possibilité d'écarter partiellement le droit d'accès aux informations contenues dans un traitement de données personnelles d'une administration, s'agissant spécifiquement de l'information selon laquelle un service de renseignement a été rendu destinataire de données contenues dans le traitement. Cette dérogation vise à assurer la protection des modes opératoires des services de renseignement afin que les personnes concernées ne soient pas informées de ce qu'elles font l'objet d'un suivi par les services de renseignement.

Un décret en Conseil d'État est prévu pour l'application de cette mesure, afin de préciser les modalités particulières de ces transmissions. Son entrée en vigueur conditionnera l'abrogation de l'article L. 135 S du livre des procédures fiscales, lequel instaure, à la charge des seuls services de l'administration fiscale, un droit de communication au bénéfice des services de renseignements, aux fins de recherche et de prévention des atteintes aux intérêts fondamentaux de la Nation en matière de sécurité publique et de sûreté de l'État.

Dès lors que le VI de l'article 7 entrera en vigueur, cette disposition spéciale sera superfétatoire et son abrogation effective.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les articles L. 822-3, L. 822-4, L. 833-2, L. 833-6, L. 854-6, L. 863-2 du code de la sécurité intérieure, l'article L. 135 S du livre des procédures fiscales et les articles 48 et 49 de la loi n° 78-17 du 6 janvier 1978 sont modifiés.

Les transmissions de renseignement et d'informations prévues par l'article 10, compte tenu des garanties dont elles sont entourées et exposées *supra*, assurent une conciliation équilibrée entre les objectifs de sauvegarde des intérêts fondamentaux de la Nation et de prévention des atteintes à l'ordre public et des infractions, d'une part, et le droit au respect de la vie privée tel qu'il est garanti par les articles 2 et 4 de la Déclaration de 1789, d'autre part.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Dès lors que les finalités de sauvegarde des intérêts fondamentaux de la Nation qu'elles poursuivent, mentionnées à l'article L. 811-3 du code de la sécurité intérieure, concourent à la sécurité nationale, laquelle relève de la seule responsabilité des États membres en application de l'article 4 §2 du traité sur l'Union européenne, les dispositions relatives aux transmissions d'information entre services de renseignement et vers ces services échappent au droit de l'Union européenne.

Par ailleurs, compte tenu des garanties précédemment exposées, elles sont conformes aux exigences résultant de l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et de la jurisprudence de la Cour rappelée *supra*.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

4.2.1. S'agissant des transmissions de renseignements entre services

Conformément aux nouvelles dispositions de l'article L. 822-3 du code de la sécurité intérieure, chaque chef de service de renseignement mentionné à l'article L. 811-2 du code de la sécurité intérieure ou d'un service désigné par le décret en Conseil d'Etat prévu à l'article L. 811-4 du même code devra désigner un agent qui aura pour mission de contrôler la bonne application des modalités légales de transmission de renseignements entre services, et notamment de s'assurer de la destruction des renseignements transmis une fois leur durée de conservation dépassée. Pour s'en assurer, il devra mener des échanges avec ses homologues désignés dans les autres services de renseignement.

En outre, la rédaction des relevés visés par les dispositions de l'article L. 822-4 du code de la sécurité intérieure devra désormais intégrer les opérations de transmission des renseignements entre services effectuées sur le fondement du II de l'article L. 822-3.

4.2.2. S'agissant des transmissions d'informations des autorités administratives aux services de renseignements

La mise en œuvre de cette disposition exige, à l'instar des transmissions de renseignements entre services de renseignement, la mise en place d'une traçabilité des échanges, qui devra être assurée par l'agent chargé de veiller au respect des durées de conservation des renseignements transmis entre services de renseignement, tel que prévu à l'article L. 822-3.

Il s'agira, *a priori*, du même agent qui devra, pour assurer la traçabilité sus-évoquée, mettre en place une organisation garantissant également la confidentialité des échanges, lorsque les échanges entrent dans le champ d'un secret professionnel.

4.3. IMPACTS SUR LES PARTICULIERS

Les transmissions de renseignements entre services de renseignement, ou entre ces derniers et d'autres administrations de l'État, répondront à un cadre strict fixé par le législateur, garantissant une atteinte adaptée et proportionnée au droit au respect de la vie privée.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure qui a rendu son avis le 7 avril 2021.

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entrent en vigueur immédiatement, à l'exception de celles tenant aux transmissions d'informations des autorités administratives aux services de renseignements, dont un décret définit les modalités et de celles abrogeant l'article L. 135 S du livre des procédures fiscales, dont l'entrée en vigueur est subordonnée à l'intervention dudit décret.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

5.2.3. Texte d'application

Un décret en Conseil d'État est nécessaire.

Article 8 : Conservation de données pour les travaux de recherche et développement

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Les durées de conservation des renseignements recueillis sur le territoire national par l'une des techniques de recueil de renseignement prévue au livre VIII varient selon la nature de ces données. Ces durées sont précisées à l'article L. 822- 2 du code de la sécurité intérieure :

- 30 jours à compter de leur recueil pour les correspondances interceptées en application des articles L. 852-1 et L. 852-2 et pour les paroles captées en application de l'article L. 853-1 ;
- 120 jours à compter de leur recueil pour les renseignements collectés par la mise en œuvre des techniques mentionnées au chapitre III du titre V du présent livre, à l'exception des informations ou documents mentionnés à l'article L. 851-1. Sont concernées par cette durée les images dans un lieu privé en application de l'article L. 853-1 ainsi que les données informatiques recueillies en application de l'article L. 853-2 ;
- quatre ans à compter de leur recueil pour les informations ou documents mentionnés à l'article L. 851-1, c'est-à-dire les données de connexion.

Ces renseignements peuvent être conservés au-delà de ces durées pour trois motifs :

- aux fins de déchiffrement de renseignements chiffrés, le délai courant alors à compter de ce déchiffrement et la durée de conservation ne pouvant, en tout état de cause, excéder six ans ;
- aux fins d'analyse technique d'éléments de cyber-attaque ou d'éléments de chiffrement et à l'exclusion de toute utilisation pour la surveillance des personnes concernées ;
- pour les besoins de la procédure devant le Conseil d'État prévue à l'article L. 841-1 du code de la sécurité intérieure.

1.2. CADRE CONSTITUTIONNEL

Dans le cadre de son examen de la loi relative au renseignement de 2015 (23 juill. 2015, n° 2015-713), le Conseil constitutionnel a relevé « *qu'en prévoyant de telles durées de conservation en fonction des caractéristiques des renseignements collectés ainsi qu'une durée maximale de conservation de six ans à compter du recueil des données chiffrées, au-delà de laquelle les renseignements collectés doivent être détruits, le législateur n'a méconnu aucune exigence constitutionnelle* », avant de déclarer l'article L. 822-2 du code de la sécurité intérieure conforme à la Constitution.

Là encore, un régime de conservation de données relatives à des personnes doit être apprécié par le prisme du droit au respect de la vie privée, principe à valeur constitutionnelle que le Conseil constitutionnel tire de l'article 2 de la Déclaration de 1789. Il convient donc d'être particulièrement attentif d'une part, à la finalité poursuivie par l'atteinte portée à ce droit et, d'autre part, à la précision avec laquelle cette atteinte est encadrée et aux autres garanties qui l'entourent.

Ainsi un régime de conservation de données, institué dans un but légitime de développement des outils susceptibles de concourir à la protection des intérêts fondamentaux de la Nation, sera d'autant moins de nature à heurter le principe du respect du droit à la vie privée que les données en cause seront expurgées des éléments susceptibles d'apporter des précisions essentielles sur la vie privée des personnes.

1.3. CADRE CONVENTIONNEL

Le droit au respect de la vie privée et des correspondances est garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales.

La Cour européenne des droits de l'Homme considère que « *le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 (...). Peu importe que les informations mémorisées soient ou non utilisées par la suite (...). Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu [un aspect] de la vie privée (...), la Cour tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées,* ***de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés*** *(...).* » (CEDH, Gde Chambre, 4 déc. 2008, n° 30562/04). De même, la Cour a jugé que « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (...).Le droit interne doit notamment assurer que ces données soient pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées,* ***et qu'elles soient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées*** *(...). [Il] doit aussi contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (...)* ».

Il en résulte que le respect, par un régime de conservation de données (en l'occurrence de données de renseignement), des dispositions de l'article 8 de la l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, devra s'apprécier au regard de la circonstance que ces données ne sont conservées sous une forme permettant l'identification des personnes que tant qu'elles s'avèrent nécessaires aux finalités pour lesquelles elles ont été enregistrées (c'est, actuellement, le régime fixé par les dispositions

de l'article L. 822-2 du code de la sécurité intérieure). Mais, *a contrario*, la jurisprudence précitée autorise une conservation plus longue de ces données dès lors que celles-ci ont été modifiées pour en extraire les éléments susceptibles de porter atteinte à la vie privée des personnes (identification des personnes concernées) et que cette conservation est justifiée par les « *résultats qui peuvent en être tirés* » en terme, par exemple, de développement des outils concourant à préserver la sécurité des États.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La mise en œuvre des techniques de renseignement et le travail de transcription et d'extraction des renseignements pertinents nécessitent le recours à des dispositifs techniques ou informatiques particuliers. L'amélioration de ces dispositifs de collecte, d'extraction ou de transcription requiert souvent un travail de recherche et de développement conduit sur des données étroitement comparables à celles qui sont collectées *via* les techniques de renseignement : traitement d'enregistrement vocaux opérationnels, couverts volontairement ou non par des bruits de fond, d'images captées par un dispositif vidéo camouflé par exemple.

Or, les modèles d'apprentissage ont besoin de données pour s'entraîner avant d'être confrontés à des données inconnues. Plus les réseaux de neurones qui constituent ces modèles d'apprentissage disposent de données pertinentes, c'est-à-dire aussi proches que possible de celles obtenues dans un contexte opérationnel, pour apprendre, plus ils sont performants et précis, la quantité de données nécessaires à leur entraînement étant directement proportionnelle à la complexité du problème à résoudre. Ceci s'applique au traitement de l'image, de la parole, du texte, ou bien d'autres types de données plus ou moins structurées et hétérogènes, extraction des informations d'intérêt telles qu'un son, une conversation dans un environnement bruyant, l'accélération du traitement de la vidéo par l'élimination ou sélection de scènes sur requête sémantique.

Véritable freins technologiques, la collecte et la catégorisation des données nécessaires à la mise au point de ces techniques de recueil s'avèrent extrêmement chronophages et ralentissent le travail des équipes de recherche et développement.

Celles-ci se trouvent confrontées à une double difficulté du fait :

- de l'absence de possibilité de conservation, à des fins de recherche et de développement, des données issues des techniques de renseignement mises en œuvre dans les conditions prévues par le livre VIII du code de la sécurité intérieure ;
- des durées de conservation imposées par les dispositions des articles L. 822-2 du code de la sécurité intérieure et strictement encadrées.

Dès lors, il n'est pas possible de conserver des renseignements, même dépourvus de tout élément d'identification permettant de les rattacher aux objectifs au titre desquels ils ont été recueillis, à des fins de développement ou de formation.

2.2. OBJECTIFS POURSUIVIS

Le but des actions de recherche qui seraient mises en œuvre par les services de renseignement est l'optimisation d'une fonction mathématique à partir d'un jeu souvent très volumineux de données, qualifié de jeu d'apprentissage. Ces modèles d'apprentissage visent à améliorer les capacités d'analyse des services et à apporter une aide à l'enquêteur dans l'exploitation de volumes souvent conséquents de données collectées.

Lors de la phase d'entraînement, des données réalistes, tirées d'exemples opérationnels concrets, sont utiles voire indispensables pour construire des modèles d'apprentissage puis entraîner les capacités de recueil et d'exploitation.

A titre d'illustration, l'élaboration d'un traducteur automatique dans une paire de langues peu fréquente, comme l'albanais et le français, par exemple, nécessite le plus d'échantillons possibles.

Il en va de même pour un modèle qui permettrait d'éliminer les bruits parasites d'une bande son (bruits d'eau, de télévision, musique, *etc.*) : c'est à partir d'une masse importante de données les plus opérationnelles donc pertinentes que l'on pourra modéliser le bruit et ensuite l'éliminer sur les bandes sons afin de faciliter l'exploitation.

Les données d'entraînement étant coûteuses à produire, à annoter, à stocker, et demeurant, dans certains cas, peu nombreuses, il est indispensable de les conserver sur une longue durée : cela permet de pouvoir tester ou ré-entraîner les algorithmes régulièrement, de comparer la performance relative de plusieurs algorithmes, et de ne pas dupliquer les coûts lorsqu'un nouvel algorithme étalonné comme plus performant est disponible pour remplacer le précédent.

Cette activité de recherche doit demeurer entièrement distincte de l'activité de surveillance mise en œuvre par les services et à cette fin, les données qu'elle utilise ne doivent en aucune manière pouvoir être exploitées à des fins de renseignement. En tout état de cause, l'intérêt de ces données réside dans leur variété et leur nombre, permettant de constituer de manière rigoureuse des jeux d'apprentissage, puis de validation de ces modèles. Ne sont en revanche en rien pertinents pour la conduite d'actions de perfectionnement des techniques de recueil de renseignement, l'identité des personnes ou la possibilité de la retrouver, ni les finalités au titre desquelles les données utilisées pour ces actions ont été recueillies.

3. DISPOSITIF RETENU

La dérogation introduite par le nouveau III de l'article L. 822-2 du code de la sécurité intérieure est soumise à des restrictions de nature à garantir la parfaite étanchéité entre l'activité de recherche et toute action représentant, de manière directe ou indirecte, une surveillance individuelle. Elle autorise les seuls services de renseignements spécialisés mentionnés à l'article L. 811-2 du CSI à conserver pour une durée dérogatoire les données recueillies par des techniques de renseignement dans les conditions suivantes :

- ces données ne peuvent être conservées qu'aux seules fins de recherche et de développement en matière de capacités techniques de recueil et d'exploitation des renseignements et à l'exclusion de toute utilisation pour la surveillance des personnes concernées. Les données ainsi conservées ne pourront servir qu'à la constitution de modèles de connaissance, à leur apprentissage par les capacités techniques de recueil et d'exploitation et à leur validation ;

- eu égard à la finalité de leur conservation, ces données doivent être expurgées de tous les éléments qui ne concourent pas à cette finalité. Ainsi, les motifs et finalités ayant présidé à leur recueil, ainsi que les éléments permettant d'identifier les personnes concernées seront supprimés dès l'expiration de la durée normale de conservation des données, telle que prévue à l'article L. 822-2 ;

- ces données seront conservées de manière à ce qu'elles ne soient accessibles qu'à des agents spécialement habilités et exclusivement affectés aux missions de recherche et développement, sur un système d'information dédié et donc étanche par rapport à ceux qui contiennent des renseignements soumis aux agents individuellement désignés et habilités, en application de l'article L. 822-4, pour les exploiter. Les renseignements conservés aux fins de recherche et développement sont préalablement traités pour faire disparaître les finalités poursuivies lors de leur recueil et les éléments ou les conditions susceptibles d'identifier les personnes. Un registre devra nécessairement faire apparaître leur date de recueil, pour en assurer une destruction en tout état de cause cinq ans après cette date.

- ces données seront détruites dès qu'elles ne seront plus utiles à la finalité de recherche et développement qui a justifié leur conservation dans les conditions qui viennent d'être décrites, et en tout état de cause, au plus tard cinq ans après leur recueil.

- le respect des différentes conditions mises à cette conservation dérogatoire sera contrôlé par la Commission nationale de contrôle des techniques de renseignements, comme le prévoit le III de l'article 8 qui lui donne un accès permanent aux données ainsi conservées.

En outre, chaque programme de recherche sera subordonné à une autorisation du Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement, tout comme l'évolution substantielle d'un programme de recherche précédemment autorisé

La CNCTR exercera un contrôle permanent sur le respect de ces garanties en veillant à ce que la mise en œuvre des programmes de recherche soit conforme aux prescriptions qui leurs sont applicables. Si ce contrôle révèle qu'un programme ne respecte plus ces prescriptions, la

CNCTR pourra adresser au Premier ministre une recommandation tendant à la suspension dudit programme.

La possibilité offerte aux services de renseignement de solliciter l'autorisation de conduire un programme de recherche est également offerte au groupement interministériel de contrôle pour les données dont il organise la centralisation, soit parce qu'il est chargé de les recueillir (notamment les données de connexion recueillies auprès des opérateurs et fournisseurs de services de communications électroniques, en application du deuxième alinéa de l'article L. 851-2), soit parce qu'il est le lieu de leur exploitation (notamment en application du V de l'article L. 852-1).

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

L'article L. 822-2 est modifié et l'article L. 822-2-1 du code de la sécurité intérieure est créé.

La constitution de cette base de données répond à des seules fins de recherche et de développement, afin d'améliorer les capacités de recueil et d'exploitation des renseignements, grâce à la constitution de jeux d'apprentissage.

La suppression de tout élément permettant de relier les données ainsi traitées à l'objectif au titre desquelles elles ont été collectées, la durée de conservation limitée à cinq ans et la traçabilité des opérations, contrôlée à tout moment par la CNCTR constituent des garanties de nature à justifier d'une conciliation équilibrée entre l'objectif recherché et la protection des libertés.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'autorisation de conserver les données collectées dans le cadre des techniques de renseignement à des fins de recherche et développement améliorera la capacité des services de renseignement ainsi que du GIC à exploiter les données collectées et renforcera, à terme, leur efficacité.

4.3. IMPACTS SUR LES PARTICULIERS

Les données conservées et exploitées à des fins de recherche et développement ayant vocation à être anonymisées, cette mesure n'aura aucun impact sur les particuliers.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure qui a rendu son avis le 7 avril 2021.

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi renseignement, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 9 : Harmonisation des durées d'autorisation pour les techniques de recueil et de captation de données informatiques

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 853-2 du code de la sécurité intérieure opère une distinction entre la technique de recueil de données informatiques et celle de la captation de données informatiques.

La captation des données informatiques consiste en un dispositif technique permettant de capter en temps réel des flux de données émis ou reçus par des périphériques (écran, clavier, périphérique audiovisuel) ou des systèmes informatiques détenus par l'objectif.

Le recueil des données informatiques permet de collecter des données stockées dans un ou plusieurs systèmes informatiques utilisés par un objectif, le recueil étant opéré soit directement en accédant au support des données informatiques, soit à distances, au travers des réseaux informatiques. Dans tous les cas, cette technique nécessite une étude de faisabilité préalable et, le cas échéant, un processus d'accès au système informatique sur lequel les données vont être recueillies.

1.2. CADRE CONSTITUTIONNEL

Dans sa décision rendue sur la loi relative au renseignement de 2015 (décision n° 2015-713 DC du 23 juillet 2015), le Conseil constitutionnel, se prononçant sur la conformité à la Constitution des dispositions de l'article L. 853-2 du code de la sécurité intérieure, s'est borné à relever que « *que l'autorisation est délivrée pour une durée de deux mois ou de trente jours selon la technique utilisée* » sans que l'on puisse déduire de cette incise qu'une uniformisation de ces durées d'autorisation serait de nature à heurter un principe constitutionnel, notamment le droit au respect de la vie privée et l'inviolabilité du domicile.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Les durées d'autorisation de mise en œuvre de ces techniques de recueil de renseignements ne sont pas harmonisées : l'autorisation de mise en œuvre de la technique de captation des données informatiques est de 60 jours alors que celle de recueil des données informatiques n'est valable actuellement que 30 jours.

Cette différence est d'autant plus regrettable qu'une fois l'autorisation obtenue, la mise en œuvre effective de la technique de recueil de données informatiques nécessite une étude de faisabilité assez longue et sa réalisation effective, demeure aléatoire.

De manière générale, ces opérations nécessitent souvent plusieurs demandes à titre de renouvellement avant que la technique de renseignement puisse être effectivement mise en œuvre.

2.2. OBJECTIFS POURSUIVIS

En alignant la durée d'autorisation de la technique de recueil de données informatiques sur celle de la captation de données informatiques, soit deux mois, les services de renseignement disposeront ainsi d'une plus grande latitude pour effectuer les études de faisabilité et les ajustements techniques nécessaires à la mise en œuvre de la technique puis pour mettre en œuvre la technique d'un point de vue opérationnel. Cette évolution se révèle d'autant plus importante que cette technique est mise en œuvre pour atteindre des cibles particulièrement sensibles et qu'elle répond à un besoin qui ne peut, légalement, pouvoir être couvert par une autre technique autorisée par la loi.

Dans ces conditions, l'allongement proposé de la durée d'autorisation de mise en œuvre du recueil des données informatiques ne remet pas en cause, dans ces conditions, le caractère proportionné de l'atteinte portée au droit au respect de la vie privée. La mise en œuvre de ces techniques demeure en effet strictement encadrée, comme l'a relevé le Conseil constitutionnel :

- ces techniques ne peuvent être utilisées que pour les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure et uniquement si les renseignements recherchés ne peuvent être recueillis par un autre moyen légalement autorisé ;
- l'autorisation est délivrée pour une durée inférieure à la durée de droit commun de quatre mois prévue à l'article L. 821-4 du CSI ;
- le service autorisé à recourir à la technique de recueil de renseignement rend compte à la Commission nationale de contrôle des techniques de renseignement de sa mise en œuvre ;
- l'utilisation des dispositifs techniques et, le cas échéant, l'introduction dans un lieu privé ou un véhicule, ne peuvent être le fait que d'agents individuellement désignés et habilités appartenant à l'un des services mentionnés aux articles L. 811-2 et L. 811-4 et dont la liste est fixée par décret en Conseil d'État ;
- lorsque l'introduction dans un lieu privé ou dans un véhicule est nécessaire pour utiliser un dispositif technique permettant d'accéder à des données stockées dans un système informatique, l'autorisation ne peut être donnée qu'après avis exprès de la Commission nationale de contrôle des techniques de renseignement, statuant en formation restreinte ou plénière, excluant ainsi l'application de la procédure d'urgence prévue à l'article L. 821-5 ;
- lorsque cette introduction est autorisée après avis défavorable de la commission nationale de contrôle des techniques de renseignement et concerne un lieu privé à usage

d'habitation, le Conseil d'État est immédiatement saisi par le président de la commission ou par l'un des membres de celle-ci mentionnés aux 2° et 3° de l'article L. 831-1 ;

- dans ce dernier cas, sauf si l'autorisation d'introduction dans un lieu privé à usage d'habitation a été délivrée pour la prévention du terrorisme et que le Premier ministre a ordonné sa mise en œuvre immédiate, la décision d'autorisation ne peut être exécutée avant que le Conseil d'État ait statué.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Une fusion des deux techniques aurait pu être envisagée, les services pouvant alors, par une même autorisation, bénéficier de la possibilité de recueillir à la fois des données de stock et des données de flux, ce d'autant que la durée de conservation et d'exploitation des données applicable à ces deux techniques est identique et fixée à cent vingt-jours.

3.2. DISPOSITIF RETENU

Toutefois, dans un souci de proportionnalité, il a été fait le choix d'harmoniser les durées d'autorisation de mise en œuvre mais de maintenir la dualité des techniques, afin que les services restent dans l'obligation de motiver leur demande de recourir à l'une ou l'autre et puissent ne solliciter ou n'obtenir que la mise en œuvre de l'une d'elles.

Ainsi, la disposition prévoit que la durée d'autorisation de recueil des données informatiques est portée de 30 à 60 jours.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

L'article L. 853-2 du code de la sécurité intérieure est modifié.

Cette harmonisation des durées d'autorisation des techniques de recueil et de captation des données informatiques permettra aux services de renseignement de disposer d'un temps de préparation et de mise en œuvre identique pour les deux techniques qui, si elles diffèrent dans leur concrétisation technique, permettent, en tout état de cause, le recueil de données de même nature.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'allongement de la durée d'autorisation de la RDI assouplira les conditions de mise en œuvre de cette technique et réduira, en conséquence, la charge administrative afférente pour les services de renseignement concernés.

4.3. IMPACTS SUR LES PARTICULIERS

Le recueil, par les services de renseignement, de données sur les terminaux informatiques d'objectifs pourra être effectué sur une durée plus longue. L'atteinte au droit au respect de la vie privée ainsi qu'au secret des correspondances est donc susceptible d'être plus importante.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure qui a rendu son avis le 7 avril 2021.

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les dispositions s'appliqueront dès l'entrée en vigueur de la loi.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront, à l'instar de la loi renseignement, à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 10 : Extension des possibilités de réquisition des opérateurs télécom pour la mise en œuvre des techniques de renseignement et des techniques spéciales d'enquête

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Les articles L. 871-3 et L. 871-6 du code de la sécurité intérieure prévoient les conditions dans lesquelles l'autorité administrative peut requérir le concours des opérateurs de communications électroniques et des fournisseurs d'accès à Internet afin qu'ils réalisent, sur leurs réseaux, des opérations matérielles nécessaires à la mise en œuvre des techniques de renseignement autorisées par la loi et des interceptions de correspondances ordonnées par l'autorité judiciaires dans le cadre de procédures pénales.

En 2015, le législateur a limité les possibilités de réquisitions, pour les besoins des services de renseignement, à quatre techniques de renseignement :

- les demandes d'accès différé aux données de connexion, prévues à l'article L. 851-1 du CSI ;
- la technique de l'accès en temps réel aux données de connexion prévue par l'article L. 851-2 du CSI ;
- la technique de détection d'une menace terroriste sur la base de traitements automatisés, dite technique de l'algorithme, prévue par l'article L. 851-3 du CSI ;
- les interceptions de sécurité prévues à l'article L. 852-1 du CSI.

Par ailleurs, en se bornant à codifier une disposition de la loi du 10 juillet 1991 relative au secret des correspondances, l'article L. 871-3 n'a pas opéré de coordination avec les techniques d'enquêtes apparues entretemps dans le code de procédure pénale, ni *a fortiori* depuis la loi de 2015.

L'article L. 33-1 du code des postes et communications électroniques prévoit que « *l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur : (…) e) Les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre et celles qui sont nécessaires pour répondre, conformément aux orientations fixées par l'autorité nationale de défense des systèmes d'informations, aux menaces et aux atteintes à la sécurité des systèmes d'information des autorités publiques et des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense* ; »

La coopération des opérateurs pour la réalisation de ces opérations matérielles est requise par le Premier ministre, ou par toute personne désignée par lui. S'agissant des interceptions judiciaires, elle est requise par le ministre en charge des communications électroniques. En raison de la confidentialité inhérente à la réalisation de ces opérations, il est prévu que ces opérations ne peuvent être réalisées que par des agents qualifiés de ces opérateurs ou fournisseurs.

L'article L. 871-7 du code de la sécurité intérieure prévoit que les coûts engendrés par ces réquisitions pour les opérateurs de communications électroniques font l'objet d'une compensation financière par l'État

1.2. CADRE CONSTITUTIONNEL

S'il ne s'est pas prononcé à ce jour sur les dispositions des articles L. 871-3 et L. 871-6 du code de la sécurité intérieure, le Conseil constitutionnel a déjà eu plusieurs fois à connaître de dispositions imposant, pour des motifs d'intérêt général, des obligations à des acteurs économiques.

À cet égard, il considère, de manière constante, que s'il « *est loisible au législateur d'apporter à [la] liberté [d'entreprendre] des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi* ».

S'agissant plus spécifiquement des opérateurs de communications électroniques et des fournisseurs d'accès à internet, le Conseil constitutionnel a eu l'occasion de considérer que les intérêts de la défense et de la sécurité nationale pouvaient justifier des atteintes à la liberté d'entreprendre. Ainsi, très récemment, dans sa décision n° 2020-882 QPC du 5 février 2021, il a estimé qu'en imposant un régime d'autorisation pour l'exploitation, par les opérateurs d'importance vitale, des équipements de réseaux 5G, le législateur s'était attaché à mettre « *en œuvre les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* » et n'avait, au regard des conditions strictes entourant ce régime d'autorisation, pas porté d'atteinte disproportionnée à la liberté d'entreprendre au regard de l'objectif poursuivi. Il a, à cet égard, notamment relevé un champ d'application de l'obligation strictement circonscrit et des conditions de mise en œuvre précisément définies par le législateur.

Lorsqu'elles engendrent des coûts, le Conseil constitutionnel examine également les obligations légales imposées à des acteurs privés à la lumière du principe d'égalité devant les charges publiques, qui résulte de l'article 13 de la Déclaration de 1789 selon lequel « *pour l'entretien de la force publique, et pour les dépenses d'administration, une contribution commune est indispensable : elle doit être également répartie entre tous les citoyens, en raison de leurs facultés* ».

En dehors du domaine fiscal, le Conseil constitutionnel juge de façon constante que « *si cet article n'interdit pas de faire supporter, pour un motif d'intérêt général, à certaines catégories*

de personnes des charges particulières, il ne doit pas en résulter de rupture caractérisée de l'égalité devant les charges publiques »[28].

Appelé à se prononcer sur des dispositions imposant aux opérateurs de réseaux de télécommunication de supporter le coût de fonctionnement de dispositifs d'interceptions de sécurité, qui auparavant étaient remboursés par l'État, il a, dans sa décision n° 2001-441 DC du 28 décembre 2000, jugé que « *s'il est loisible au législateur, dans le respect des libertés constitutionnellement garanties, d'imposer aux opérateurs de réseaux de télécommunications de mettre en place et de faire fonctionner les dispositifs techniques permettant les interceptions justifiées par les nécessités de la sécurité publique, le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt général de la population, est étranger à l'exploitation des réseaux de télécommunications ; que les dépenses en résultant ne sauraient dès lors, en raison de leur nature, incomber directement aux opérateurs* ».

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

L'assistance des opérateurs de communications électroniques ou des fournisseurs d'accès à internet ne se limite pas aux cas actuellement couverts par les articles L. 871-3 et L. 871-6 du code de la sécurité intérieure, dont le champ d'application défini par le législateur en 2015 se révèle, en pratique, insuffisant pour couvrir l'ensemble des situations opérationnelles.

Une modification de la loi apparaît dès lors nécessaire pour permettre à l'autorité administrative de requérir l'assistance des opérateurs pour la mise en œuvre des techniques de renseignement visées aux articles L. 851-6 et L. 853-2 du même code, d'une part, et aux techniques spéciales d'enquête prévues par le code de procédure pénale, d'autre part. En effet, les contraintes techniques exposées relatives au recueil de données techniques de connexion et des interceptions de correspondances émises par la voie des communications électroniques sont les mêmes en matière judiciaire qu'en matière renseignement.

3. DISPOSITIF RETENU

Le dispositif retenu vise à étendre le champ d'application des articles L. 871-3 et L. 871-6 du code de la sécurité intérieure, afin d'ajouter au champ des techniques pour lesquelles l'assistance des opérateurs de communications électroniques et des fournisseurs d'accès à internet peut être requise par l'autorité administrative :

- en matière de renseignement, les techniques de recueil ou de captation des données informatiques visées à l'article L. 853-2 du code de la sécurité intérieure ainsi que la technique de recueil des données techniques de connexion par le biais d'un dispositif de

[28] Voir décision n° 2019-821 QPC du 24 janvier 2020, Société nationale d'exploitation industrielle des tabacs et allumettes.

captation de proximité de type *Imsi-catching*[29], prévue par l'article L. 851-6 du même code. Il s'agit notamment d'anticiper le déploiement de la 5G (communications mobiles de 5e génération), qui aura pour conséquence que les identifiants des terminaux mobiles deviendront temporaires, évolueront à une fréquence élevée, et seront donnés par le réseau. Seul l'opérateur pourra établir le lien entre ces identifiants temporaires et les identifiants pérennes des abonnements ou des équipements terminaux utilisés. Il sera donc nécessaire, pour que la technique de l'IMSI-catcher visée à l'article L. 851-6 du code de la sécurité intérieure conserve un intérêt opérationnel, de pouvoir obtenir des opérateurs de communications électroniques le lien entre ces deux types d'identifiants ;

- en matière judiciaire, les techniques de recueil de données informatiques visées aux articles 706-95 à 706-102-5 du code de procédure pénale. Outre les interceptions de communication, ces techniques correspondent à l'accès à distance aux correspondances stockées par la voie des communications électroniques, et au recueil de données techniques de connexion et des interceptions de correspondances émises par la voie des communications électroniques de type IMSI-catching.

Par voie de conséquence, le dispositif retenu prévoit de compléter l'article L. 871-7 du code de la sécurité intérieure afin de prévoir une compensation financière pour les opérateurs de communications électroniques et les fournisseurs d'accès à internet dont l'assistance serait requise dans le cadre de la mise en œuvre de ces techniques de renseignement.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Les articles L. 871-3, L. 871-6 et L. 871-7 sont modifiés.

L'article 4 paragraphe 2 du Traité sur l'Union européenne prévoit que l'Union respecte les fonctions essentielles de l'Etat et que la sécurité nationale reste de la seule responsabilité de chaque Etat membre. A ce titre, le droit de l'Union européenne n'a pas vocation à régir les conditions dans lesquelles le Premier ministre requiert une assistance des opérateurs de communications électroniques ou des fournisseurs d'accès à internet pour la mise en œuvre des techniques de recueil de renseignement, *a fortiori* lorsque cette assistance ne nécessite ni conservation de données ni transmission de données par ces opérateurs.

[29] Les dispositifs d'Imsi-catching fonctionnent comme une antenne relais mobile factice, imposant aux terminaux mobiles situés dans son périmètre de se connecter à elle. La différence entre les deux techniques, qui empruntent le même dispositif technique, porte sur la nature des données collectées : l'article L. 852-1 porte sur une interception de correspondances c'est-à-dire le contenu des communications et l'article L. 851-6 porte sur les seules données de connexion, autrement dit les métadonnées.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

Les coûts engendrés par ces dispositions pour les opérateurs de communications électroniques et les fournisseurs d'accès à internet feront l'objet d'une compensation par l'Etat, dans des conditions définies par arrêté, à l'instar de la pratique déjà mise en œuvre pour les opérateurs.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure qui a rendu son avis le 7 avril 2021.

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

Cette disposition a été présentée, conformément à L. 36-5 du code des postes et communications électroniques, à l'autorité de régulation des communications électroniques, des postes et de la distribution de la pressequi a rendu son avis le 16 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entrent en vigueur immédiatement.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

5.2.3. Textes d'application

Les conditions de compensation financière par l'État des obligations complémentaires imposées aux opérateurs en application de l'article L. 871-7 modifié seront définies par arrêté.

Article 11 : Expérimentation d'une technique d'interception des communications empruntant la voie satellitaire

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 852-1 du code de la sécurité intérieure autorise, pour l'ensemble des finalités mentionnées à l'article L. 811-3, les interceptions de correspondance émises par la voie des communications électroniques, plus communément appelées interceptions de sécurité.

Ouvertes à l'ensemble des services spécialisés de renseignement mentionnés à l'article L. 811-2 ainsi qu'à certains des services mentionnés à l'article L. 811-4, ces interceptions font l'objet, conformément aux articles L. 821-1 et suivants du code, d'une autorisation du Premier ministre, prise après avis de la Commission nationale de contrôle des techniques de renseignement, qui est délivrée pour une durée de quatre mois, renouvelable dans les mêmes conditions.

Les opérations d'interceptions ne sont pas mises en œuvre directement par les services demandeurs, mais sont assurées par un service du Premier ministre, le Groupement interministériel de contrôle (GIC), qui bénéficie de l'exclusivité de la relation avec les opérateurs de communications électroniques et les fournisseurs de services sur Internet. Les opérations de transcription et d'extractions des communications interceptées sont également réalisées en son sein.

Les opérateurs de communications électroniques sont astreints, pour la mise en œuvre des interceptions de sécurité, à un certain nombre d'obligations.

L'article L. 33-1 du code des postes et des communications électroniques prévoit ainsi que « *l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur […] les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique* ». L'article D. 98-7, III, du même code précise que les opérateurs de communications électroniques sont chargés d'assurer la mise en œuvre des moyens nécessaires à l'application des dispositions relatives aux interceptions de sécurité. Ces moyens doivent respecter un certain nombre de conditions : ils doivent ainsi être mis en place sur le territoire national et ne peuvent être mis en œuvre à partir d'un pays étranger ; lorsque les données produites transitent en dehors du territoire national, elles doivent être chiffrées, par un moyen validé par l'Etat français ; enfin, les interceptions de sécurité ne peuvent être mises en œuvre que par des agents qualifiés, au sens des dispositions de l'article R. 872-1 du code de la sécurité intérieure, c'est-à-dire habilités à connaître d'éléments couverts par le secret de la défense nationale et n'ayant fait l'objet d'aucune condamnation pénale inscrite au bulletin n° 2 de leur casier judiciaire. Il peut être dérogé à ces obligations, sur décision du ministre chargé des

communications électroniques, « *lorsque des obstacles techniques le justifient ou lorsque les coûts à exposer pour satisfaire à ces conditions sont disproportionnés au regard du nombre d'interceptions susceptibles d'être demandées à cet opérateur* ».

Sur le fondement de ces dispositions, l'article L. 42-1 du même code prévoit que « *L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse attribue l'autorisation d'utilisation des fréquences radioélectriques dans des conditions objectives, transparentes et non discriminatoires tenant compte des besoins d'aménagement du territoire. Cette autorisation ne peut être refusée par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse que pour l'un des motifs suivants :*

> *1° La sauvegarde de l'ordre public ou de la sécurité publique ;*
> *2° La bonne utilisation des fréquences ;*
> *3° L'incapacité technique ou financière du demandeur à faire face durablement aux obligations résultant des conditions d'exercice de son activité ;*
> *4° La condamnation du demandeur à l'une des sanctions mentionnées aux articles L. 36-11, L. 39, L. 39-1, L. 39-1-1 et L. 39-4.*

L'ensemble de ces dispositions devrait permettre de s'assurer de la coopération des opérateurs de communication électroniques, dans la plupart des cas.

Il est toutefois possible que dans certains cas, les opérateurs proposent des services commerciaux sur le territoire français sans y disposer d'installation sur le territoire national, sous couvert d'une autorisation délivrée par un autre État. En pareil cas, l'ARCEP ne disposera d'aucun moyen de coercition à leur encontre s'ils ne donnent pas suite à une réquisition. Par ailleurs, à supposer même que ces opérateurs soient situés sur le territoire national, les exigences de protection du secret de la défense nationale pourront, dans certaines hypothèses tenant par exemple à leur nationalité, être incompatibles avec leur intervention.

Les services de renseignement se trouveraient alors dans l'impossibilité d'obtenir la mise en œuvre d'interceptions de sécurité sur des cibles recourant aux communications électroniques par voie satellitaire. Or, ainsi qu'il est expliqué au point 2., il convient d'anticiper une bascule d'une partie peut-être significative des communications électroniques de la voie terrestre à la voie satellitaire.

Parallèlement aux interceptions de sécurité prévues au I de l'article L. 852-1 du code de la sécurité intérieure, la loi du 24 juillet 2015 relative au renseignement a également autorisé les services de renseignement à procéder à des **interceptions de correspondances par le biais d'un appareil ou d'un dispositif technique de proximité (« *Imsi-catcher* »).** Prévue par le II du même article L. 852-1 du code de la sécurité intérieure, cette technique consiste à collecter les communications dans une zone relativement circonscrite par le biais d'un appareil se comportant comme une antenne relais mobile factice se substituant, dans un périmètre donné, aux antennes relais des opérateurs, et permettant, ce faisant, aux services de capter les données transitant sur les terminaux qui s'y sont connectés.

Pensée pour répondre à des situations d'urgence opérationnelle, cette technique est strictement encadrée par la loi. Elle ne peut ainsi être autorisée, par le Premier ministre après avis de la CNCTR, pour une durée supérieure à quarante-huit heures. Elle ne peut, par ailleurs, être mise en œuvre que pour trois finalités : la protection de l'indépendance nationale, de l'intégrité du territoire et de la défense nationale (1° de l'article L. 811-3 du CSI) ; la prévention du terrorisme (4° du même article) ; la prévention des atteintes à la forme républicaine des institutions (5° *a* du même article). Si la technique du II de l'article L. 852-1 offre la possibilité de réaliser une interception sans adresser de réquisition à l'opérateur concerné, elle ne peut donc constituer une alternative aux difficultés décrites ci-dessus. Elle n'a pratiquement jamais été mise en œuvre depuis l'entrée en vigueur de la loi du 24 juillet 2015.

1.2. CADRE CONSTITUTIONNEL

Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel a déclaré conformes à la Constitution l'ensemble des dispositions prévues à l'article L. 852-1 du code de la sécurité intérieure.

Il a estimé que ces dispositions opéraient une conciliation qui n'était manifestement pas déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public, et, d'autre part, le droit au respect de la vie privée et le secret des correspondances, au regard d'un faisceau de garanties.

S'agissant des interceptions de sécurité mentionnées au I de cet article, le Conseil constitutionnel a notamment relevé :

- la mise en place d'un contingentement du nombre d'interception, fixé par le Premier ministre après avis de la CNCTR ;

- la centralisation de l'exécution des interceptions par un service du Premier ministre (GIC) ;

- une durée de conservation des correspondances interceptées limitée à 30 jours.

En ce qui concerne le II du même article L. 852-1, le Conseil constitutionnel a en outre fait état de conditions strictes de mises en œuvre, relevant dans sa décision :

- un recours limité à certaines finalités seulement, « *relatives à la prévention d'atteintes particulièrement graves à l'ordre public* » ;

- une obligation de destruction des correspondances interceptées sans lien avec l'autorisation délivrée, et au plus tard 30 jours à compter du recueil.

1.3. CADRE EUROPEEN

La Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales admet, de façon constante depuis son arrêt Klass et autres c. Allemagne (n° 5029/71, 6 septembre 1978), que les services de renseignement étatiques puissent se munir de moyens de surveiller les individus pour faire face à des menaces pouvant mettre en péril une société démocratique. Les mesures prises à cet égard, qui peuvent concerner un grand nombre de données ne portent ainsi pas, par nature, une atteinte disproportionnée au droit à la vie privée protégée par l'article 8 de la Convention.

Dans son arrêt Weber et Saravia c. Allemagne (n° 54934/00, 29 juin 2006, § 95), la Cour a exposé les principes généraux à l'aune desquels une mesure de surveillance secrète doit être appréciée pour déterminer si elle est ou pas conforme aux exigences de l'article 8 § 2 de la Convention, à savoir : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

Encore résiduels il y a encore quelques années, les moyens de communication par voie satellitaire tendent à se développer à l'échelle internationale, sous l'impact de la mise en orbite de plusieurs constellations satellitaires dits de basse altitude offrant des possibilités de communications mobiles identiques à celles des réseaux de communications terrestres.

D'ores et déjà, il est constaté des **usages de ces nouveaux moyens de communication sur le territoire national**, dont une fraction est liée à des activités criminelles ou de nature à porter atteinte aux intérêts fondamentaux de la Nation. À ce jour, les services sont ainsi en mesure de **détecter l'utilisation, sur le territoire national, de plusieurs centaines de boîtiers satellitaires**, pour lesquels il existe des raisons sérieuses de penser qu'ils sont, au moins pour partie, utilisés par des individus dont les activités sont de nature à porter atteinte aux intérêts fondamentaux de la Nation. Ces détections sont évidemment loin d'être exhaustives et ne correspondent qu'aux utilisations détectées par les moyens actuels des services de renseignement.

Le déploiement annoncé, d'ici à 2025, de nouvelles constellations satellitaires d'ampleur portées par des entreprises étrangères laisse à penser que ces usages devraient aller croissants et se banaliser au cours des prochaines années. Parmi les projets visant le grand public actuellement en cours de déploiement peuvent notamment être cités :

- le projet Starlink a été initié par la société SpaceX, avec pour ambition d'offrir au grand public une offre d'accès Internet, sur une couverture mondiale. La mise en

service initiale est prévue pour la fin de l'année 2021 au Canada et le nord des Etats-Unis, avec une montée en puissance progressive sur l'ensemble du globe jusqu'à 2025 ;

- le projet Oneweb, dont la mise en service est annoncée pour 2022 et devrait comporter 648 satellites ;

- enfin, la société Amazon a également initié un projet de déploiement satellitaire qui devrait être mis en service à horizon 2026 et comporter, à terme, 3 236 satellites.

A relativement court terme, il existera une offre complète de télécommunications transitant par la voie satellitaire, qui plus est à des tarifs avantageux, qui pourrait être de nature à concurrencer les offres des opérateurs de communications électroniques traditionnels empruntant le réseau terrestre.

Cette évolution significative des modes de communication pose, pour les services de renseignement, un **enjeu majeur de préservation de leurs capacités techniques de surveillance**.

Dans un premier temps, des individus ou des groupes se livrant à des activités criminelles pourraient se tourner vers ces nouveaux moyens de communication afin d'échapper à la surveillance. À terme, avec la démocratisation des terminaux satellitaires, les services de renseignement risquent de se trouver dans l'incapacité d'intercepter une partie importante des communications émises ou reçues depuis le territoire national.

Plusieurs caractéristiques des réseaux de communications par satellite rendent l'interception sur le territoire national difficilement appréhendable par le droit en vigueur.

Bien que les opérateurs de communications par satellite soient, en droit, assimilables à tout opérateur de communications électroniques au sens du code des postes et des communications électroniques et soient donc soumis aux obligations fixées par ce code et rappelées au point 1, se pose, en pratique, l'effectivité de ce cadre légal, fait aujourd'hui, les concernant, l'objet d'interrogations pour trois séries de raisons.

En premier lieu, les constellations satellitaires actuelles, de même que les constellations en cours de déploiement, sont à ce jour toutes exploitées par des opérateurs étrangers[30], qui ne disposent le plus souvent pas de représentant légal sur le territoire national et se révèlent, dès lors, plus difficiles à réquisitionner au titre de la loi renseignement. La mise en œuvre des réquisitions légales à leur endroit serait ainsi incertaine ou difficile

En deuxième lieu, à supposer même qu'un opérateur étranger défère à une réquisition délivrée par l'autorité administrative tendant à la mise en œuvre d'interceptions de sécurité, cela ne serait pas sans soulever une problématique de confidentialité dans la mesure où elle conduirait, à droit

constant, à révéler à une entreprise étrangère l'identité de certains des objectifs suivis par les services de renseignement français.

En troisième lieu, les protocoles de communication entre le satellite et les terminaux ne garantissent pas, à l'heure actuelle, qu'il sera toujours possible de disposer d'un identifiant précis dont l'interception des communications pourra être demandé

A cet égard, il convient en outre d'observer que l'exploitation d'un réseau satellitaire en France n'imposant pas toujours techniquement l'installation d'équipements sur le territoire national, la plupart des opérateurs satellitaires actuels sont en mesure d'offrir un service sur le territoire français sans pour autant respecter strictement les exigences fixées aux articles L. 33-1 et D. 98-7 du code des postes et des communications électroniques. Or, ces conditions sont celles qui assurent non seulement la disponibilité des opérateurs pour répondre aux réquisitions de l'autorité administrative pour la mise en œuvre d'une interception légale, mais aussi le respect d'un niveau satisfaisant de confidentialité.

A ce stade, il faut donc envisager que les conditions permettant la mise en œuvre du I de l'article L. 852-1 ne seront pas réunies dans nombre de cas. Or, la loi actuelle n'offre aucun cadre alternatif qui permettrait de pallier cette grave lacune si une partie importante des communications devaient, demain, transiter par la voie satellitaire, puisque la technique d'interceptions *via* un dispositif de proximité (II de l'article L. 851-2 du code de la sécurité intérieure) ne permet pas de répondre au besoin identifié, dès lors que les conditions entourant sa mise en œuvre, en particulier la limitation de la durée d'autorisation à 48 heures, se révèlent en pratique trop restrictives pour permettre son déploiement par les services de renseignement. En outre, la limitation à seulement trois finalités ne permettrait pas de couvrir l'ensemble des besoins identifiés, en particulier en matière de lutte contre la criminalité organisée.

Dans ces conditions, la modification du cadre légal apparaît nécessaire pour permettre aux services de renseignement de préserver, à moyen terme, leurs capacités de surveillance technique sur le territoire national, en les autorisant à intercepter les correspondances transitant par la voie satellitaire, au même titre que par les autres voies de communications électroniques aujourd'hui couvertes par le droit.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

1) Il aurait pu être envisagé de modifier ou d'élargir les conditions d'application des techniques de recueil de renseignement autorisées par le I de l'article L. 852-1 du code de la sécurité intérieure, afin d'y inclure les besoins spécifiques liés à la captation des communications satellitaires.

Cependant, en raison d'une part, des difficultés susmentionnées liées à la réquisition d'opérateurs étrangers et, d'autre part, des difficultés techniques propres aux communications

satellitaires limitant les possibilités de procéder à des interceptions ciblées sur un élément technique, l'extension de la technique prévue au I de cet article est apparue inadaptée au besoin identifié.

2) De la même manière, a été écartée l'option consistant à assouplir les critères de mise en œuvre de la technique autorisée par le II du même article L. 852-1, bien qu'elle se rapproche le plus, sur le plan technique, du besoin identifié. Pour l'interception de communications satellitaires, le recours à un dispositif de captation de proximité ne constitue pas, contrairement à l'interception des communications empruntant les réseaux terrestres, une alternative à la réquisition, mais bien l'unique option technique à ce jour envisageable eu égard aux caractéristiques propres de ces nouveaux moyens de communication. Aussi est-il apparu préférable de privilégier la création d'un cadre légal adapté répondant à des critères de mise en œuvre propres.

3) S'agissant enfin des critères de mise en œuvre de l'expérimentation proposée, plusieurs solutions ont été écartées.

Il aurait tout d'abord pu être décidé de n'ouvrir cette nouvelle technique qu'aux seuls services spécialisés de renseignement. Une telle limitation est toutefois apparue contradictoire avec l'objectif même de la modification législative envisagée, qui consiste non pas à ajouter un nouvel outil à l'arsenal des services de renseignement, mais uniquement à combler le déficit opérationnel qui pourrait résulter du changement technologique induit par l'émergence des terminaux de communications satellitaires. Dans ces conditions, les services appartenant au second cercle du renseignement étant également susceptibles de pâtir du déport de certaines communications vers les moyens satellitaires, il est indispensable que leur soit également ouverte la possibilité de recourir à cette technique, étant observé que, à la fois pour des questions de coût et des questions de technicité, la mise en œuvre effective des interceptions sera opérée par les services du premier cercle. Par ailleurs, elle sera contingentée.

En effet, la seule circonstance que le service demandeur de la mise en œuvre d'une telle technique soit un service du second cercle ne paraît pas de nature à majorer l'atteinte à la vie privée, dès lors que l'ensemble des opérations postérieures à la demande sont prises en charge par les services du premier cercle (pour la captation) et par le GIC (pour la centralisation, le tri et la suppression des informations sans lien avec la cible, le service demandeur ne pouvant exploiter en retour que des informations concernant sa cible.

Par ailleurs, a été écartée **l'option qui aurait consisté à proposer une expérimentation de courte durée, inférieure à quatre ans**. En l'espèce, une durée technique suffisamment longue apparaît en effet nécessaire :

- d'une part, en raison du délai nécessaire à la définition des conditions techniques de mise en œuvre de la technique, qui pourra nécessiter plusieurs mois après la promulgation de la loi ;

- d'autre part, du déploiement de nouvelles constellations satellitaires d'ici à 2025, dont le fonctionnement est à ce stade inconnu. Il importe que la période d'expérimentation laisse le temps aux services de conduire de premiers tests sur ces nouvelles constellations, ce que ne permettrait pas une durée inférieure à 4 ans.

3.2. DISPOSITIF RETENU

Le dispositif retenu consiste à créer une nouvelle modalité d'interception de correspondances qui serait mise en œuvre directement à l'aide d'un dispositif ou d'un appareil de captation, sans que l'opérateur ne réponde à une réquisition d'interception. Une telle modalité est en effet celle qui répond le mieux, techniquement, au besoin identifié pour les communications satellitaires, dès lors qu'elle autorise une captation tactique de l'ensemble des communications transitant sur une zone, aux fins d'identifier les communications de la cible surveillée.

Le dispositif n'ajoute pas un nouvel outil à l'arsenal existant, mais a pour seul objectif de compenser la perte opérationnelle qui pourrait résulter de l'évolution des moyens de communications électroniques, avec deux objectifs :

- d'une part, donner un cadre légal à des besoins opérationnels identifiés par les services de renseignement qui, s'ils ne sont pas encore majoritaires, n'en présentent pas moins un intérêt opérationnel fort. Dans la plupart des cas identifiés, il s'agit de pouvoir poursuivre, sur le territoire national, une surveillance initiée dans le cadre de la surveillance internationale sur les constellations satellitaires existantes, ce qui n'est pas possible dans le cadre légal actuel ;

- d'autre part, se préparer, sur le plan technique, à l'émergence de nouvelles constellations satellitaires qui pourraient, à terme, supplanter, pour partie, le recours aux moyens de communications électroniques classiques. Face à un monde des communications électroniques en pleine évolution, il est indispensable que les services de renseignement se mettent en situation de pouvoir répondre aux besoins opérationnels liés au déploiement engagé de nouvelles constellations satellitaires.

Cette nouvelle technique d'interception serait ouverte à quatre finalités prévues à l'article L. 811-3 du même code : l'indépendance nationale, l'intégrité du territoire et la défense nationale (1°), la prévention du terrorisme (4°), la promotion et la défense des intérêts majeurs de la politique étrangère, de l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère (2°), la lutte contre la criminalité et la délinquance organisées (6°)

Par ailleurs, la technique serait ouverte à l'ensemble des services de renseignement, y compris aux services du second cercle, dont la liste sera définie par décret en Conseil d'État. Le fait que le service demandeur soit un service du premier ou du second cercle est neutre en termes d'atteinte à la vie privée et au secret des correspondances. A cet égard, il peut être observé que l'ouverture à l'ensemble des services ne préjuge en rien d'éventuelles coopérations techniques

qui pourront par la suite être mises en œuvre, par exemple afin qu'une assistance technique soit apportée, par les services relevant du premier cercle, aux services du second cercle. De telles mutualisations, qui sont d'ores et déjà pratiquées pour d'autres techniques de renseignement, permettent de faire bénéficier tous les services de l'expertise de ceux qui sont les plus avancés sur certaines techniques et de mutualiser des investissements coûteux.

De plus, cette technique pourrait être autorisée pour une durée de 30 jours renouvelable, contre 4 mois pour les interceptions de sécurité de droit commun. L'autorisation délivrée vaudrait également autorisation de recueil des données de connexion.

En contrepartie, sa mise en œuvre répondrait à des garanties strictes :

- contrairement à la technique prévue par le II de l'article L. 852-1 du code de la sécurité intérieure, qui vise des cas qui pourraient être couverts par une interception de sécurité réalisée par l'intermédiaire d'un opérateur, le nouveau cas d'usage répondrait à **un principe de subsidiarité** et ne pourrait être mis en œuvre que lorsque l'interception de correspondances ne peut être réalisée par le biais de la réquisition d'un opérateur. Dans la pratique, l'impossibilité de réquisitionner un opérateur pourra recouvrir deux situations : soit des situations d'impossibilité technique, lorsque l'opérateur ne dispose d'aucun représentant légal ni d'aucun équipement sur le territoire national permettant de procéder à une interception, ou ne répond pas à la réquisition qui lui est adressée par l'autorité administrative ; soit des situations dans lesquelles l'interception ne peut être mise en œuvre dans des conditions de confidentialité satisfaisantes.

- Si, pour des raisons opérationnelles et tactiques, les opérations de captation seront réalisées par les services de renseignement, il est prévu une **centralisation au GIC des communications interceptées**. Cette centralisation devra être mise en place dès le stade de l'interception. Il est toutefois maintenu la possibilité de procéder à cette centralisation de manière différée, afin de couvrir les situations d'impossibilité technique faisant obstacle à un transfert des flux d'interceptions vers les locaux du GIC. Dans cette dernière hypothèse, les flux de données feront l'objet d'un chiffrement asymétrique, dont seul le GIC aura la clé, le temps qu'il soit procédé à la centralisation desdites données ;

- à l'instar des interceptions de sécurité, **les opérations d'extraction et de transcription des correspondances interceptées ne pourront être mises en œuvre qu'au sein et sous le contrôle du GIC et les données seront conservées pour un maximum de 30 jours** ;

- à l'instar des interceptions de sécurité, **un contingentement serait imposé à ces techniques**, fixé par arrêté du Premier ministre pris après avis de la CNCTR ;

- enfin, les correspondances interceptées sans lien avec la personne faisant l'objet de l'autorisation de mise en œuvre de cette technique seraient **détruites, au plus tard**

30 jours à compter de leur recueil. En effet, lors de l'interception des communications entre des terminaux et les satellites par un dispositif tactique, il ne sera pas techniquement possible dans certains cas de discriminer les seules communications du terminal utilisé par la personne désignée dans l'autorisation du Premier ministre. Le GIC procèdera donc à la destruction, le plus tôt possible et en tout état de cause, dans un délai de 30 jours, des communications interceptées n'appartenant pas à la personne désignée, étant précisé que dans tous les cas, le service demandeur ne disposera, *in fine*, que des renseignements concernant la personne faisant l'objet de l'autorisation.

La liste des services de renseignement autorisés à mettre en œuvre cette technique est renvoyée à un décret en Conseil d'État, pris après avis de la CNCTR.

Compte tenu des incertitudes qui pèsent encore sur l'évolution de l'environnement technologique, il est proposé de n'ouvrir cette nouvelle technique qu'à titre temporaire, pour une durée de quatre ans à compter de l'entrée en vigueur du projet de loi. Cette phase permettra d'une part, aux services de renseignement de tester et d'expérimenter de nouvelles capacités techniques et, d'autre part, de s'adapter aux nouvelles constellations satellitaires qui seront déployées.

Une durée suffisamment longue est nécessaire pour permettre d'évaluer techniquement l'efficacité du dispositif légal adopté, en particulier compte tenu des évolutions importantes à venir du secteur des communications satellitaires.

C'est également la raison pour laquelle toute limitation de la technique à certains services, constituerait une perte opérationnelle pour les services, pendant toute la durée de l'expérimentation, avec de réels risques de contournement immédiat de la part des individus ayant le projet de porter atteinte aux intérêts fondamentaux de la Nation.

Six mois avant l'échéance de la disposition, un rapport d'évaluation sera remis au Parlement. Le cas échéant, selon la confidentialité des données de l'évaluation, une partie du rapport sera remis à la délégation parlementaire au renseignement, habilitée à connaître d'éléments relevant du secret de la défense nationale.

L'évaluation s'attachera à apprécier l'utilité, sur le plan opérationnel, de la technique créée ainsi que la pertinence des conditions de sa mise en œuvre, telles que prévues par le nouvel article L. 852-3 du code de la sécurité intérieure, notamment au regard de l'évolution observée des moyens de communications satellitaires. Ces éléments pourront être appréciés au vu de plusieurs critères, parmi lesquels :

- le nombre d'interceptions effectivement autorisées et mises en œuvre sur le fondement du nouvel article L. 852-3 du code de la sécurité intérieure, par service et par finalité ;

l'évaluation des obstacles juridiques, techniques ou opérationnels, ayant empêché le recours au régime des interceptions de sécurité de droit commun du I de l'article L. 852-1 du même code ;

- le nombre de communications interceptées sans rapport avec la cible visée par le biais des capteurs déployés ;

- l'évaluation des conditions techniques de centralisation au GIC, en particulier le nombre de techniques pour lesquelles cette centralisation, pour des raisons techniques, a dû être opérée de manière différée, avec mise en place d'un chiffrement.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Un nouvel article L. 852-3 est créé au code de la sécurité intérieure et l'article L. 822-2 est modifié.

4.2. IMPACTS SUR LES ADMINISTRATIONS

Le lancement de l'expérimentation n'aura pas d'incident directe sur les effectifs des services de renseignement qui seront autorisés à mettre en œuvre la technique créée.

4.3. IMPACTS SUR LES FINANCES PUBLIQUES

Le lancement de l'expérimentation rend nécessaire l'acquisition, par les services de renseignement, de nouveaux équipements adaptés à la captation de communications satellitaires, dont le coût dépendra de l'évolution de l'environnement technique et du déploiement de nouvelles constellations au cours des années à venir.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Le projet de loi a été présenté à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure. La Commission a rendu son avis le 15 avril 2021.

Cette disposition a été présentée, conformément à L. 36-5 du code des postes et communications électroniques, à l'autorité de régulation des communications électroniques, des postes et de la distribution de la pressequi a rendu son avis le 16 avril 2021.

Cette disposition a été présentée, à titre facultatif, à la Commission nationale informatique et liberté qui a rendu son avis le 15 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions s'appliqueront dès le lendemain de la publication de la loi au Journal officiel de la République française.

5.2.2. Application dans l'espace

Elles sont d'application immédiate sur l'ensemble du territoire français.

5.2.3. Textes d'application

L'établissement de la liste des services de renseignement autorisés à mettre en œuvre cette expérimentation sera précisé par un décret en Conseil d'Etat, pris après avis de la CNCTR.

Article 12 : Pérennisation des dispositions relatives à l'algorithme

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 851-3 du code de la sécurité intérieure, créé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, ouvre la possibilité d'imposer la mise en place, sur les réseaux des opérateurs de communications électroniques et des fournisseurs de services sur internet, de traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste, plus communément appelés algorithmes, sans qu'il soit possible de procéder, dans un premier temps, à l'identification des personnes concernées. Ce n'est que lorsque la menace est avérée que le Premier ministre peut, après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), autoriser l'identification de la personne en cause et le recueil des données de connexion afférentes.

Cet article est applicable jusqu'au 31 décembre 2021, conformément aux dispositions modifiées de l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, le Gouvernement devant adresser au Parlement un nouveau rapport sur l'application de cette disposition, au plus tard le 30 juin 2021.

Contrairement aux autres techniques de renseignement (balisage, captations de paroles et d'images…) qui lui préexistaient à la loi de 2015 et dont le législateur a encadré les conditions de mise en œuvre, la technique de l'algorithme n'avait pas encore été mise au point ; c'est d'ailleurs pourquoi une période d'expérimentation a été exigée par le législateur.

A la suite de la promulgation de la loi du 24 juillet 2015, le groupement interministériel de contrôle (GIC), en liaison avec la direction générale de la sécurité intérieure (DGSI) et la direction générale de la sécurité extérieure (DGSE), a ainsi examiné plusieurs options possibles d'exécution des algorithmes, sous le contrôle permanent de la Commission nationale de contrôle des techniques de renseignement (CNCTR).

Ces travaux visaient à garantir le bon fonctionnement du dispositif et à élaborer une architecture technique préservant l'intérêt opérationnel de l'outil de détection prévu à l'article L. 851-3 du CSI. Deux facteurs conditionnent l'efficacité du dispositif :

- les paramètres d'alerte doivent être définis de manière suffisamment précise pour répondre au besoin opérationnel de détection de données susceptibles de caractériser l'existence d'une menace terroriste. Des paramètres trop restrictifs aboutiraient en effet à un nombre quasi nul d'alertes produites par les traitements automatisés ; des critères trop larges contribueraient au contraire à de nombreux « hits » sans intérêt opérationnel pour les services, avec le risque de ne pas être en capacité de traiter l'ensemble des alertes et de passer à côté d'une menace réelle. L'objectif des services est bien de minimiser le nombre d'alertes ;

– la qualité des données traitées par les algorithmes est essentielle. Pour construire leurs algorithmes, les services de renseignement se sont appuyés sur des éléments recueillis lors de leurs investigations relatives à des faits de terrorisme ou à des opérations militaires à l'étranger qui leur ont permis de comprendre quels étaient les événements télécom caractéristiques d'une activité terroriste ou de la préparation d'une telle activité.

La modalité initialement envisagée pour mettre en œuvre la technique des algorithmes consistait à placer physiquement les dispositifs techniques de détection en plusieurs points des réseaux des opérateurs. Au sein de chaque dispositif, des algorithmes se seraient exécutés sur les flux de données de connexion en transit sur chacun de ces points. Les investigations conduites au cours de la phase d'expérimentation ont cependant montré que cette modalité aurait conduit à une impasse pour plusieurs raisons pratiques.

La principale d'entre elles tient au fait que positionner des traitements algorithmiques au sein des réseaux des opérateurs présente le risque de perturber la sécurité de ces réseaux.

Par ailleurs, les cibles terroristes utilisent des moyens de communication discrets et se dissimulent sur les réseaux en utilisant plusieurs abonnements, des adresses fictives ou des « téléphones de guerre », potentiellement chez de multiples opérateurs. Certains algorithmes ayant vocation à être configurés pour détecter une séquence d'événements de communication, chaque dispositif de détection aurait dû être relié avec tous les autres pour pouvoir communiquer avec eux afin de détecter efficacement des successions d'événements de connexion susceptibles de révéler une menace terroriste.

Enfin, les algorithmes peuvent avoir, parmi leurs paramètres de détection, des identifiants particuliers issus de techniques ou d'activités de renseignement, y compris de services partenaires. Ces données et paramètres de détection, qui revêtent une sensibilité particulière, doivent être utilisés par les algorithmes mais dans des conditions garantissant une stricte confidentialité.

Au terme d'une réflexion conduite en concertation avec les opérateurs de communications électroniques, le Gouvernement a donc opté pour une modalité d'exécution centralisée des algorithmes, qui permet :

- de garantir aux opérateurs que l'exécution de ces derniers ne perturbe pas les services de communications électroniques qu'ils offrent à leurs abonnés ;

- de simplifier considérablement l'architecture technique en évitant de recourir à une exécution répartie entre plusieurs points relevant d'opérateurs différents ;

- de limiter considérablement les délais de réalisation ;

- de limiter le risque de compromission des paramètres de détection utilisés par les algorithmes.

Le Gouvernement a communiqué à la CNCTR une description détaillée de l'architecture envisagée. La Commission a rendu un avis favorable en 2016, estimant que la proposition selon laquelle les flux de données de connexion étaient dupliqués chez les opérateurs puis acheminés pour être soumis à des dispositifs de détection centralisés était une interprétation permise par la lettre de la loi, les opérations de sélection, duplication, acheminement des données puis d'exécution des algorithmes constituant des traitements dont la mise en œuvre est imposée aux opérateurs sur leurs réseaux.

La CNCTR a cependant rappelé que l'objet de la technique de l'algorithme était d'agir à la manière d'un tamis sur les flux de données de connexion, de sorte qu'il ne permettait aucune conservation des données autre que strictement nécessaire à la détection de successions d'événements de télécommunication traduisant la séquence révélatrice d'une menace terroriste que l'algorithme a été configuré pour détecter. Elle a par ailleurs subordonné son avis favorable à deux conditions :

- d'une part, le dispositif centralisé de détection algorithmique devait être placé sous la seule responsabilité du GIC, chargé de garantir l'étanchéité de ce dispositif vis-à-vis des services de renseignement ;

- d'autre part, le Gouvernement devait clarifier devant le Parlement l'option finalement retenue pour la mise en œuvre de l'article L. 851-3 du code de la sécurité intérieure.

Les deux conditions ont été remplies préalablement à la mise en œuvre du premier algorithme fin 2017 :

- le GIC est seul habilité à exécuter les algorithmes, dans les conditions définies par la loi, sous le contrôle de la CNCTR qui « *dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies* » (II de l'article L. 851-3). Il est le seul destinataire des alertes automatiques et c'est lui seul qui, après nouvelle autorisation, remet au service de renseignement les données qui ont déclenché l'alerte. Aucun service de renseignement ne peut accéder aux données soumises aux traitements automatisés ; les seules données susceptibles de leur être transmises sont celles qui ont donné lieu à une alerte de la part d'un algorithme autorisé par une première décision du Premier ministre, prononcée en application du I de l'article L. 851-3 et dont l'anonymat est levé par une seconde décision du Premier ministre, prononcée en application du IV du même article ;

- une description du dispositif retenu et les raisons qui ont présidé à son choix ont été communiquées à la Délégation parlementaire au renseignement.

Le dispositif a finalement été mis en œuvre fin 2017, après avis favorable de la CNCTR. Trois algorithmes ont été autorisés depuis lors par le Premier ministre ; ils avaient préalablement fait l'objet d'un avis favorable de la CNCTR. Le paramétrage des algorithmes, placé sous le contrôle de la CNCTR, a permis de contenir la fréquence des alertes tout en maintenant un seuil de détection utile : le nombre d'alertes issues des trois algorithmes autorisés s'est ainsi élevé à

1739 pour l'année 2020. Ces alertes ont donné lieu à autant de levées d'anonymat sur le fondement du IV de l'article L. 851-3, systématiquement effectuées après avis favorable de la CNCTR.

L'expérimentation de cette technique innovante expirait le 31 décembre 2018. Elle a néanmoins été prorogée au 31 décembre 2020 par la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, afin de donner le temps aux services de mesurer les apports opérationnels des algorithmes, dont le premier n'était en service que depuis la fin de l'année 2017. Elle a été à nouveau prorogée 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, cette fois en raison des circonstances sanitaires exceptionnelles résultant de l'épidémie de COVID-19.

Le Gouvernement doit adresser au Parlement un nouveau rapport sur l'application de cette disposition, au plus tard le 30 juin 2021. Celui-ci contribuera à démontrer que ce dispositif s'avère indispensable pour permettre de détecter des individus inconnus des services de renseignement ou que leurs comportements antérieurs n'avaient jusqu'ici pas permis d'identifier comme menaçants, dans un contexte de persistance de la menace terroriste.

Comme l'illustrent les attaques ou projets d'attaques terroristes récents, la menace terroriste endogène demeure élevée et présente un caractère particulièrement diffus et évolutif. Elle se nourrit et s'inspire d'une propagande terroriste toujours très présente et relayée sur les réseaux numériques. L'accès à cette propagande est particulièrement aisé et le recours aux moyens de communications numériques favorise en outre des contacts à distance d'individus radicalisés avec des réseaux ou groupes terroristes, ainsi qu'un passage à l'acte rapide difficilement détectable par les autres moyens à la disposition des services spécialisés.

S'il n'est pas possible de détailler les résultats obtenus au moyen de ces algorithmes, qui sont protégés au titre de la protection du secret de la défense nationale, conformément à l'article 413-9 du code pénal, il peut néanmoins être mentionné que ces algorithmes ont notamment permis :

- d'identifier des individus porteurs d'une menace à caractère terroriste et de détecter des contacts entre les individus porteurs de menace ;
- d'obtenir des informations sur la localisation d'individus en lien avec cette menace ;
- de mettre à jour des comportements d'individus connus des services de renseignement et nécessitant des investigations plus approfondies ;
- d'améliorer la connaissance des services sur la manière de procéder des individus de la mouvance terroriste.

L'apport de ce dispositif est donc majeur dans la lutte contre le terrorisme.

1.2. CADRE CONSTITUTIONNEL

Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel a déclaré conformes à la Constitution les dispositions de l'article L. 851-3 du code de la sécurité intérieure.

Il a estimé que ces dispositions ne portaient pas une atteinte disproportionnée au droit au respect de la vie privée au regard de l'existence de nombreuses garanties :

- l'existence d'une autorisation du Premier ministre délivrée sur demande écrite et motivée d'un ministre ;
- l'obligation de solliciter un avis préalable d'une autorité administrative indépendante, dotée en outre de prérogatives de contrôle ;
- l'existence d'une voie de recours spéciale devant le Conseil d'Etat, ouverte à la CNCTR comme à toute personne souhaitant vérifier que la technique n'a pas été irrégulièrement mise en œuvre à son encontre.

Le Conseil constitutionnel a également relevé que :

- cette technique ne peut être mise en œuvre qu'aux fins de prévention du terrorisme ;
- la première autorisation est délivrée pour une durée limitée à deux mois renouvelable dans le cadre d'une demande comportant un relevé du nombre d'identifiants techniques signalés par le traitement automatisé et une analyse de la pertinence de ces signalements ;
- cette technique utilise exclusivement les informations ou documents mentionnés à l'article L. 851-1 du code de la sécurité intérieure 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 ;
- l'identification de la ou des personnes dont les données ont été détectées par l'algorithme ne peut intervenir qu'après qu'une nouvelle autorisation a été délivrée par le Premier ministre après avis de la Commission, permettant d'exploiter les données recueillies dans un délai maximal de soixante jours avant destruction des données sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste.

Le caractère expérimental de la mesure n'est donc pas au nombre des caractéristiques qui garantissent sa conformité à la Constitution.

1.3. CADRE EUROPEEN

➢ *Droit de l'Union européenne*

Dans un arrêt La Quadrature du Net E.A. du 6 octobre 2020, la Cour de justice de l'Union européenne (CJUE) a jugé que la Charte des droits fondamentaux de l'Union européenne ne s'oppose pas à la mise en œuvre de la technique de recueil de renseignement mentionnée à l'article L. 851-3 du code de la sécurité intérieure dès lors qu'elle est « *limitée 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* » et sous réserve qu'elle « [*fasse] 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 ».

Dans sa décision en date du 21 avril 2021, qui tire les conséquences de cet arrêt (Ass., French Data Network et autres, n° 393099), l'assemblée du Conseil d'État a confirmé que l'article L. 851-3 du code de la sécurité intérieure et les décrets pris pour son application ne méconnaissaient le droit de l'Union européenne qu'en tant seulement qu'ils permettent la mise en œuvre de traitements automatisés sans prévoir, avant l'identification des personnes dont les données sont susceptibles de révéler une menace à caractère terroriste, un contrôle préalable par une juridiction ou par une autorité administrative dotée d'un pouvoir contraignant. Si, comme pour toutes les techniques de renseignement, l'identification des personnes détectées par le biais d'un algorithme ne peut être mis en œuvre qu'après l'avis d'un organisme de contrôle indépendant, la CNCTR, celui-ci n'est en effet pas contraignant pour le Premier ministre. L'article 16 du présent projet en tire les conséquences, en apportant à la loi les modifications qui s'imposent sur ce point.

La décision du Conseil d'État reconnaît en revanche que les autres exigences posées par la Cour sont satisfaites par le droit en vigueur ainsi que par les modifications que le présent projet de loi entend y apporter, observant à cet égard que l'algorithme ne peut être mis en œuvre que pour les seuls besoins de la prévention du terrorisme et que la Commission nationale de contrôle des techniques de renseignement, chargée d'émettre un avis préalable à la mise en œuvre de la technique, « *vérifie l'existence et l'actualité de la menace grave pour la sécurité nationale susceptible de justifier une telle mesure* ».

> ➢ *Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales*

La Cour de Strasbourg admet, de façon constante depuis son arrêt *Klass et autres c. Allemagne* (n° 5029/71, 6 septembre 1978), que les services de renseignement des États puissent se munir de moyens de surveiller les individus pour faire face à des menaces pouvant mettre en péril une société démocratique. Les mesures prises à cet égard, qui peuvent concerner un grand nombre de données ne portent ainsi pas, par nature, une atteinte disproportionnée au droit à la vie privée protégée par l'article 8 de la Convention.

Dans son arrêt *Weber et Saravia c. Allemagne* (n° 54934/00, 29 juin 2006, § 95), la Cour a exposé les principes généraux à l'aune desquels une mesure de surveillance secrète doit être appréciée pour déterminer si elle est ou pas conforme aux exigences de l'article 8 § 2 de la Convention : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.

La Cour a fait application de ces critères à un système d'interception généralisée des communications dans son arrêt de grande chambre, req. n° 47143/06, 4 décembre 2015, *Zakharov c. Russie*, § 227 s.) : elle y déduit de l'article 8 de la Convention qu'une ingérence dans ce droit ne peut se justifier que si :

- elle est prévue par la loi, c'est-à-dire qu'elle doit avoir une base en droit interne et être compatible avec la prééminence du droit ; elle doit être accessible à la personne concernée, prévisible quant à ses effets et assurer une protection adéquate contre l'arbitraire ;
- elle doit viser un ou plusieurs des buts légitimes énumérés à l'article 8§2 et être nécessaire, dans une société démocratique, pour atteindre ce ou ces buts.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

En matière de renseignement, la technique de recueil de renseignement prévue à l'article L. 851-3 du code de sécurité intérieure, dite « algorithme », a été instaurée à titre d'expérimentation pour une durée limitée par l'article 25 modifié de la loi n° 2015-912 du 24 juillet 2015, qui arrive à son terme le 31 décembre 2021.

La technique mentionnée à l'article L. 851-3 répond à un besoin essentiel de détection précoce de la menace terroriste. L'un des enjeux les plus cruciaux de l'activité de renseignement consiste en effet à être en mesure de détecter une nouvelle menace, dont les auteurs et les modes opératoires ne sont pas connus et ne peuvent par définition faire l'objet d'une surveillance ciblée *a priori*, afin de la caractériser et de l'évaluer. Ce besoin est particulièrement prégnant en matière de lutte contre le terrorisme pour deux raisons.

En premier lieu, du fait du caractère diffus et très évolutif de la menace terroriste. Les dispositifs de nature algorithmique visent ainsi à repérer et discriminer sur les réseaux de communications électroniques des données caractéristiques de comportements typiques d'organisations et de cellules terroristes, afin de repérer des menaces et d'engager, le cas échéant, des mesures de surveillance individuelle aussi précisément ciblées qu'il est possible. Les algorithmes sont conçus à partir d'éléments recueillis au cours d'enquêtes menées en France ou à l'étranger sur des faits de terrorisme ou d'opérations militaires conduites à l'étranger qui permettent, notamment à l'occasion de saisies d'ordinateurs, de découvrir des modes particuliers de communication qui constituent une « signature » caractéristique de ces groupes terroristes (ex : comportement caractéristique d'une diffusion de propagande djihadiste). Par exemple, lorsqu'un terroriste se livre à des exactions dans un pays étranger, des connexions se mettent en place sur notre territoire, pour identifier les réseaux sociaux qui montrent la scène. Un algorithme peut permettre de vérifier immédiatement les connexions qui assurent la diffusion de l'acte terroriste commis à l'étranger.

En second lieu, la nécessité de disposer d'un outil de détection est directement liée à l'apparition de nouveaux comportements, à la faveur notamment de la diffusion informatique d'une vaste propagande terroriste et de l'émergence de nouveaux moyens de communication électroniques.

Les actions terroristes sont ainsi, de plus en plus, le fait d'individus qui s'inspirent des messages de propagande qui émanent des organisations terroristes, incitant au passage à l'acte en fournissant les tutoriels pour leur réalisation, mais qui ne sont pas entrés en contact visible ou direct avec des organisations, réseaux ou groupes terroristes, échappant ainsi à toute capacité de détection par le biais d'une surveillance ciblée. En effet, si le maillage territorial des services de renseignement et de police ainsi que la sensibilisation des différents acteurs administratifs et sociaux permettent de détecter une évolution du comportement social d'un individu susceptible de révéler l'existence d'une menace terroriste, cette capacité disparaît lorsque ces indices n'apparaissent que par l'activité numérique de la personne.

La mise en œuvre des mesures autorisées par ces dispositions est donc essentielle, tant en matière d'entrave pour prévenir les actes de terrorisme, ainsi que le démontrent les rapports détaillés adressés chaque année au Parlement, qu'en matière de renseignement. **C'est pour l'ensemble de ces motifs qu'une pérennisation du dispositif apparaît nécessaire.**

3. DISPOSITIF RETENU

Le dispositif prévu à l'article L. 851-3 du code de la sécurité intérieure ayant déjà vu sa date d'échéance repoussée, et son utilité opérationnelle étant indéniable, l'option consistant à proroger une nouvelle fois ce dispositif pour une durée déterminée a été écartée au profit d'une pérennisation du dispositif, afin de conforter durablement l'action des services de renseignement.

Cette pérennisation est proportionnée, au regard des conditions entourant la mise en œuvre de cette technique et des garanties nouvelles qui sont apportées.

En premier lieu, les algorithmes **ne permettent en aucun cas** aux services de renseignement d'accéder à l'ensemble des données des réseaux des opérateurs.

Ce dispositif de détection vise, au contraire, à discriminer sur les données des opérateurs celles de nature à révéler un risque de nature terroriste afin d'orienter de la manière la plus ciblée possible l'activité de surveillance, par la mise en œuvre subséquente d'une technique permettant aux services d'accéder aux données d'un individu détecté par l'algorithme. Le service demandeur conçoit ainsi l'algorithme en fonction du comportement qu'il sait ou suppose être celui des individus porteurs de la menace qu'il cherche à détecter. Ce comportement est modélisé informatiquement : cela signifie que le service définit des paramètres techniques caractérisant le comportement recherché et reposant sur la seule analyse des données de connexion. L'objectif du service est que l'algorithme soit le plus discriminant possible afin d'éviter au maximum qu'il produise des faux positifs. En effet, un trop grand nombre de faux positifs remettrait en cause l'utilité de l'algorithme, qui vise à orienter au mieux l'action des services et à éviter la mobilisation de leurs moyens en vain.

En deuxième lieu, les garanties procédurales qui entourent la mise en œuvre de l'algorithme sont particulièrement fortes.

Les paramètres de détection sont contrôlés par la CNCTR, autorité administrative indépendante. La Commission s'assure notamment que les paramètres retenus correspondent précisément à la finalité annoncée par le service et que la demande de mise en œuvre de l'algorithme est motivée de manière détaillée et circonstanciée. Concrètement, les ingénieurs de la CNCTR analysent le code de l'algorithme dans le détail. L'autorisation le cas échéant délivrée l'est pour une période limitée à deux mois. Par ailleurs, toute modification de l'algorithme nécessite un nouvel examen de la part de la Commission préalablement à sa mise en œuvre.

Si l'algorithme fait l'objet d'une demande de renouvellement, les services sont légalement obligés d'indiquer dans leur demande le nombre d'alertes produites par l'algorithme. Ils doivent également transmettre à la CNCTR une analyse de la pertinence de ces alertes.

Pendant la durée de validité de l'autorisation (deux mois pour la demande initiale, quatre mois en cas de renouvellement de l'autorisation), les services de renseignement ne peuvent à aucun moment accéder aux données des opérateurs.

En cas d'alerte, le service de renseignement concerné est simplement averti, sans qu'aucune autre information ne lui soit transmise. Il doit alors former une nouvelle demande motivée pour que le Premier ministre permette, après avis de la CNCTR, que lui soit transmis l'identifiant technique lié à l'alerte.

Le service de renseignement effectue alors généralement une demande d'identification de l'utilisateur de l'identifiant signalé en sollicitant la mise en œuvre de la technique prévue à l'article L. 851-1 du CSI. Si cette première démarche confirme le caractère crédible de la détection, le service pourra poursuivre ses investigations en se soumettant à toutes les obligations matérielles et procédurales prévues par la loi pour la mise en œuvre d'une technique de recueil de renseignement.

Seules les données relatives aux personnes dont la mise sous surveillance est précisément justifiée seront donc conservées. Toutes les autres données seront immédiatement détruites.

La mise en œuvre de ces traitements automatisés permet donc aux services de renseignement de procéder par levée de doute, de la manière la moins intrusive possible, et de ne solliciter ensuite la mise en œuvre de mesures de surveillance individuelle que si le besoin en est avéré.

Enfin, la pérennisation de la technique de l'algorithme s'accompagnera de plusieurs garanties nouvelles (cf. article 13 du projet de loi), résultant des enseignements tirés de l'expérimentation et qui viennent renforcer la proportionnalité du dispositif :

- la mise en œuvre des traitements ne pourra plus être sollicitée que par les seuls services spécialisés de renseignement,
- la possibilité de proroger la durée de conservation des données correspondant aux paramètres de détection et dont le Premier ministre autorise le recueil est supprimée. En l'état de la loi, cette durée est fixée à soixante jours mais peut être prolongée, en cas d'éléments sérieux confirmant l'existence d'une menace terroriste, jusqu'à quatre ans. L'expérimentation a fait apparaître qu'une telle prolongation n'est pas nécessaire, dès

lors que le délai normal de soixante jours permet, en tout état de cause, de solliciter la mise en œuvre d'une technique de renseignement ciblée sur la personne à laquelle se rapporte les données détectées par les traitements ;

– un service du Premier ministre, distinct des services de renseignement, sera seul habilité à exécuter, à la demande des services, les traitements autorisés. Cette mission incombera au groupement interministériel de contrôle, service à compétence nationale doté de compétences juridiques et d'effectifs déjà chargés de veiller de manière centralisée à la mise en œuvre des traitements dans les conditions définies par la loi, sous le contrôle de la CNCTR.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGÉES

4.1. IMPACTS JURIDIQUES

L'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement est abrogé.

Une telle pérennisation ne remet pas en cause la constitutionnalité de l'article L. 851-3 du code de la sécurité intérieure, telle qu'elle a été reconnue par le Conseil constitutionnel dans sa décision n° 2015-713 DC précitée. Celle-ci, en effet, n'a tenu aucun compte du fait que ces dispositions avaient été adoptées pour une durée limitée pour les déclarer conformes à la Constitution (considérant 60).

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services de renseignement continueront, avec le GIC et sous le contrôle de la Commission nationale de contrôle des techniques de renseignement, à mettre en œuvre ce dispositif, dans les mêmes conditions que celles actuellement en vigueur.

4.3. IMPACTS SUR LES PARTICULIERS

Le dispositif prévu à l'article L. 851-3 du CSI a pour finalité de détecter un comportement susceptible de constituer une menace de nature terroriste. L'identification de la ou des personnes dont les données ont été détectées par l'algorithme ne peut intervenir que dans un second temps, à l'issue d'une nouvelle autorisation délivrée par le Premier Ministre après avis de la CNCTR. Compte-tenu, entre autres, de cette garantie, le Conseil constitutionnel a considéré que cette disposition ne portait pas une atteinte disproportionnée au droit au respect de la vie privée.

5. CONSULATION ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure qui a rendu son avis le 7 avril 2021.

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

Cette disposition a été présentée, conformément à L. 36-5 du code des postes et communications électroniques, à l'autorité de régulation des communications électroniques, des postes et de la distribution de la presse qui a rendu son avis le 16 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article qui a pour conséquence de pérenniser la possibilité de mise en œuvre de la technique de renseignement prévue par l'article L. 851-3 du code de la sécurité intérieure entrera en vigueur au lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions envisagées s'appliqueront à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 13 : Modalités d'exécution des traitements automatisés et extension aux adresses complètes de ressources sur internet (URL)

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Comme évoqué dans les développements relatifs à l'article 12 du projet de loi, la technique de l'algorithme, prévue par l'article L. 851-3 du code de la sécurité intérieure, permet la mise en place, sur les réseaux des opérateurs de communications électroniques et des fournisseurs de services sur internet, de traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste. Il s'agit particulièrement de contribuer à la détection d'individus inconnus des services de renseignement ou que leurs comportements antérieurs n'avaient jusqu'ici pas permis d'identifier comme menaçants.

Ces traitements ne peuvent utiliser que les informations ou documents mentionnés à l'article L. 851-1 du code de la sécurité intérieure, c'est-à-dire les données de connexion, à l'exclusion de toute donnée révélant le contenu des communications. L'article L. 34-1 du code des postes et des communications électroniques (CPCE) relatif au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques donne une définition en creux des données de connexion en excluant la conservation des données portant sur le contenu des correspondances échangées ou des informations consultées. Cette définition en creux est reprise à l'article R. 851-5 du CSI qui prévoit que « *les informations ou documents mentionnés à l'article L. 851-1 sont, à l'exclusion du contenu des correspondances échangées ou des informations consultées : (...)* ».

1.2. CADRE CONSTITUTIONNEL

Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel a déclaré conformes à la Constitution les dispositions de l'article L. 851-3 du code de la sécurité intérieure (voir développements à l'article 12).

Il précisait explicitement (cons. 55) « *que selon les dispositions du paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques, les données conservées et traitées par les opérateurs de communications électroniques et les personnes offrant au public une connexion permettant une telle communication 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 et 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* ». Selon le Conseil constitutionnel, c'est donc le renvoi à l'article L. 34-1 du CPCE (qui pourtant n'est opéré par le L. 851-1 du CSI que pour identifier « les personnes »

mentionnées par cet article) qui exclut de la catégorie des « données de connexion » le contenu des correspondances échangées ou des informations consultées. Cela amène donc à distinguer deux sous catégories au sein des correspondances, les correspondances échangées et les « informations consultées » distinctes des « données de connexion ».

1.3. CADRE EUROPEEN

➢ *Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales*

La Cour de Strasbourg admet, de façon constante depuis son arrêt *Klass et autres c. Allemagne* (n° 5029/71, 6 septembre 1978), que les services de renseignement des Etats puissent se munir de moyens de surveiller les individus pour faire face à des menaces pouvant mettre en péril une société démocratique. Les mesures prises à cet égard, qui peuvent concerner un grand nombre de données ne portent ainsi pas, par nature, une atteinte disproportionnée au droit à la vie privée protégée par l'article 8 de la Convention.

S'agissant d'un système d'interception généralisée des communications[31], la Cour déduit de l'article 8 de la Convention qu'une ingérence dans ce droit ne peut se justifier que si :

- elle est prévue par la loi, c'est-à-dire qu'elle doit avoir une base en droit interne et être compatible avec la prééminence du droit ; elle doit être accessible à la personne concernée, prévisible quant à ses effets et assurer une protection adéquate contre l'arbitraire ;
- elle doit viser un ou plusieurs des buts légitimes énumérés à l'article 8§2 et être nécessaire, dans une société démocratique, pour atteindre ce ou ces buts.

➢ *Droit de l'Union européenne*

Dans un arrêt La Quadrature du Net E.A. du 6 octobre 2020, la Cour de justice de l'Union européenne (CJUE) a jugé que la Charte des droits fondamentaux de l'Union européenne ne s'oppose pas à la mise en œuvre de la technique de recueil de renseignement mentionnée à l'article L. 851-3 du code de la sécurité intérieure dès lors qu'elle est « *limitée à des situations dans lesquelles un Etat membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible* » et sous réserve qu'elle « [*fasse] 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* ».

Dans sa décision en date du 21 avril 2021, qui tire les conséquences de cet arrêt (Ass., French Data Network et autres, n° 393099), l'assemblée du Conseil d'État a confirmé que l'article

[31] Arrêt Zakharov c. Russie, req. n° 47143/06, 4 décembre 2015, § 227 s.

L. 851-3 du code de la sécurité intérieure et les décrets pris pour son application ne méconnaissaient le droit de l'Union européenne qu'en tant seulement qu'ils permettent la mise en œuvre de traitements automatisés sans prévoir, avant l'identification des personnes dont les données sont susceptibles de révéler une menace à caractère terroriste, un contrôle préalable par une juridiction ou par une autorité administrative dotée d'un pouvoir contraignant. Si, comme pour toutes les techniques de renseignement, l'identification des personnes détectées par le biais d'un algorithme ne peut être mis en œuvre qu'après l'avis d'un organisme de contrôle indépendant, la CNCTR, celui-ci n'est en effet pas contraignant pour le Premier ministre. Comme indiqué précédemment, l'article 16 en tire les conséquences en apportant à la loi les modifications qui s'imposent.

La décision du Conseil d'État reconnaît en revanche que les autres exigences posées par la Cour sont satisfaites par le droit en vigueur ainsi que par les modifications que le présent projet de loi entend y apporter, observant à cet égard que l'algorithme ne peut être mis en œuvre que pour les seuls besoins de la prévention du terrorisme et que la Commission nationale de contrôle des techniques de renseignement, chargée d'émettre un avis préalable à la mise en œuvre de la technique, « *vérifie l'existence et l'actualité de la menace grave pour la sécurité nationale susceptible de justifier une telle mesure* ».

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

La technique mentionnée à l'article L. 851-3 du code de la sécurité intérieure répond à un besoin essentiel de détection précoce de la menace terroriste.

L'un des enjeux les plus cruciaux de l'activité de renseignement consiste en effet à être en mesure de détecter une nouvelle menace, dont les auteurs et les modes opératoires ne sont pas connus et ne peuvent par définition faire l'objet d'une surveillance ciblée *a priori*, afin de la caractériser et de l'évaluer. Ce besoin est particulièrement prégnant en matière de lutte contre le terrorisme du fait du caractère diffus et très évolutif de la menace.

Les dispositifs de nature algorithmique visent ainsi à repérer et discriminer sur les réseaux de communications électroniques des données caractéristiques de comportements typiques d'organisations et de cellules terroristes, afin de repérer des menaces et d'engager, le cas échéant, des mesures de surveillance individuelle aussi précisément ciblées qu'il est possible.

De nouveaux comportements sont également apparus, à la faveur notamment de la diffusion informatique d'une vaste propagande terroriste et de l'émergence de nouveaux moyens de communication électroniques. Les actions terroristes sont ainsi, de plus en plus, le fait d'individus qui s'inspirent des messages de propagande qui émanent des organisations terroristes, incitant au passage à l'acte en fournissant les tutoriels pour leur réalisation, mais qui ne sont pas entrés en contact visible ou direct avec des organisations, réseaux ou groupes terroristes, échappant ainsi à toute capacité de détection par le biais d'une surveillance ciblée. En effet, si le maillage territorial des services de renseignement et de police ainsi que la sensibilisation des différents acteurs administratifs et sociaux permettent de détecter une

évolution du comportement social d'un individu susceptible de révéler l'existence d'une menace terroriste, cette capacité disparaît lorsque ces indices n'apparaissent que par l'activité numérique de la personne.

Dans ces conditions, il est utile, en même temps que l'on pérennise cette technique, de lui permettre de s'adapter au caractère évolutif de la menace. À ce titre, ces dispositifs, qui ne traitent aujourd'hui que les seules données téléphoniques, doivent pouvoir être déployés sur les adresses de ressources sur internet (URL), y compris lorsqu'elles sont susceptibles de révéler indirectement, au regard de la nature de l'adresse complète permettant l'acheminement de la communication électronique, des informations sur le contenu des sites consultés.

Les usages contemporains en matière de télécommunications recourent en effet de plus en plus à des applications Internet et non aux voies téléphoniques classiques. C'est particulièrement le cas pour la population visée. Les données de connexion produites par l'utilisation d'internet prennent notamment la forme d'adresses de ressources sur internet (URL). Ces données sont, au regard des usages actuels en matière de communication, les plus pertinentes pour détecter les comportements caractérisés par les paramètres d'un algorithme définis sous le contrôle de la CNCTR. Un algorithme spécifique, fondé en partie sur les URL, pourrait ainsi permettre la détection de consultations ou de téléchargements de fichiers caractérisant une menace (manuels de création d'explosifs ou de poisons, vidéo de revendications ou d'appel au djihad, *etc*…). Il est rappelé que la CNCTR accède aux codes sources de ces algorithmes pour vérifier leur complète conformité aux traitements attendus.

L'élargissement du champ des données traitées aux URL, données particulièrement pertinentes pour la détection des comportements terroristes, est également de nature à favoriser un meilleur ciblage des alertes, à réduire le nombre de faux positifs et, en conséquence, à améliorer l'efficacité de la technique, dans le strict respect de la vie privée et du secret des correspondances.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et des infractions, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et des libertés constitutionnellement garantis, au nombre desquels figure le droit au respect de la vie privée.

Deux options ont été envisagées :

Une première option possible consiste à compléter la liste, fixée par voie réglementaire, des données de connexion que les services de renseignement sont habilités à recueillir pour y inclure l'ensemble des URL. Ceci suppose de considérer que les informations dont sont porteuses les adresses complètes des ressources sur internet (URL) sont limitées et ne donnent pas

nécessairement par elles-mêmes d'indication directe et précise sur la nature des informations consultées, et encore moins sur les activités de la personne qui procède à la consultation.

De fait, s'il prend en compte le fait que l'algorithme ne peut traiter que des données de connexion, à l'exclusion du contenu des correspondances échangées ou des informations consultées (cf. décision précitée n° 2015-713 DC du 23 juillet 2015), le Conseil constitutionnel ne s'est pas prononcé sur la nature juridique des adresses de ressources sur internet qui ne permettent qu'indirectement d'obtenir des indications sur le contenu des informations consultées sur un site internet.

Pour autant, la Commission nationale de contrôle des techniques de renseignement a considéré dans sa délibération n° 1/2016 du 14 janvier 2016 précitée que les adresses de ressources sur internet constituaient une catégorie de données mixte, ces adresses pouvant constituer de simples données de connexion comme des données de contenu lorsqu'elles « *sont porteuses par nature des informations consultées* ».

Par ailleurs, ajouter les URL aux données visées par l'article L. 851-1, impliquerait que cette catégorie de donnée puisse être consultée pour toutes les techniques de renseignement permettant le recueil des « données visées à l'article L. 851-1 », à savoir :

- Le recueil des données de connexion (L. 851-1 CSI) ;
- Le recueil en temps réel (L. 851-2) ;
- Les traitements automatisés (L. 851-3) ;
- l'autorisation d'interception de sécurité vaudra autorisation de recueil des URL (III de l'article L. 852-1 et 2d alinéa de l'article L. 852-2) ;

Enfin, la durée de conservation de cette catégorie de données serait alignée sur celle des données de connexion, ce qui n'est pas souhaitable, au regard de leur nature mixte.

La seconde option consiste à restreindre la possibilité de recueillir les *adresses complètes de ressources utilisées sur internet*, sans que cela ne puisse concerner le contenu des informations consultées, aux seules techniques de renseignement des articles L. 851-2 et L. 851-3 du CSI, solution qui correspond au principe de nécessité et de proportionnalité, les URL étant particulièrement utiles dans ce cadre.

3.2. DISPOSITIF RETENU

> ➢ *Étendre le champ de la technique prévue à l'article L. 851-3 du CSI aux adresses complètes de ressources utilisées sur Internet*

En droit, ces adresses, lorsqu'elles ont la nature de données de connexion peuvent d'ores et déjà être prises en compte par les algorithmes. Ces « URL-données de connexion » sont très majoritairement celles qui présentent un intérêt opérationnel. Toutefois, dès lors qu'il est techniquement impossible *a priori* de les isoler des adresses qui « *sont porteuses par nature*

des informations consultées », et que ces dernières peuvent également contribuer à la pertinence de l'algorithme, les algorithmes pourront concerner les unes et les autres.

Il est entendu que les adresses complètes de ressources utilisées sur internet qui feront l'objet d'un traitement automatisé en application de l'article L. 851-3 seront celles des seules ressources auxquelles un utilisateur accède, à l'exclusion de celles pouvant figurer au sein de contenus de correspondances électroniques, par exemple des liens dans des SMS ou des courriers électroniques, ou au sein de contenus consultés, par exemple des liens dans des pages web. Dès lors, il n'est pas apparu nécessaire de les exclure expressément du dispositif.

Enfin, il convient de noter que les données URL ne sont pas traitées par les opérateurs de communications électroniques et doivent donc être recueillies par d'autres moyens techniques, ce que permet le dispositif retenu.

➢ *Renforcer les garanties applicables à la mise en œuvre de l'algorithme*

Le dispositif retenu vise par ailleurs à assortir l'élargissement des données susceptibles d'être traitées par l'algorithme aux adresses complètes d'une ressource sur internet d'un renforcement des garanties fortes qui entourent, depuis l'entrée en vigueur de la loi relative au renseignement du 24 juillet 2015, la mise en œuvre de ces traitements automatisés dont les paramètres de détection sont contrôlés par la CNCTR.

En pratique, les ingénieurs de la Commission nationale de contrôle des techniques de renseignement accompagnent les services de l'État dans la définition des paramètres et de leur évolution, ainsi que dans la mise en œuvre des algorithmes qu'ils contrôlent périodiquement tout au long de la durée de l'autorisation.

Toute modification de l'algorithme nécessite un nouvel examen de la part de la Commission préalablement à sa mise en œuvre. En cas de demande de renouvellement, les services de renseignement sont légalement tenus d'indiquer dans leur demande le nombre d'alertes produites par l'algorithme. Ils doivent également transmettre à la CNCTR une analyse de la pertinence de ces alertes.

Une seconde autorisation est requise pour obtenir l'identifiant technique à l'origine d'une alerte et les données techniques afférentes, ainsi le cas échéant que l'identité de l'utilisateur du numéro de téléphone ou de l'adresse IP concerné.

Les données recueillies en cas d'alerte ne peuvent être exploitées que pour une durée maximale de soixante jours. Toutefois, en l'état actuel de la législation, ces données peuvent être conservées au-delà de cette durée, lorsqu'il existe des éléments sérieux confirmant une menace à caractère terroriste. Dans ce cas, elles peuvent être conservées jusqu'à quatre ans à compter de leur recueil, par application du 3° du I l'article L. 822-2 du code de la sécurité intérieure. En tout état de cause, les données non détectées par les traitements comme susceptibles de révéler une menace à caractère terroriste sont détruites immédiatement.

Le projet de loi supprime cette possibilité de conservation prolongée des données afférentes à la détection d'une menace terroriste par l'algorithme. Ainsi, compte tenu de l'extension des catégories de données exploitées par les traitements automatisés concernés, les services de renseignement seront tenus de confirmer l'existence d'une menace dans ce délai de soixante jours afin de décider le cas échéant de demander la possibilité d'engager une mesure de surveillance ciblée au moyen d'une des techniques de recueil de renseignement prévues au livre VIII du code de la sécurité intérieure (analyse des facturations détaillées liées à un numéro de téléphone, placement sur écoutes administratives, *etc.*).

Il convient de rappeler que l'engagement d'une telle mesure est soumis à une nouvelle autorisation du Premier ministre après avis de la CNCTR, qui intervient après deux autorisations données dans les mêmes conditions pour mettre en œuvre l'algorithme puis pour obtenir la communication de l'identifiant technique que les paramètres de détection auraient signalé.

Enfin, le projet de loi entend limiter le nombre des services de renseignement autorisés à solliciter la mise en œuvre d'un algorithme sur le fondement de l'article L. 851-3 en précisant que seuls les services spécialisés de renseignement mentionnés à l'article L. 811-2 peuvent présenter une telle demande.

➢ *Clarification de l'architecture de l'algorithme*

Le projet de loi clarifie enfin les modalités de fonctionnement des algorithmes, telles qu'elles résultent du travail progressif de construction de cet outil, en concertation avec les opérateurs et en accord avec la CNCTR, entre l'adoption de la loi et la mise en service du premier algorithme fin 2017.

Il précise ainsi que l'exécution des algorithmes est assurée de manière centralisée, sous le contrôle de la CNCTR, par un service du Premier ministre, en l'occurrence le GIC, qui fait écran entre les données passées au tamis des algorithmes et les services de renseignement ayant demandé leur mise en œuvre. Ce faisant, le projet de loi formalise la garantie dont la CNCTR avait exigé le respect lorsqu'elle a rendu son avis favorable en 2016.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

L'article L. 851-3 du code de la sécurité intérieure est modifié.

La responsabilité de la mise en œuvre des traitements automatisés de l'article L. 851-3 du code de la sécurité intérieure est transférée des opérateurs de communications électroniques vers un service du Premier ministre, le GIC. Les services spécialisés de renseignement ne pourront recevoir communication que des données de connexion, résiduelles, afférentes aux seules communications repérées par l'algorithme au titre de la prévention du terrorisme, et à condition

d'y avoir été spécialement autorisés au préalable par une nouvelle décision du Premier ministre prise après avis de la CNCTR.

4.2. IMPACTS SUR LES ADMINISTRATIONS

Les modifications prévues (centralisation par le GIC, prise en compte des adresses complètes des ressources sur internet) rendent nécessaires une adaptation de l'architecture technique actuellement mise en œuvre. Ces évolutions nécessitent un renfort de 25 ETP. La cellule commune pilotée par la DGSI chargée de concevoir et paramétrer les algorithmes ainsi que de gérer les alertes devra élargir sa compétence pour définir des traitements automatisés tirant bénéfice des nouvelles possibilités offertes par les URL.

4.3. IMPACTS SUR LES FINANCES PUBLIQUES

Le coût d'adaptation de l'architecture technique est évalué à 20 M€ pour l'achat et la mise en œuvre des dispositifs techniques et de 4 M€ annuels pour leur maintien en condition opérationnelle.

5. CONSULATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Cette disposition a été présentée à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure qui a rendu son avis le 7 avril 2021.

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

Cette disposition a été présentée, conformément à L. 36-5 du code des postes et communications électroniques, à l'autorité de régulation des communications électroniques, des postes et de la distribution de la presse qui a rendu son avis le 16 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions s'appliqueront dès le lendemain de la publication de la loi au Journal officiel de la République française.

5.2.2. Application dans l'espace

Elles sont d’application immédiate sur l’ensemble du territoire français.

Article 14 : Ajout des adresses complètes de ressource sur internet (URL) aux données susceptibles d'être recueillies en temps réel (1°) et définition de leur durée de conservation (2°)

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Prévue à l'article L. 851-2 du CSI, la technique de recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents relatifs à une personne préalablement identifiée susceptible d'être en lien avec une menace, cette technique concerne, les seules données visées à l'articles L. 851-1 du même code, c'est-à-dire 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.

Conformément à l'article L. 821-4 du même code, cette technique peut être mise en œuvre pour une durée de quatre mois, sur autorisation du Premier ministre délivrée après avis de la CNCTR. Elle est renouvelable dans les mêmes conditions.

La procédure prévue à l'article L. 821-5 du CSI, qui permet au Premier ministre, en cas d'urgence absolue, d'autoriser cette technique sans attendre l'avis de la CNCTR, n'est pas applicable.

1.2. CADRE CONSTITUTIONNEL

Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel a déclaré conformes à la Constitution les dispositions de l'article L. 851-2 du code de la sécurité intérieure. Il a estimé que ces dispositions ne portaient pas une atteinte disproportionnée au droit au respect de la vie privée au regard d'un faisceau de garanties. Au nombre de ces garanties figurent :

- l'existence d'une autorisation du Premier ministre délivrée sur demande écrite et motivée d'un ministre ;
- l'obligation de solliciter un avis préalable d'une autorité administrative indépendante, dotée en outre de prérogatives de contrôle ;
- l'existence d'une voie de recours spéciale devant le Conseil d'Etat, ouverte à la CNCTR comme à toute personne souhaitant vérifier que la technique n'a pas été irrégulièrement mise en œuvre à son encontre.

Le Conseil constitutionnel a également relevé que :

- une telle autorisation de recueil des données en temps réel ne pourra être délivrée que pour les besoins de la prévention du terrorisme ;
- l'autorisation de recueil de renseignement en cause porte uniquement 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 et ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit ;
- elle est autorisée pour une durée de quatre mois renouvelable conformément à l'article L. 821-4 du CSI ;
- elle ne peut être mise en œuvre qu'à l'égard de personnes dont il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme, ce ciblage étant soumis à un contrôle préalable d'une AAI, la CNCTR et, le cas échéant, du Conseil d'État dont la décision sera dotée d'un effet contraignant
- l'article L. 821-5 du code de la sécurité intérieure, qui permet, en cas d'urgence absolue, au Premier ministre de délivrer une autorisation sans avis préalable de la CNCTR, n'est pas applicable à cette technique de renseignement.

1.3. CADRE CONVENTIONNEL

La Cour de Strasbourg admet, de façon constante depuis son arrêt *Klass et autres c. Allemagne* (n° 5029/71, 6 septembre 1978), que les services de renseignement des Etats puissent se munir de moyens de surveiller les individus pour faire face à des menaces pouvant mettre en péril une société démocratique. Les mesures prises à cet égard, qui peuvent concerner un grand nombre de données ne portent ainsi pas, par nature, une atteinte disproportionnée au droit à la vie privée protégée par l'article 8 de la Convention.

Dans son arrêt *Weber et Saravia c. Allemagne* (n° 54934/00, 29 juin 2006, § 95), la Cour a exposé les principes généraux à l'aune desquels une mesure de surveillance secrète doit être appréciée pour déterminer si elle est ou pas conforme aux exigences de l'article 8 § 2 de la Convention : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.

La Cour a fait application de ces critères à un système d'interception généralisée des communications dans son arrêt de grande chambre, req. n° 47143/06, 4 décembre 2015, *Zakharov c. Russie*, § 227 s.) : elle y déduit de l'article 8 de la Convention qu'une ingérence dans ce droit ne peut se justifier que si :

- elle est prévue par la loi, c'est-à-dire qu'elle doit avoir une base en droit interne et être compatible avec la prééminence du droit ; elle doit être accessible à la personne concernée, prévisible quant à ses effets et assurer une protection adéquate contre l'arbitraire ;
- elle doit viser un ou plusieurs des buts légitimes énumérés à l'article 8§2 et être nécessaire, dans une société démocratique, pour atteindre ce ou ces buts.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

La technique mentionnée à l'article L. 851-2 répond à un besoin essentiel de détection de la menace terroriste. Comme pour la technique de l'algorithme, l'efficacité des alertes produites reste très dépendante de la nature des données intégrées dans les paramètres initiaux. En effet, le dispositif actuel n'intègre pas les données internet mais uniquement les données de téléphonie.

Or, les usages contemporains en matière de télécommunications recourent en effet de plus en plus à des applications Internet et non aux voies téléphoniques classiques. C'est particulièrement le cas pour la population visée. Les données de connexion produites par l'utilisation d'internet prennent notamment la forme d'adresses de ressources sur internet (URL).

A ce titre, et sans permettre d'accéder au contenu des sites internet consultés, cette technique doit, néanmoins pouvoir être déployée sur les adresses de ressources sur internet (URL) utilisées par la personne concernée, y compris lorsqu'elles sont susceptibles de révéler indirectement, au regard de la nature de l'adresse complète permettant l'acheminement de la communication électronique, des informations sur le contenu des sites consultés.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Le livre VIII du code de la sécurité intérieure est organisé autour de deux catégories de données : les données de connexion (L. 851-1) et les correspondances (L. 852-1 ; L. 852-2).

Ces deux catégories de données répondent à des régimes différents de recueil et de durée de conservation.

Or, il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et des infractions, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et des libertés constitutionnellement garantis, au nombre desquels figure le droit au respect de la vie privée.

Une option possible consiste à compléter la liste, fixée par voie réglementaire, des données de connexion que les services de renseignement sont habilités à recueillir pour y inclure l'ensemble des URL. Ceci suppose de considérer que les informations dont sont porteuses les adresses complètes des ressources sur internet sont limitées et ne donnent pas nécessairement par elles-mêmes d'indication directe et précise sur la nature des informations consultées, et encore moins sur les activités de la personne qui procède à la consultation.

De fait, s'il prend en compte le fait que la technique de renseignement visée à l'article L. 851-2 du CSI ne peut traiter que des données de connexion, à l'exclusion du contenu des correspondances échangées ou des informations consultées (cf. décision n° 2015-713 DC du 23 juillet 2015, cons. 55), le Conseil constitutionnel ne s'est pas prononcé sur la nature juridique des adresses de ressources sur internet qui ne permettent qu'indirectement d'obtenir des indications sur le contenu des informations consultées sur un site internet.

Pour autant, la Commission nationale de contrôle des techniques de renseignement a considéré dans sa délibération n° 1/2016 du 14 janvier 2016 que les adresses de ressources sur internet constituaient une catégorie de données mixte, ces adresses pouvant constituer de simples données de connexion comme des données de contenu lorsqu'elles « *sont porteuses par nature des informations consultées* ».

Au regard de cette analyse, l'extension des données susceptibles d'être recueillies en temps réel en application de l'article L. 851-2 au-delà des seules données de connexion, pour inclure les URL porteuses des informations consultées, appelle nécessairement l'intervention du législateur.

Cette extension porte uniquement sur les URL ayant donné lieu à une consultation effective par les utilisateurs. En effet, la technique de recueil en temps réel des données de connexion n'ayant en aucun cas vocation à recueillir et analyser le contenu des communications, qui demeure exclu du champ d'application de l'article L. 851-2 du CSI, défini par référence à l'article L. 851-1 du même code, les URL qui, sans avoir été consultées, se trouveraient dans le contenu de correspondances échangées ne pourront pas être collectées dans ce cadre. Dès lors, il n'est pas apparu nécessaire de préciser le dispositif afin d'exclure ces dernières URL.

Par ailleurs, ces données constituant une catégorie particulière de données de connexion, le 2° du présent article prévoit leur durée de conservation en l'alignant, non pas sur celle des données de connexion, que le 3° de l'article L. 822-2 porte à quatre ans mais sur celle des données mixtes, prévues à au 2° du même article, soit cent vingt jours : en effet, ces données ne sont pas des données de contenu (dont la conservation est limitée à trente jours) mais sont susceptibles de révéler certaines informations et portent donc une atteinte à la vie privée supérieure à celle des données de connexion classiques.

3.2. DISPOSITIF RETENU

Le dispositif retenu vise à assortir l'élargissement des données susceptibles d'être traitées recueillies en temps réel via la technique de renseignement visée à l'article L. 852-1 du CSI aux adresses complètes d'une ressource sur internet utilisées par une personne d'une distinction de la durée de conservation des deux types de données susceptibles d'être recueillies par ce biais. Cette détection est effectuée pour les seuls besoins de la prévention du terrorisme, à l'encontre de personnes préalablement identifiées comme étant susceptibles d'être en lien avec une menace terroriste, ou de personnes de leur entourage.

Ainsi, il conviendra de distinguer, lorsque la technique visée à l'article L. 852-1 sera mise en œuvre, entre les données de connexion « classiques », qui pourront être conservées quatre ans, conformément au droit applicable actuellement, et les données relatives aux URL qui, elles, devront être détruites au terme d'un délai beaucoup plus réduit de 120 jours, conformément aux dispositions de l'article L. 822-2 modifié.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Les articles L. 822-2 et L. 851-2 du code de la sécurité intérieure sont modifiés.

4.2. IMPACTS SUR LES PARTICULIERS

Les adresses des sites consultés sur internet par des personnes présentant une menace de nature terroriste et à l'égard desquelles la technique prévue à l'article L. 851-2 du code de la sécurité intérieure aura été autorisée par le Premier ministre après avis de la CNCTR, pourront être transmises et exploitées par les services de renseignement.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure qui a rendu son avis le 7 avril 2021.

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 8 avril 2021.

Cette disposition a été présentée, conformément à L. 36-5 du code des postes et communications électroniques, à l'autorité de régulation des communications électroniques, des postes et de la distribution de la pressequi a rendu son avis le 16 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entrent en vigueur immédiatement.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront à l'échelle nationale, y compris dans les collectivités régies par les articles 73 et 74 de la Constitution.

Article 15 : Modalités de conservation des données de connexion en cas de menace grave, actuelle ou prévisible sur la sécurité nationale

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Les données de connexion, parfois appelées métadonnées pour les distinguer de celles qui portent sur le contenu des communications échangées, jouent aujourd'hui un rôle central dans la recherche, la constatation et la poursuite des infractions pénales et dans, le domaine du renseignement, pour la défense et la promotion des intérêts fondamentaux de la Nation.

Ainsi, dans le domaine judiciaire, près de deux millions environ de réquisitions portant sur ces données sont effectuées annuellement par l'intermédiaire de la plateforme nationale des interceptions judiciaires (PNIJ), procédure mise en œuvre dans plus de quatre enquêtes judiciaires sur cinq. Une telle procédure revêt notamment un intérêt fondamental dans la répression de la criminalité organisée où elle est utilisée systématiquement.

Dans le domaine du renseignement, plusieurs techniques visées au livre VIII du code de la sécurité intérieure consiste en un accès aux données de connexion en possession des opérateurs, accès opéré *via* un service du Premier ministre, le groupement interministériel de contrôle (GIC). Chaque année, environ 50 000 accès à ces données sont autorisés pour les besoins du renseignement.

Ces techniques d'accès aux données de connexion par les services de renseignement font l'objet du titre V du livre II du code de la sécurité intérieure. Il s'agit de :

- la technique de recueil en temps différé des données de connexion (article L. 851-1) ;
- la technique du recueil en temps réel de ces mêmes données (article L. 851-2) ;
- la technique dite de l' « algorithme », qui, appliqué à un flux de données de connexion, permet le cas échéant un accès à ces données, en cas de détection d'une menace terroriste (article L. 851-3) ;
- la technique de géolocalisation en temps réel (article L. 851-4).

Les règles en matière de conservation de certaines des données de connexion sont définies à l'article L. 34-1 du code des postes et des communications électroniques. Cet article, applicable aux *« opérateurs de communications électroniques, (...) notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* » pose tout d'abord le principe selon lequel ces personnes effacent ou rendent anonyme toute donnée relative au trafic.

Ce principe est toutefois assorti d'exceptions.

La première, visée au III de l'article L. 34-1, concerne les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation de respect du droit d'auteur sur internet 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. Pour ces besoins, et dans le seul but de permettre la mise à disposition de ces données à l'autorité judiciaire, à la Haute autorité pour la diffusion des œuvres et de la protection des droits sur internet (HADOPI) ou à l'autorité nationale de sécurité des systèmes d'information (ANSSI), les opérateurs sont tenus de différer, pour une durée d'un an, les opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques, définies aux articles R. 10-13 (besoins judiciaires) et R. 10-13-1 (ANSSI) du code des postes et des communications électronique.

La seconde, visée au IV de l'article L. 34-1, concerne les besoins de la facturation et du paiement des prestations de communications électroniques, pour la satisfaction desquels les opérateurs peuvent, 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, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques visées à l'article R. 10-14 du code des postes et des communications électronique.

Ces modalités trouvent leur pendant, s'agissant des fournisseurs d'accès à internet et des hébergeurs, à l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) qui fait obligation aux personnes précitées de conserver les données nécessaires à l'identification des personnes créant, modifiant ou supprimant des contenus en ligne (la liste des données concernées étant fixée à l'article 1er du décret n° 2011-218 du 25 février 2011). Le même article 6 prévoit un droit d'accès aux données ainsi conservées ouvert à l'autorité judiciaire pour la recherche ou la poursuite des infractions.

Bien que l'article L. 34-1 du CPCE ne traite pas spécifiquement de la conservation des données de connexion pour les besoins des services de renseignement, le Conseil d'État a jugé qu'il résultait des dispositions des articles L. 851-1 et L. 811-3 du code de la sécurité intérieure (qui organisent l'accès aux données de connexion conservées en application des articles L. 34-1 CPCE et 6 de la LCEN) que le législateur a également 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 des missions de défense et de promotion des intérêts fondamentaux de la Nation confiées aux services de renseignement (CE ass. 21 avr. 2021, *French data Network et a.*, n° 393099, 394922, 397844, 397851, 424717, 424718)

1.2. CADRE EUROPEEN

1.2.1. Le droit de l'Union européenne

La directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications est venue prévoir, à son article 6 § 1 que « *les données relatives au trafic concernant les abonnés et les utilisateurs traitées en vue d'établir des communications et stockées par le fournisseur d'un réseau public de télécommunications et/ou d'un service de télécommunications accessible au public doivent être effacées ou rendues anonymes dès que la communication est terminée* », ce principe étant assorti d'une exception, prévue au § 2 du même article, liée aux besoins de la facturation.

Les obligations découlant de cette directive ont été reprises par 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 (dite « *e-privacy* »), notamment l'obligation d'effacement ou d'anonymisation des données « relatives au trafic », reprise à l'article 6 de cette directive.

Cette directive prévoit néanmoins, à son article 1er § 3 (« champs d'application ») qu'elle « ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union 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 ».

En outre, son article 15 § 1 permet aux Etats membres d'adopter des mesures législatives visant à limiter, notamment, l'obligation d'effacement ou d'anonymisation, « *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* ».

Si, dans les premières années d'application de cette directive, la jurisprudence de la Cour de justice de l'Union européenne semblait admettre la possibilité d'une conservation généralisée et indifférenciée pour les besoins des services d'enquête, elle a néanmoins, par trois principaux arrêts (CJUE, 21 déc. 2016, *Télé2 Sverige AB*, n° C-203/15 et C-698/15 ; CJUE 2 oct. 2018, *Ministerio fiscal*, n° C-207/16 et CJUE 6 oct. 2020, *La Quadrature du Net et a*., n° C-511/18, C-512/18 et C-520/18), adopté une lecture différente des textes européens applicables à la conservation des données de connexion et aux modalités d'accès des autorités publiques à ces données.

A rebours de nombreux Etats membres, la Cour a tout d'abord, dans son arrêt *Télé2*, considéré que la directive *e-privacy* trouvait à s'appliquer aux mesures nationales qui prévoient tant l'obligation des fournisseurs de conserver les données de connexion que l'accès des autorités nationales à ces données, à des fins de lutte contre la criminalité. Sur l'autorisation, prévue à l'article 15 § 1 de la directive, donnée aux Etats de limiter, notamment, l'obligation d'effacement ou d'anonymisation, pour des finalités de protection de la sécurité et de répression

de la criminalité, la Cour considère qu'une telle autorisation, sauf à la priver de tout effet utile, « *présuppose nécessairement que les mesures nationales qui y sont visées, telles que celles relatives à la conservation de données à des fins de lutte contre la criminalité, relèvent du champ d'application de cette même directive, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit* ».

Cette applicabilité de la directive e-privacy a conduit la Cour à une condamnation du principe de conservation généralisée et indifférenciée des données, au regard des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, qui garantissent respectivement le droit à la vie privée et le droit à la protection des données personnelles, comme de l'article 11 de la Charte qui garantit la liberté d'expression.

Aussi, selon la Cour, la conservation généralisée des données de connexion constitue-t-elle une ingérence « *particulièrement grave* » excédant « *les limites du strict nécessaire et ne [pouvant] être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte* » CJUE, 21 déc. 2016, Télé2 Sverige AB, n° C-203/15 et C-698/15).

Dans son dernier arrêt, *La Quadrature du Net* (CJUE 6 oct. 2020, n° C-511/18, C-512/18 et C-520/18), la Cour, se prononçant sur la possibilité d'une conservation généralisée des données de connexion lorsqu'est en cause la sécurité nationale, a rappelé que des limitations à l'exercice du droit à la vie privée étaient possibles, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui. La Cour énonce que l'objectif de sauvegarde de la sécurité nationale est susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier les autres objectifs visés à l'article 15 de la directive *e-privacy*.

Elle a ainsi jugé que, si une conservation systématiquement générale et indifférenciée des données n'est pas possible, le législateur peut adopter une mesure de conservation pour une période limitée au strict nécessaire, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Cette injonction de conservation doit pouvoir 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.

De l'ensemble de ces arrêts, il ressort que la Cour identifie trois objectifs dont la « gravité » justifie une conservation plus importante de données dont la « sensibilité » augmente parallèlement : la « lutte contre la criminalité et la prévention des menaces contre la sécurité publique », la « lutte contre la criminalité grave et prévention des menaces graves pour la sécurité publique » et la « sauvegarde de la sécurité nationale ». Le premier peut justifier la conservation des données les moins révélatrices de la vie privée des personnes, le deuxième la conservation ciblée de données plus vastes et, enfin, le troisième la conservation généralisée

et indifférenciée des données, y compris celles qui apportent les informations les plus précises sur la personne à laquelle elles se rapportent, mais dans la limite et le délai circonscrit par la réalité de la menace qui pèse sur la sécurité nationale.

Par ailleurs, la Cour établit une gradation entre les catégories de données de connexion susceptibles d'être conservées et distingue entre :

- les données relatives à l'identité civile de l'utilisateur qui, eu égard à leur faible sensibilité, peuvent être conservées de manière généralisée et indifférenciée, quel que soit l'objectif poursuivi ;
- les adresses IP, qui présentent davantage de sensibilité, et qui ne peuvent donc être conservées de manière généralisée et indifférenciée que pour lutter contre la criminalité grave et pour sauvegarder la sécurité nationale ;
- et enfin les autres données de connexion, dont la conservation est réservée aux objectifs les plus graves, et selon deux modalités différentes en fonction de l'objectif poursuivi.

S'agissant de la lutte contre la criminalité grave et de la prévention des atteintes à la sécurité publique, la CJUE admet seulement la possibilité d'adopter une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation afin de lutter contre la criminalité grave à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire. La Cour propose deux exemples : ciblage de personnes (notamment celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et celles présentant sur la base d'éléments objectifs une menace pour la sécurité publique ou la sécurité nationale) et/ou de lieux (lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages).

En outre, pour cet objectif, la Cour juge possible une « conservation rapide » des données, conformément à l'article 16 de la convention du Budapest sur la cybercriminalité du 23 novembre 2001. Une telle conservation rapide, à des fins de la lutte contre la criminalité grave et de la prévention des atteintes à la sécurité publique, ne pourra concerner que les données susceptibles de contribuer à la prévention ou à la répression d'une infraction déterminée, étant précisé qu'elle pourra concerner les personnes de l'entourage de la personne soupçonnée (victime ou complice potentiel par exemple).

S'agissant de la sécurité nationale, le législateur peut adopter une mesure de conservation généralisée et indifférenciée pour une période limitée au strict nécessaire, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une **menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible**. Cette injonction de conservation doit être soumise à un examen régulier de sa nécessité (et donc à une réévaluation périodique de l'état de la menace) et soumise au contrôle

d'un juge ou d'une autorité indépendante dotée d'un pouvoir contraignant qui appréciera son caractère proportionné.

1.2.2. Cadre conventionnel

La Cour européenne des droits de l'Homme (CEDH) considère que le simple fait de conserver des données relatives à la vie privée des individus constitue une ingérence au sens de l'article 8 de la Convention qui garantit le droit au respect de la vie privée et familiale et surtout de la correspondance, peu importe que ces informations soient ou non utilisées par la suite. Pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu un aspect de la vie privée, la Cour tient toutefois compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et des résultats qui peuvent en être tirés (CEDH gr.ch., 4 déc. 2008, *S. & Marper c. Royaume-Uni*, aff. n° 30562/04).

Sur l'accès aux données à caractère personnel conservées par ailleurs, la Cour a eu l'occasion de se prononcer à de nombreuses reprises. Ainsi, dans le domaine judiciaire, la Cour juge-t-elle par exemple que ne méconnaît pas l'article 8 de la Convention une réquisition judiciaire adressée à un opérateur de téléphonie mobile pour obtenir la liste des bornes déclenchées par une ligne téléphonique dans le cadre d'une procédure pénale relative à des faits d'importation de stupéfiants en bande organisée, d'association de malfaiteurs et de blanchiment. La Cour relève qu'une telle réquisition poursuivait un but légitime et avaient été utilisées dans le cadre d'une enquête et d'un procès pénal au cours duquel le requérant avait bénéficié d'un contrôle effectif (CEDH 8 févr. 2018, Ben Faiza c. France, n° 31446/12).

Dans le domaine du renseignement, la Cour admet, de façon constante depuis son arrêt *Klass et autres c. Allemagne* (n° 5029/71, 6 septembre 1978), que les services de renseignement étatiques puissent se munir de moyens de surveiller les individus pour faire face à des menaces pouvant mettre en péril une société démocratique. Les mesures prises à cet égard, qui peuvent concerner un grand nombre de données ne portent ainsi pas, par nature, une atteinte disproportionnée au droit à la vie privée protégée par l'article 8 de la Convention.

En 2018, la Cour s'est penchée spécifiquement sur le degré d'atteinte à la vie privée d'une personne susceptible de résulter de l'accès et de l'examen de données de connexion dans son arrêt Big Brother Watch. Et a. c. Royaume-Uni (n° 58170/13). Elle a jugé en l'espèce que tout système permettant l'accès à des données détenues par des fournisseurs de services de communication doit se limiter au but que constitue la lutte contre le crime, et l'accès doit être soumis au contrôle préalable d'un tribunal ou d'un organe administratif indépendant. Dans cet arrêt, elle reconnaît expressément la gravité des menaces qui pèsent actuellement sur de nombreux État contractants, notamment le terrorisme international et d'autres crimes tels que le trafic de stupéfiants, la traite d'êtres humains, l'exploitation sexuelle d'enfants et la cybercriminalité. Elle considère en conséquence que les États doivent jouir d'une ample marge d'appréciation pour choisir le meilleur moyen de protéger la sécurité nationale.

1.2.3. Cadre constitutionnel

Les dispositions législatives de l'article L. 851-1 du code de la sécurité intérieure, qui permettent aux services de renseignement d'accéder, à certaines conditions, aux données de connexion conservées de manière généralisée par les opérateurs – et donc, implicitement mais nécessairement, le principe même d'une telle conservation, également prévu aux articles L.34-1 du CPCE et 6 de la LCEN (v. CE ass. 21 avr. *French data Network et a*., n° 393099, 394922, 397844, 397851, 424717, 424718, préc.) – ont été jugées conformes à la Constitution par le Conseil constitutionnel, à la lumière de l'ensemble des droits, libertés, principes et objectifs à valeur constitutionnelle, conformément à son office (décision n° 2015-713 DC du 23 juillet 2015). Ce faisant, validant les techniques de recueil de renseignement permettant l'accès aux données de connexion conservées, il a validé implicitement leur conservation.

En outre, le Conseil constitutionnel avait déjà eu l'occasion de valider l'accès aux données de connexion par diverses administrations. Il avait, notamment, jugé conforme à la Constitution, dans son principe, le dispositif de réquisition d'accès aux données de connexion prévu par l'article 6 de la loi n° 2006-64 du 23 janvier 2006, dont est issu l'article L. 851-1 (décision n° 2005-532 DC du 19 janvier 2006).

Par ailleurs, le Conseil constitutionnel a été amené à reconnaître plusieurs principes et objectifs constitutionnels de nature à justifier que des données à caractère personnel soient conservées ou réquisitionnées par une autorité publique. Il en est ainsi de l'exigence constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire (décision n° 2011-192 QPC du 10 novembre 2011), l'objectif à valeur constitutionnelle de prévention des infractions et de recherche des auteurs d'infraction pénale (décision n° 2004-492 DC du 2 mars 2004) et, enfin, l'objectif de lutte contre le terrorisme, composante de l'objectif à valeur constitutionnelle de protection de l'ordre public (décisions n° 2017-691 QPC du 16 février 2018 et n° 2017-695 du 29 mars 2018).

1.2.4. La décision du Conseil d'État, après question préjudicielle

Le Conseil d'État a, par une décision de l'Assemblée du contentieux du 21 avril 2021 (*French data Network et a*., n° 393099, 394922, 397844, 397851, 424717, 424718) tracé les modalités de transposition, en droit interne, des décisions précitées de la CJUE et plus particulièrement de l'arrêt rendu sur sa question préjudicielle, *La Quadrature du Net*, du 6 octobre 2020.

Il a d'abord considéré qu'il ressort 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 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 constitutionnel, nécessaires à la sauvegarde de droits et de principes de même valeur et 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.

Or, considère le Conseil d'État, ces exigences constitutionnelles, qui s'appliquent à des domaines relevant exclusivement ou essentiellement de la compétence des Etats 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. Faisant application de sa jurisprudence *Arcelor* (8 février 2007, *Société Arcelor Atlantique Lorraine*, n°287110), il considère dès lors qu'il lui revient d'examiner si, en écartant la règle de droit national contestée au motif de sa contrariété avec le droit de l'Union européenne, il priverait de garanties effectives ces exigences constitutionnelles dont le défendeur se prévaut et, le cas échéant, d'écarter le moyen dont le requérant l'a saisi.

Le Conseil d'État a donc appliqué cette grille de lecture aux différentes modalités de conservation des données de connexion applicables en France.

S'agissant des données relatives à l'identité civile, **aux paiements et aux comptes de l'abonné**, le Conseil d'État relève, comme la CJUE, qu'elles 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.

S'agissant des adresses IP, si leur conservation généralisée et indifférenciée ne saurait être justifiée par les besoins de la lutte contre l'ensemble des infractions pénales, mais uniquement pour les besoins de la lutte contre la criminalité grave, il a considéré en revanche, que le législateur n'est pas 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 qui fait application du principe de proportionnalité consacré par l'article préliminaire du code de procédure pénale, 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.

S'agissant des autres données de connexion, le Conseil d'État distingue selon que cette conservation est opérée aux fins de sauvegarde de la sécurité nationale ou aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public.

S'agissant de sauvegarde de la sécurité nationale, la CJUE a défini cette notion comme « 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 ». En écho, le Conseil d'État estime que cette notion

doit être « 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 ».

Le Conseil relève ensuite, avec la CJUE, que l'objectif de sauvegarde de la sécurité nationale peut justifier une conservation généralisée et indifférenciée des données de connexion lorsque pèse sur elle une menace grave, actuelle ou prévisible.

Par suite, en l'état actuel de la menace grave qui pèse sur la France, analysée par le Conseil d'État dans son arrêt au regard de la persistance d'un risque terroriste élevé ainsi qu'en témoigne les attentats perpétrés ou empêchés récemment, exposition au risque d'espionnage et d'ingérence étrangère en raison notamment des capacités de la France et de ses engagements militaires et de son potentiel technologique et économique ainsi que menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes, cette conservation généralisée et indifférenciée, prévue à l'article L. 34-1 du CPCE et à l'article 6 de la LCNE et, au niveau réglementaire, par l'article R. 10-13 du CPCE, est bien justifiée. Néanmoins, dès lors que l'état de cette menace et, par suite, la nécessité de l'injonction de conservation (qui ne peut excéder un an) doivent être régulièrement réévalués, il considère que les dispositions législatives précitées ainsi que les dispositions réglementaires prises pour leur application méconnaissent le droit de l'Union européenne en tant que leurs dispositions ne prévoient pas un réexamen périodique de l'existence d'une menace grave, actuelle ou prévisible pour la sécurité nationale.

S'agissant de la lutte contre la criminalité et la prévention des menaces à l'ordre public, le Conseil d'État rappelle que si la CJUE estime que ces objectifs ne sauraient justifier une conservation généralisée et indifférenciée des données de connexion, et ce, quel que soit le degré de gravité de cette criminalité ou de ces menaces et n'admet qu'une conservation ciblée de ces données pour la seule lutte et répression de la criminalité grave, une telle conservation ciblée, à supposer qu'elle soit techniquement réalisable, ferait obstacle à l'action des services d'enquête et serait contraire au principe constitutionnel d'égalité devant la loi.

En outre, si la CJUE admet que la lutte contre la criminalité et la prévention des menaces à l'ordre public peut justifier une « conservation rapide » des données de connexion, encore faut-il que ces données aient été conservées. Dès lors que, en l'absence de conservation de ces données pour un autre motif, cette conservation rapide ne peut concerner que les données émises à compter de la date et de l'heure à laquelle il est enjoint à un opérateur d'y procéder, un tel dispositif ne présentera un intérêt que si les données ont été effectivement conservées par ailleurs.

Le Conseil d'État en déduit donc 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.

Il ajoute toutefois que, tant que la France sera soumise à une menace grave actuelle ou prévisible sur sa sécurité nationale, le mécanisme de conservation rapide pourra s'appliquer aux données conservées à ce titre. Aussi, tant que cette menace perdure, l'autorité judiciaire et les 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 sont 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. Par conséquent, en l'état actuel de la menace, il n'y a pas lieu de considérer que la mise à l'écart des dispositions législatives qui imposent une conservation généralisée et indifférenciée des données de connexion à des fins judiciaires, au motif qu'elles seraient contraires au droit de l'Union européenne, priverait de garanties effectives les objectifs de valeur constitutionnelle invoqués.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

Dans sa décision précitée, le Conseil d'État désigne plusieurs dispositions législatives qui sont contraires au droit de l'Union européenne et qu'il appartient, par conséquent, au législateur de modifier.

Il s'agit tout d'abord des dispositions des articles L. 34-1 du CPCE et de l'article 6 de la LCEN qui fixent les motifs pour lesquels les opérateurs et les fournisseurs d'accès à internet peuvent différer l'effacement des données de connexion, et donc de les conserver de manière généralisée et indifférenciée hors cas de menace grave, actuelle ou prévisible sur la sécurité nationale. Cela concerne en particulier le III de l'article L. 34-1 qui impose cette conservation notamment pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, ou d'un manquement à l'obligation de respect du droit d'auteur sur internet 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.

Par ailleurs, la CJUE et le Conseil d'État ayant précisé le cadre juridique permettant de procéder à la conservation généralisée et indifférenciée des données de connexion, en cas de menace grave, il convient que le législateur en tire les conséquences, au moyen d'une disposition précise et encadrée.

En outre, il importe de prévoir que les autorités qui disposent actuellement, en vertu de la loi, d'un droit d'accès aux données de connexion conservées par les opérateurs, peuvent enjoindre une « conservation rapide » de ces données, dans une finalités de répression de la criminalités graves ou des manquements graves aux règles dont elles ont la charge d'assurer le respect.

Enfin, il convient également de préciser les catégories de données de connexion pouvant être conservées de manière plus large au regard de leur nature, à savoir les informations relatives à l'identité des utilisateurs, les informations fournies lors de la souscription du contrat et les adresses IP.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

3.1.1. Les modalités de conservation

Il aurait pu être envisagé, comme le suggère la CJUE, de prévoir un cadre de conservation ciblé des données à des fins judiciaires ou de renseignement, applicable en l'absence de menace grave, actuelle ou prévisible sur la sécurité nationale, en ciblant par exemple les personnes au regard de leurs condamnations passées ou de leur inscription dans un fichier à finalité de prévention de la récidive ou de souveraineté ou en ciblant certaines données de connexion en fonction de leur zone géographique d'émission, ces zones étant définies au regard de la prévalence des infractions graves.

Toutefois, au-delà des obstacles techniques dirimants relevés par ailleurs par le Conseil d'État dans sa décision et de la méconnaissance du principe d'égalité devant la loi qu'elle induirait, les moyens des services de renseignement ou de l'autorité judiciaire et leur efficacité variant en fonction de ce ciblage, cette solution se heurte également à des considérations de confidentialité dès lors qu'un tel ciblage nécessiterait de communiquer aux opérateurs de communications électroniques la liste des personnes dont l'État estime qu'elles sont susceptibles de constituer une menace pour la sécurité publique ou de commettre des infractions ou la liste de zones plus exposées à la criminalité grave.

Par ailleurs, de telles listes sont nécessairement amenées à évoluer, en fonction de l'évolution du ciblage, ne serait-ce que pour faire échec aux tentatives de contournement des personnes surveillées. Outre la difficulté technique, pour les opérateurs, de mettre à jour, en permanence, les listes inhérentes à ce ciblage, s'ajoute le coût de tels traitements, à la charge de l'État.

Cette solution n'est donc pas apparue de nature à garantir l'effectivité des exigences constitutionnelles de prévention des atteintes à l'ordre public et de recherche des auteurs d'infraction.

Par ailleurs, le Conseil d'État ayant admis l'existence d'une menace grave actuelle ou prévisible pesant sur la sécurité nationale depuis de nombreuses années, au regard de la persistance d'un risque terroriste élevé ainsi qu'en témoigne les attentats perpétrés ou empêchés récemment, exposition au risque d'espionnage et d'ingérence étrangère en raison notamment des capacités de la France et de ses engagements militaires et de son potentiel technologique et économique ainsi que menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes, il a été considéré que seule cette hypothèse de conservation des données de connexion pouvait être envisagée.

Enfin, si le Conseil d'État a traduit, dans sa décision, la notion de menace pesant sur la sécurité nationale retenue par la CJUE comme devant être « *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* », il a été préféré la notion de « menace pesant sur la sécurité nationale » à celle de « menace

pesant sur les intérêts fondamentaux de la Nation » afin de permettre d'englober, au titre de cette injonction de conservation, les besoins des services du renseignement pénitentiaire créé par l'article L. 855-1 du code de la sécurité intérieure, qui ont pour mission la collecte et l'exploitation du renseignement dans les domaines de la lutte antiterroriste, de la lutte contre la criminalité organisée et du renforcement de la sécurité pénitentiaire (notamment prévention des émeutes et des évasions) et participent, de ce fait, à la prévention des atteintes à la sécurité nationale.

3.1.2. Le niveau de norme imposant la conservation en cas de menace grave, actuelle et prévisible, sur la sécurité nationale

S'il appartient au législateur de définir avec précision les conditions dans lesquelles pèse sur les opérateurs de communications électroniques une obligation de conservation des données de connexion et d'assortir ce dispositif de garanties suffisantes pour assurer le respect des droits et libertés constitutionnellement garantis (en particulier le droit au respect de la vie privée), la Constitution confère au pouvoir exécutif des responsabilités particulières en matière de protection des intérêts fondamentaux de la Nation, ce qui justifie que la loi lui confie le pouvoir de décision en matière de renseignement.

En vertu de l'article 5 de la Constitution, le Président de la République est le garant de l'indépendance nationale et de l'intégrité du territoire. L'article 20 de la Constitution prévoit en outre que « *le Gouvernement détermine et conduit la politique de la Nation* » et « *dispose de l'administration et de la force armée* », tandis que l'article 21 prévoit que le Premier ministre « *dirige l'action du Gouvernement* » et « *est responsable de la Défense nationale* ». Ceci justifie que le pouvoir de décision soit confié au Premier ministre, s'agissant d'une matière relevant en outre de la police administrative et, partant, de la seule responsabilité du pouvoir exécutif (décision n°2005-532 DC, cons. 5).

Dès lors, le pouvoir d'injonction aux opérateurs en matière de sécurité nationale paraît naturellement relever des prérogatives de l'exécutif, l'option consistant en une injonction directement fixée par la loi se heurtant à l'exigence d'une réitération au moins une fois par an qui n'est pas nécessairement compatible avec les contraintes du calendrier parlementaire.

Tout en respectant le principe de séparation des pouvoirs, la solution de niveau réglementaire, qui permet de contester directement l'injonction devant le juge administratif, y compris en urgence, et d'en demander l'abrogation à tout moment (le refus d'abroger pouvant lui-même être contesté), ouvre de larges possibilités de contrôle sur la mesure. Le Gouvernement sera en outre amené à rendre compte de son action en la matière suivant les mécanismes de contrôle parlementaire prévus par la Constitution.

3.1.3. Le contrôle juridictionnel sur l'injonction de conservation

L'article L. 841-1 du code de la sécurité intérieure a prévu une procédure spécifique pour connaître des requêtes concernant la mise en œuvre des techniques de renseignement

mentionnées au titre V du livre VIII du même code. La juridiction compétente est une formation spécialisée du Conseil d'État, dont les juges sont habilités ès qualité au secret de la défense nationale.

Le recours à cette juridiction et à la procédure, prévue à l'article L. 773-2 du code de justice administrative, fondée sur le principe d'un contradictoire asymétrique, a été envisagé comme permettant au juge d'exercer un contrôle de proportionnalité sur l'existence d'une menace grave, actuelle ou prévisible telle qu'exigée par la loi, en lui permettant de disposer d'éléments d'information éventuellement couverts par le secret de la défense nationale.

Toutefois, une telle option n'a pas été retenue, le contrôle juridictionnel relevant du droit commun, dès lors qu'en tout état de cause, l'article L. 5 du code de la justice administrative permet, le cas échéant, d'adapter les exigences du débat contradictoire à celles de la défense nationale.

3.2. DISPOSITIF RETENU

Est en premier lieu supprimée toute possibilité d'effacement différé des données de connexion par les opérateurs de communication électroniques, non justifiée par leur besoin de facturation d'une part ou par l'existence d'une menace grave actuelle ou prévisible sur la sécurité nationale d'autre part. Sont ainsi supprimées les dispositions du III de l'article L. 34-1 du CPCE, qui permettaient de différer d'un an cet effacement pour les besoins de l'autorité judiciaire, de l'HADOPI et de l'ANNSI ainsi que les dispositions du II de l'article 6 de la LCEN qui l'imposaient pour l'autorité judiciaire.

Sont ensuite regroupées dans un nouveau II *bis* de l'article L. 34-1 du CPCE les règles de conservation des données les moins sensibles et qui peuvent, à ce titre, faire l'objet d'une conservation généralisée pour diverses finalités. Il s'agit, 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, des informations relatives à l'identité civile de l'utilisateur, conservées jusqu'à l'expiration d'un délai de cinq ans après la fin de validité de son contrat, pour les mêmes finalités, des autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte, ainsi que des informations relatives au paiement, conservées jusqu'à l'expiration d'un délai d'un an après la fin de validité de son contrat ou la clôture de son compte, et enfin, pour les besoins de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, des données techniques permettant d'identifier la source de la connexion ou relatives aux équipements terminaux de connexion utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux.

De plus, le nouveau III de l'article L. 34-1 du CPCE, prévoit l'hypothèse dans laquelle il peut être fait obligation d'une conservation généralisée et indifférenciée des données de connexion pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée menace grave, actuelle ou prévisible contre cette dernière. Cette conservation est strictement encadrée :

- elle doit être décidée par décret du Premier ministre au regard de l'existence d'une menace grave, actuelle ou prévisible, pour la sécurité nationale ;
- la durée de cette injonction de conservation ne peut excéder un an ;
- elle peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies ;
- elle doit, en tout état de cause, faire l'objet d'une réévaluation annuelle ;
- cette injonction et ses renouvellements font l'objet d'un contrôle du Conseil d'État qui peut être saisi de conclusions en annulation du décret la prononçant, mais également et à tout moment, de conclusions dirigées contre un refus d'abrogation de ce décret ;
- l'éventuelle expiration ou abrogation de l'injonction de conservation générale et indifférenciée est sans incidence sur la durée de conservation de chacune des données qui est fixée à un an.

En outre, les données conservées par les opérateurs peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant en vertu de la loi d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect afin d'y accéder.

Enfin, un décret en Conseil d'État précisera, comme le fait actuellement l'article R. 10-13 CPCE, celles des données qui font l'objet d'une conservation, notamment au titre de la menace grave ainsi que les modalités de compensation des surcoûts induits par cette conservation pour les opérateurs.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

L'article L. 34-1 du code des postes et communications électronique et l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique sont modifiés.

4.2. IMPACTS SUR LES ENTREPRISES

Les coûts induits pour les opérateurs par ces règles de conservation des données de connexion seront compensés financièrement par l'État, dans des conditions similaires à celles actuellement prévues par le cadre réglementaire.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée, à la Commission nationale informatique et liberté, à la Commission nationale de contrôle des techniques de renseignement et à l'Autorité de régulation des communications électroniques et de la distribution de la presse qui ont émis leur avis le 30 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application de la loi dans le temps

Ces mesures s'appliqueront dès la publication de la loi.

5.2.2. Application de la loi dans l'espace

Cette mesure s'applique sur l'ensemble du territoire

5.2.3. Textes d'application

Les nouvelles dispositions appellent l'adoption d'un décret en Conseil d'Etat qui déterminera, selon l'activité des opérateurs et la nature des communications, les informations et catégories de données conservées en application des II *bis* et III de l'article L. 34-1 du CPCE, ainsi que les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs.

Article 16 : Procédure de contrôle préalable à la mise en œuvre des techniques de renseignement sur le territoire national

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 821-1 du code de la sécurité intérieure prévoit que la mise en œuvre sur le territoire national d'une technique de recueil de renseignement est soumise à autorisation préalable du Premier ministre, délivrée après avis d'une autorité administrative indépendante, la Commission nationale de contrôle des techniques de renseignement (CNCTR).

La demande écrite et motivée de mise en œuvre d'une technique de renseignement est présentée par le ministre dont relève le service de renseignement qui la sollicite, cette attribution ne pouvant être déléguée qu'à des collaborateurs directs habilités au secret de la défense nationale.

Elle est transmise au président de la commission (ou, à défaut, à l'un de ses membres désigné parmi ceux qui sont issus du Conseil d'Etat ou de la Cour de cassation), qui rend son avis au Premier ministre dans un délai de vingt-quatre heures.

Dans trois cas particuliers, la demande est examinée en formation restreinte (composée du président et des membres issus du Conseil d'Etat et de la Cour de cassation) ou plénière de la commission :

- lorsqu'elle soulève une question nouvelle ou sérieuse, ou si la validité de la demande n'est pas certaine (article L. 832-3) ;
- lorsqu'elle porte sur l'introduction dans un lieu privé (article L. 853-3) à usage d'habitation ou en vue de la mise en œuvre de la technique prévue au 1° du I de l'article L. 853-2 (recueil de données stockées dans un système informatique) ;
- lorsqu'elle concerne une personne exerçant une profession ou un mandat bénéficiant d'une protection particulière (parlementaire, magistrat, avocat, journaliste), ses véhicules, ses bureaux ou ses domiciles (article L. 821-7) ; dans ce cas, seule la formation plénière est compétente.

Dans ces cas de figure, l'avis de la commission est rendu dans un délai de 72 heures. La formation restreinte et la formation plénière ne peuvent valablement délibérer que si, respectivement, au moins trois et quatre membres sont présents.

Dans l'hypothèse où l'avis ne serait pas transmis au Premier ministre dans les délais prévus par la loi, l'avis est alors réputé rendu.

Une fois l'autorisation délivrée par le Premier ministre, la technique de renseignement concernée peut être immédiatement mise en œuvre par le service à l'origine de la demande. Dans le cas où l'autorisation aurait été délivrée en dépit d'un avis défavorable de la CNCTR, elle indique les motifs pour lesquels cet avis n'a pas été suivi. La commission peut alors, en application de l'article L. 833-8 du code de la sécurité intérieure, saisir la formation spécialisée

du Conseil d'Etat[32] mentionnée à l'article L. 773-2 du code de justice administrative afin que celle-ci en contrôle la légalité et, le cas échéant, en suspende l'exécution ou l'annule dans les conditions prévues par le code de justice administrative.

Il convient de souligner que si, en droit, l'avis de la CNCTR n'est pas contraignant, il est, en pratique, systématiquement suivi par le Premier ministre.

Ce cadre général est ainsi marqué par deux caractéristiques :

- le Premier ministre ne peut décider sans avoir recueilli l'avis d'une autorité administrative indépendante ;
- cet avis est non contraignant, de sorte que les décisions du Premier ministre bénéficient du privilège du préalable et sont immédiatement exécutoires.

Deux tempéraments sont néanmoins prévus par la loi :

Absence d'effet exécutoire de l'autorisation du Premier ministre en cas d'avis défavorable de la CNCTR à une demande d'introduction dans un lieu privé à usage d'habitation

L'article L. 853-3 du code de la sécurité intérieure prévoit une règle spéciale pour le cas où l'avis rendu par la formation restreinte de la CNCTR serait défavorable à l'introduction dans un lieu privé à usage d'habitation. Dans une telle hypothèse (qui ne s'est jamais produite depuis l'entrée en vigueur de la loi), le Conseil d'État est immédiatement saisi par le président de la commission ou l'un des membres mentionnés aux 2° et 3° de l'article L. 831-1 et statue, dans un délai de vingt-quatre heures, sur ce recours.

Cette saisine est obligatoire, la commission étant tenue d'y procéder ; elle est également suspensive, l'autorisation du Premier ministre ne pouvant alors être exécutée avant que le Conseil d'État n'ait statué. Il ne peut en aller autrement que si l'autorisation a été délivrée au titre de la prévention du terrorisme et que le Premier ministre en a ordonné la mise en œuvre immédiate.

Dispense d'avis préalable de la CNCTR en cas d'urgence absolue

Par dérogation à l'article L. 821-1 du code de la sécurité intérieure, l'article L. 821-5 prévoit que le Premier ministre peut, en cas d'urgence absolue, délivrer l'autorisation de mise en œuvre de la technique de renseignement sans avis préalable de la CNCTR. Cette procédure dérogatoire est, néanmoins, strictement encadrée et ne peut trouver à s'appliquer, aux termes de la loi, que « *de manière exceptionnelle* » :

[32] Dont les membres sont habilités ès qualité au secret de la défense nationale et qui disposent des pouvoirs d'instruction les plus larges pour contrôler la régularité de la mise en œuvre des techniques de renseignement, sur saisine de la CNCTR ou de toute personne souhaitant vérifier qu'elle ne fait pas irrégulièrement l'objet d'une telle mise en œuvre.

- elle n'est ouverte que pour trois finalités (indépendance nationale, intégrité du territoire et défense nationale ; prévention du terrorisme ; prévention des atteintes à la forme républicaine des institutions) ;
- elle est exclue pour certaines techniques de renseignement (détection en temps réel, prévue à l'article L. 851-2 ; algorithme, prévu à l'article L. 851-3 ; introduction dans un lieu privé, prévue à l'article L. 853-3, lorsque ce lieu est à usage d'habitation ou qu'il s'agit de procéder au recueil de données informatiques[33]) ;
- elle est également exclue, quelle que soit la technique ou la finalité, lorsque la demande concerne une profession ou un mandat protégés par l'article L. 821-7.

S'il met en œuvre cette procédure, le Premier ministre doit faire parvenir à la commission, dans un délai maximal de vingt-quatre heures à compter de la demande d'autorisation, tous les éléments de motivation fournis à l'appui de celle-ci ainsi que ceux justifiant l'urgence absolue.

En pratique, le Premier ministre n'a eu recours qu'une seule fois à la procédure de l'article L.821-5. En dehors de ce cas, aucune autorisation n'a été délivrée sans avis préalable de la CNCTR. Le dispositif interne d'astreinte suivant lequel la commission s'est organisée lui permet de rendre un avis à tout moment et dans des délais très restreints, sur sollicitation du groupement interministériel de contrôle, service du Premier ministre auquel parviennent les demandes.

L'arrêt de grande chambre de la Cour de justice de l'Union européenne en date du 6 octobre 2020 (*La Quadrature du Net*, C-511/18) comme la décision d'assemblée du Conseil d'Etat en date du 21 avril 2021, qui en tire les conséquences (Ass., *French Data Network et autres*, n° 393099) nécessitent de revoir ce cadre général ainsi que les tempéraments dont il est assorti. Ces deux juridictions ont en effet jugé contraire au droit de l'Union européenne la possibilité de mettre en œuvre certaines techniques de renseignement 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.

1.2. CADRE CONSTITUTIONNEL

D'une part, la mise en œuvre des techniques de renseignement doit être entourée de garanties suffisantes définies par la loi.

Il appartient en effet au législateur de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Il lui incombe en particulier d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et des infractions, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et des libertés constitutionnellement garantis. Au nombre de ces derniers figurent le droit au respect de la vie privée, l'inviolabilité du domicile et le secret des correspondances, protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789. Ceci justifie en particulier l'organisation d'un contrôle par une autorité

[33] Cf. considérants 72 et 73 de la décision n°2005-532 DC du Conseil constitutionnel.

indépendante sur la mise en œuvre des techniques de renseignement et nécessite l'aménagement de règles permettant de garantir le droit au recours effectif.

D'autre part, la Constitution confère au pouvoir exécutif des responsabilités particulières en matière de protection des intérêts fondamentaux de la Nation, ce qui justifie que la loi lui confie le pouvoir de décision en matière de renseignement.

En vertu de l'article 5 de la Constitution, le Président de la République est le garant de l'indépendance nationale et de l'intégrité du territoire. L'article 20 de la Constitution prévoit en outre que « *le Gouvernement détermine et conduit la politique de la Nation* » et « *dispose de l'administration et de la force armée* », tandis que l'article 21 prévoit que le Premier ministre « *dirige l'action du Gouvernement* » et « *est responsable de la Défense nationale* ». Ceci justifie que le pouvoir de décision soit confié au Premier ministre, s'agissant d'une matière relevant en outre de la police administrative et, partant, de la seule responsabilité du pouvoir exécutif (décision n°2005-532 DC, cons. 5), et qu'aucune technique de renseignement ne puisse être mise en œuvre sans son autorisation préalable[34].

Ainsi, dans le cadre du contrôle *a priori* de la loi relative au renseignement du 23 juillet 2015, le Conseil constitutionnel a rejeté le grief tiré de ce que les dispositions de l'article L. 821-1 du code de la sécurité intérieure, en permettant que l'autorisation puisse être délivrée en dépit d'un avis défavorable de la CNCTR, présenteraient des garanties insuffisantes au regard des droits et libertés constitutionnellement garantis. Il a motivé sa décision en rappelant les garanties applicables (demande motivée, avis préalable d'une autorité indépendante, mise en œuvre pour une durée maximale de quatre mois par des agents individuellement désignés et habilités) et relevé que « *le législateur s'est fondé sur l'article 21 de la Constitution pour confier au Premier ministre le pouvoir d'autoriser la mise en œuvre des techniques de recueil de renseignement dans le cadre de la police administrative* » (décision n° 2015-713 DC, cons. 16 à 22). Il a également déclaré conformes à la Constitution, compte tenu des garanties qu'elles prévoient, les dispositions de l'article L. 821-5 relatives à la procédure d'urgence absolue (même décision, cons. 23 à 26).

La jurisprudence constitutionnelle donne encore d'autres indications sur les conditions dans lesquelles doivent être articulés les prérogatives constitutionnelles de l'exécutif et les pouvoirs de contrôle dont sont dotées les autorités administratives indépendantes. Ainsi, s'agissant de l'exercice du pouvoir réglementaire, confié au Premier ministre par l'article 21 de la Constitution, le Conseil constitutionnel pose en principe qu'il ne peut être subordonné à l'avis

[34] A cet égard, il convient de rappeler que le Conseil constitutionnel a censuré l'article L. 821-6 du code de la sécurité intérieure, qui permettait la mise en œuvre sans avis préalable de la CNCTR ni autorisation du Premier ministre de certaines techniques de renseignement « *en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement* ». Relevant notamment que cette procédure ne prévoyait pas non plus l'information du Premier ministre et du ministre concerné préalablement à la mise en œuvre d'une technique dans ce cadre, il a jugé que ces dispositions portaient une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances (décision n° 2015-713 DC, cons. 27 à 29).

conforme d'une autorité de l'Etat autre que le Premier ministre (voir décisions n° 2006-544 DC, cons. 35 à 38 ; n° 2015-715 DC, cons. 45 ; n° 2020-800 DC).

Le Conseil constitutionnel a toutefois déclaré conformes à la Constitution les dispositions du III de l'article L. 853-3 du code de la sécurité intérieure faisant obstacle, jusqu'à l'intervention de la décision du Conseil d'Etat, à l'exécution immédiate d'une décision du Premier ministre autorisant l'intrusion dans un lieu privé à usage d'habitation en cas d'avis défavorable de la CNCTR sur la demande de mise en œuvre de cette technique (décision n° 2015-713, cons. 73), en considérant que le législateur avait ainsi « *entouré la mise en œuvre des techniques prévues aux articles L. 853-1 à L. 853-3, lorsqu'elles imposent l'introduction dans un lieu privé à usage d'habitation, de dispositions de nature à garantir que les restrictions apportées au droit au respect de la vie privée et à l'inviolabilité du domicile ne revêtent pas un caractère manifestement disproportionné* ».

1.3. CADRE EUROPEEN

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 soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante* ». Le point 120 de cet arrêt précise qu' « *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* ».

Saisi par le Conseil d'Etat d'une question préjudicielle relative à la conformité au droit de l'Union européenne des dispositions des articles L. 851-2 à L. 851-4 du code de la sécurité intérieure, la Cour de justice a rappelé cette règle dans son arrêt du 6 octobre 2020 susmentionné à propos du recueil en temps réel des données de connexion par les services de renseignement, tout en réservant le cas de l'urgence dûment justifiée. Elle a ainsi considéré qu' « *une décision autorisant le recueil en temps réel des données relatives au trafic et des données de localisation doit être fondée sur des critères objectifs et non discriminatoires prévus dans la législation nationale. Aux fins de garantir, en pratique, le respect de ces conditions, il est essentiel que la mise en œuvre de la mesure autorisant le recueil en temps réel soit soumise à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, cette juridiction ou cette entité devant notamment s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et*

C-698/15, EU:C:2016:970, point 120). En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais. »

Tirant les conséquences de cette jurisprudence européenne, le Conseil d'Etat a jugé, par sa décision susmentionnée en date du 21 avril 2021, 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* » (§ 69).

Il a jugé de même s'agissant des techniques mises en œuvre en application du IV de l'article L. 851-3 (identification au moyen d'un algorithme des personnes dont les données de connexion sont susceptibles de révéler une menace terroriste et recueil des données de connexion correspondantes), de l'article L. 851-2 (détection en temps réel) et de l'article L. 851-4 (géolocalisation en temps réel).

Par conséquent, le Conseil d'Etat a annulé les décrets pris pour l'application des articles L. 851-1, L. 851-2, L. 851-4 et du IV de l'article L. 851-3 en tant seulement qu'ils permettent la mise en œuvre 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* ».

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

Il est nécessaire, pour tirer les conséquences de la jurisprudence de la Cour de justice de l'Union européenne et du Conseil d'Etat, de modifier les dispositions législatives relatives au renseignement afin de les mettre en conformité avec le droit de l'Union européenne pour :

- d'une part, renforcer le contrôle préalable à la mise en œuvre des techniques de renseignement concernées, en prévoyant qu'il est assuré par une autorité administrative indépendante dont les décisions sont dotées d'un effet contraignant ou par une juridiction ;

- d'autre part, adapter les conditions dans lesquelles il peut être dérogé à ce contrôle préalable en cas d'urgence dûment justifiée.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Plusieurs options sont envisageables s'agissant :

- du champ d'application de la procédure de contrôle préalable renforcé ;
- des modalités du contrôle préalable ;
- des modalités de la procédure d'urgence dûment justifiée.

En ce qui concerne le champ d'application de la procédure de contrôle préalable renforcé

La décision du Conseil d'Etat ne concerne directement que les techniques de renseignement prévues aux articles L. 851-1, L. 851-2, L. 851-4 et par le IV de l'article L. 851-3.

La compatibilité des dispositions relatives aux autres techniques de renseignement mises en œuvre sur le territoire national avec le droit de l'Union européenne (à supposer qu'il s'applique à elles) n'a été examinée ni par la Cour de justice de l'Union européenne ni par le Conseil d'Etat, de sorte qu'il pourrait théoriquement être envisagé de ne pas leur appliquer la procédure renforcée.

A l'inverse, leur caractère au moins aussi intrusif et attentatoire au droit au respect de la vie privée que celles qui ont été examinées par les deux juridictions, ainsi que la cohérence et la lisibilité du dispositif, peuvent inciter à leur appliquer les mêmes garanties.

En revanche, la décision du Conseil d'Etat a clairement jugé que le droit de l'Union européenne ne s'applique pas aux techniques mises en œuvre en application du chapitre IV du titre V du livre VIII du code de la sécurité intérieure, relatif à la surveillance des communications électroniques internationales (§ 95), de sorte que les dispositions législatives en la matière n'ont pas à être modifiées.

En ce qui concerne les modalités du contrôle préalable

S'agissant de l'autorité compétente pour exercer ce contrôle préalable contraignant, la jurisprudence de la CJUE et du Conseil d'Etat ouvre une alternative.

Il peut s'agir :

- soit d'une autorité administrative indépendante (en l'espèce, la CNCTR) dotée d'un avis conforme,
- soit d'une juridiction (en l'espèce, la formation spécialisée du Conseil d'Etat).

Il est possible, en conséquence, de choisir de généraliser le dispositif prévu au III de l'article L. 853-3 du code de la sécurité intérieure en ce qui concerne l'introduction dans un lieu privé à usage d'habitation. Il prévoit que le juge est obligatoirement et immédiatement saisi par la CNCTR d'un recours suspensif en cas d'autorisation délivrée par le Premier ministre en dépit d'un avis défavorable de la commission. Ainsi, c'est le juge qui trancherait, sous vingt-quatre heures, le désaccord entre le Premier ministre et la CNCTR.

En toute hypothèse, l'avis conforme de l'autorité indépendante ou l'autorisation du juge doivent intervenir aussi rapidement que possible, afin de garantir la préservation des intérêts fondamentaux de la Nation auxquels concourt la mise en œuvre des techniques de renseignement.

En ce qui concerne le champ d'application et les modalités de la procédure d'urgence dûment justifiée.

Deux options paraissent envisageables.

Une première option peut consister à maintenir ou, en contrepartie de l'introduction d'une procédure d'avis conforme par la CNCTR ou d'autorisation préalable par le juge, à élargir les cas dans lesquels la procédure d'urgence absolue prévue à l'article L. 821-5 du code de la sécurité intérieure, permet de se dispenser à titre exceptionnel de l'avis préalable de la CNCTR.

Un tel élargissement ne serait pas contraire au droit de l'Union européenne : la Cour de justice de l'Union européenne, au § 189 de l'arrêt du 6 octobre 2020, a précisément autorisé que, dans les cas d'urgence dûment justifiée, le contrôle de l'autorité indépendante ou de la juridiction intervienne, non pas à titre préalable, mais dans de brefs délais et a fait ce constat à l'issue de son examen des dispositions de l'article L. 851-2 du code de la sécurité intérieure, pour lesquelles la procédure prévue par l'article L. 821-5 n'est pourtant pas applicable. Toutefois, cet élargissement ne serait pas sans risque constitutionnel, dès lors que la limitation de cette procédure à certaines finalités et son exclusion pour certaines techniques ont été relevées par le Conseil constitutionnel comme des garanties permettant de déclarer cet article conforme à la Constitution.

Une seconde option consiste :

- d'une part, à prévoir la suppression de la procédure d'urgence absolue de l'article L. 821-5,
- d'autre part, à assortir la procédure d'avis conforme de la CNCTR (ou de saisine automatique du juge en cas d'autorisation délivrée en dépit d'un avis défavorable de la CNCTR) d'une clause permettant au Premier ministre d'ordonner néanmoins la mise en œuvre immédiate de l'autorisation sans attendre la décision du juge, en cas d'urgence dûment justifiée auprès de lui par le service de renseignement à l'origine de la demande.

Une telle clause, de nature à préserver les prérogatives constitutionnelles du Premier ministre, serait disponible pour les différentes finalités de l'article L. 811-3 et pour tout ou partie des techniques de renseignement. Elle serait la transposition de celle qui est prévue au III de l'article L. 853-3, pour l'introduction dans un lieu privé à usage d'habitation, pour les seules autorisations délivrées au titre de la finalité de prévention du terrorisme.

3.2. DISPOSITIF RETENU

Le projet de loi prévoit :

- que la procédure de contrôle préalable renforcé s'applique à l'ensemble des techniques de renseignement mises en œuvre sur le territoire national, et non pas seulement à celles d'entre elles qui sont directement visées par la décision du Conseil d'Etat en date du 21 avril 2021 ;

- la suppression de la procédure d'urgence absolue prévue à l'article L. 821-5 du code de la sécurité intérieure, excluant ainsi toute possibilité de mettre en œuvre une technique de renseignement sans que l'avis de la CNCTR ait été préalablement sollicité ;

- que l'autorisation délivrée par le Premier ministre en dépit d'un avis défavorable de la CNCTR ne puisse être exécutée avant que le Conseil d'Etat, obligatoirement saisi par la commission, n'ait statué, dans un délai de vingt-quatre heures ;

- la faculté, pour le Premier ministre, d'ordonner néanmoins, en cas d'urgence dûment justifiée, la mise en œuvre immédiate de la technique qu'il a autorisée en dépit d'un tel avis défavorable, sans attendre que le Conseil d'État se soit prononcé, cette faculté étant :

    - limitée à trois finalités (indépendance nationale, intégrité du territoire, défense nationale ; prévention du terrorisme ; prévention des atteintes à la forme républicaine des institutions) pour les techniques, plus intrusives, prévues aux articles L. 853-1 à L. 853-3 (captation de paroles ou d'images, recueil ou captation de données informatiques ; introduction dans les lieux privés) voire à une seule (prévention du terrorisme) pour l'introduction dans un lieu privé à usage d'habitation ;

    - exclue pour l'application des I et II de l'article L. 851-3 (mise en œuvre de la technique de l'algorithme), qui ne s'inscrit pas dans un contexte de menace imminente mais suppose une élaboration fine des paramètres de l'algorithme en lien étroit avec la CNCTR ;

    - exclue concernant l'une des personnes mentionnées au premier alinéa de l'article L. 821-7, autrement dit un parlementaire, un magistrat, un avocat ou un journaliste, ou ses véhicules, ses bureaux ou ses domiciles.

  En tout état de cause et comme le permet d'ores et déjà la loi en vigueur, dans l'hypothèse où le Conseil d'État, saisi par la CNCTR, jugerait que la technique de renseignement a été mise en œuvre illégalement, il pourra, en application de l'article L.773-7 du code de justice administrative, annuler l'autorisation délivrée par le Premier ministre et ordonner la destruction des renseignements irrégulièrement collectés.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Les modifications proposées assurent la conformité des dispositions relatives au renseignement aux exigences résultant du droit de l'Union européenne telles qu'elles ont été précisées par la Cour de justice de l'Union européenne puis le Conseil d'Etat.

Elles préservent en outre une capacité d'action immédiate au bénéfice du Premier ministre et des services de renseignement en cas d'avis défavorable de la CNCTR à la mise en œuvre d'une technique de renseignement, lorsque l'urgence le justifie.

4.2. IMPACTS SUR LES ADMINISTRATIONS

La suppression de la procédure d'urgence absolue, d'application particulièrement rare, ne devrait pas avoir d'impact majeur sur le fonctionnement des administrations concernées.

Le cabinet du Premier ministre, le GIC et la CNCTR sont en effet organisés suivant un dispositif de permanence et d'astreinte leur permettant un traitement en temps réel des demandes qui leur sont adressées par les services de renseignement.

Dans l'hypothèse où une telle procédure ne pourrait être mise en œuvre au regard de son extrême urgence, le Premier ministre conserverait en tout état de cause la possibilité de faire application de la théorie des circonstances exceptionnelles pour faire face à une situation de crise telle que les délais de ces procédures ne puissent être respectés (CE, 28 juin 1918, *Heyriès*, req. n° 63412).

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS

Le projet de loi a été présenté à la Commission nationale de contrôle des techniques de renseignement en application de l'article L. 833-11 du code de la sécurité intérieure. La Commission a rendu son avis le 30 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ainsi que l'indique le Conseil d'Etat dans sa décision du 21 avril dernier (§ 98), « *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'Etat, qu'il appartiendra alors à la commission de saisir en application de l'article L. 833-8 du même code ». L'application des nouvelles dispositions proposées à compter de l'entrée en vigueur de la loi prendra le relai du dispositif transitoire ainsi défini par le Conseil d'Etat.

5.2.2. Application dans l'espace

Le présent article s'applique sur l'ensemble du territoire national.

Article 17 : Echanges d'informations entre les services judiciaires et les services de renseignement dans le cadre de la lutte contre la cybercriminalité et la criminalité organisée et entre les services judiciaires et l'ANSSI dans le cadre de la lutte contre la cybercriminalité

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article 11 du code de procédure pénale prévoit que, sauf dans le cas où la loi en dispose autrement et sans préjudice des droits de la défense, la procédure au cours de l'enquête et de l'instruction est secrète. Cet article ajoute que toute personne qui concourt à la procédure est tenue au secret professionnel dans les conditions et sous les peines prévues aux articles 226-13 et 226-14 du code pénal.

Plusieurs dispositions législatives dérogent à la règle du secret de l'enquête pour permettre au procureur de la République ou au juge d'instruction de communiquer des informations issues de procédures judiciaires, dans des cas précis encadrés par la loi.

Ainsi, le dernier alinéa de l'article 11 susmentionné prévoit que le procureur de la République peut, d'office et à la demande de la juridiction d'instruction ou des parties, rendre publics des éléments objectifs tirés de la procédure ne comportant aucune appréciation sur le bien-fondé des charges retenues contre les personnes mises en cause, afin d'éviter la propagation d'informations parcellaires ou inexactes ou pour mettre fin à un trouble à l'ordre public.

Par ailleurs, sur autorisation du procureur de la République ou du juge d'instruction selon les cas, peuvent être communiqués à des autorités ou organismes habilités à cette fin par arrêté du ministre de la justice, des éléments des procédures judiciaires en cours afin de permettre la réalisation de recherches ou d'enquêtes scientifiques ou techniques, destinées notamment à prévenir la commission d'accidents, ou de faciliter l'indemnisation des victimes ou la prise en charge de la réparation de leur préjudice[35].

En outre, le ministère public peut informer par écrit l'administration, les personnes publiques, les personnes morales de droit privé chargées d'une mission de service public ou les ordres professionnels des décisions de condamnation, de poursuites devant un tribunal ou de mise en examen rendues contre une personne qu'elles emploient lorsqu'elles concernent un crime ou un délit puni d'une peine d'emprisonnement. Le ministère public ne peut procéder à cette information que lorsqu'il estime cette transmission nécessaire, en raison de la nature des faits

[35] Article 11-1 du code de procédure pénale

ou des circonstances de leur commission, pour mettre fin ou prévenir un trouble à l'ordre public ou pour assurer la sécurité des personnes ou des biens[36].

Enfin, et sans prétendre à l'exhaustivité, l'article 706-25-2 du code de procédure pénale, récemment modifié par la loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée, prévoit que le procureur de la République antiterroriste, pour les procédures d'enquête ou d'instruction ouvertes sur le fondement d'une ou de plusieurs infractions terroristes, peut communiquer aux services spécialisés de renseignement des éléments de toute nature figurant dans ces procédures et nécessaires à l'exercice des missions de ces services en matière de prévention du terrorisme.

Le deuxième alinéa de l'article 706-25-2 dispose que cette communication peut également être réalisée, selon les mêmes modalités et pour les mêmes finalités, à destination des autorités et services compétents pour la prévention du terrorisme par tout procureur de la République pour des procédures ouvertes pour un crime ou un délit puni d'une peine d'emprisonnement, lorsque ces procédures font apparaître des éléments concernant une personne dont le comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes.

1.2. CADRE CONSTITUTIONNEL

À l'occasion d'une question prioritaire de constitutionnalité, le Conseil constitutionnel a admis que le secret de l'enquête et de l'instruction avait deux finalités : *« d'une part, garantir le bon déroulement de l'enquête et de l'instruction, poursuivant ainsi les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions, tous deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle […], d'autre part, protéger les personnes concernées par une enquête ou une instruction, afin de garantir le droit au respect de la vie privée et de la présomption d'innocence, qui résulte des articles 2 et 9 de la Déclaration de 1789 »* [37].

La transmission d'informations, lorsque celles-ci ont la nature de données à caractère personnel, doit donc notamment être appréciée au regard du droit au respect de la vie privée et de la présomption d'innocence.

Par ailleurs, le Conseil constitutionnel estime que, si « *aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire ; que, toutefois, cette utilisation*

[36] Article 11-2 du code de procédure pénale

[37] Décision n° 2017-693 QPC du 2 mars 2018, Association de la presse judiciaire [Présence des journalistes au cours d'une perquisition], paragr. 8.

méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées »[38]

La transmission d'informations nominatives à caractère pénal par l'autorité judiciaire doit être justifiée par des impératifs protégeant d'autres droits ou intérêts de même valeur avec lesquels les droits ou intérêts légitimes des personnes concernées doivent se concilier.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

Les procédures judiciaires peuvent comporter des informations qui, au-delà de leur valeur probatoire au regard d'une infraction commise et poursuivie, révèlent l'existence d'une menace distincte sans que celle-ci se matérialise par la commission d'infractions et peuvent, dès lors, se révéler intéressantes pour les services de renseignement.

Ainsi, une personne condamnée pour infraction à caractère terroriste dans le cadre d'une procédure judiciaire peut également être suivi par un service de renseignement afin de s'assurer de la nature de la menace qu'il représente, à raison de ses contacts, de ses activités, de son endoctrinement ou tout autre critère de nature à entraîner la nécessité d'un suivi administratif.

Au-delà du terrorisme, il apparaît tout aussi nécessaire de favoriser des transmissions d'informations ciblées par l'autorité judiciaire vers les services de renseignement en matière de criminalité organisée ainsi que vers les différents services compétents en matière de lutte contre la cybercriminalité.

Ces deux champs du droit pénal sont définis de manière précise et limitée par le code pénal et le code de procédure pénale, à la fois par un critère matériel (champ des infractions concernées) et par un critère organique, celui de la juridiction compétente.

Ainsi, les articles 706-73 à 706-74 figurant au sein du titre XXV au sein du livre IV du code de procédure pénale intitulé : « *De la procédure applicable à la criminalité et à la délinquance organisées* », recensent les infractions pour lesquelles s'applique cette procédure. S'agissant de la cybercriminalité, il s'agit des infractions pénales commises sur un système de traitement automatisé d'informations mentionnées à l'article 706-72 du code de procédure pénale.

Le tribunal judiciaire de Paris dispose d'une compétence nationale concurrente, en application du dernier alinéa de l'article 706-75 du code de procédure pénale, pour lutter contre la criminalité organisée de très grande complexité et, en application de l'article 706-72-1 du même code pour lutter contre la cybercriminalité.

Les spécificités de ces deux contentieux, qui les distinguent fondamentalement de la criminalité de droit commun, sont multiples et justifient la mise en place d'un dispositif permettant des transmissions plus nourries par l'autorité judiciaire vers les services de renseignement. En

[38] Décision n° 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, cons. 32.

l'absence de cadre légal, une telle démarche est en effet très contrainte, et ce dans un contexte où la prévention et la lutte contre la cybercriminalité et la très grande criminalité organisée ont changé de dimension.

En premier lieu, la prévention et la lutte contre ces deux phénomènes est caractérisée par sa complexité et son caractère international.

Il apparaît en pratique que le parquet de Paris se saisit, au titre de sa compétence nationale, de faits mettant en cause des individus et des organisations criminelles agissant le plus souvent au-delà du territoire national, implantés ou bénéficiant de relais à l'étranger et, pour certains faits, pouvant être commis par certains États (notamment en matière de cybercriminalité) ou avec leur complicité ou une facilitation de leur part (trafic d'êtres humains ou trafics de stupéfiants).

Malgré des mécanismes de coopération judiciaire dont l'efficacité a progressé au cours des années, l'autorité judiciaire nationale est néanmoins parfois limitée dans sa capacité à mener des enquêtes dans les pays d'origine des criminels, surtout lorsque ces derniers choisissent de mener leurs activités depuis des territoires peu coopératifs. Ces particularités sont autant d'obstacles à la conduite de procédures judiciaires efficaces contre une forme de très grande délinquance organisée dont la gravité peut apparaître sans rapport avec sa répression pénale.

Face à de tels phénomènes criminels, la mobilisation collective des services compétents et la complémentarité de leur action sont cruciales. Elles exigent de donner sa pleine effectivité au continuum justice-renseignement-cyber

En second lieu, l'ampleur et la sophistication des phénomènes criminels concernés par la présente disposition ont conduit les enquêteurs à adopter des méthodes et techniques d'enquête innovantes. Les données, notamment numériques ou techniques, issues des procédures judiciaires constituent une source de renseignement majeure pour les services qui, contrairement à leurs principaux partenaires étrangers, ne se les voient pas transmettre et ne sont ainsi pas en situation de compléter la connaissance qu'ils ont de réseaux et des acteurs s'agissant de la criminalité organisée la plus complexe comme de la menace des cyber-attaquants et de leurs modes opératoires. Ce décalage entre les cadres juridiques de différents pays entraîne un décrochage des capacités françaises à lutter contre la cybercriminalité et la très grande criminalité organisée.

Le Gouvernement, conscient de ces évolutions et de l'impact de ces formes de criminalité sur le territoire national, a d'ailleurs confié aux services de renseignement la mission d'analyser et de prévenir ces menaces. Il est, par conséquent, important qu'ils puissent disposer de l'ensemble des moyens et des informations leur permettant d'accomplir leurs missions aux fins de sauvegarde des intérêts fondamentaux de la Nation.

Pour ces raisons, les informations collectées dans le cadre des procédures judiciaires doivent pouvoir être communiquées aux services de renseignement qui ont notamment pour mission, aux termes de l'article L. 811-3 du code de la sécurité intérieure, la prévention de toute forme d'ingérence étrangère et la défense des intérêts économiques, industriels et scientifiques

majeurs de la France et la prévention de la criminalité et de la délinquance organisées ainsi qu'aux services de l'Etat compétents en matière de cyberdéfense pour le strict champ de la lutte contre les menaces cyber.

Par conséquent, le mécanisme existant à l'article 706-25-2 du code de procédure pénale en matière terroriste doit être transposé et adapté au domaine de la criminalité organisée et de la cybercriminalité, afin de permettre une coordination efficace entre le parquet de Paris et les services spécialisés de renseignement afin de lutter de concert contre la cybercriminalité et les formes les plus graves de criminalité organisée.

De même, il apparaît nécessaire de développer les échanges entre les services judiciaires et les services qui interviennent en matière de sécurité et de défense des systèmes d'information dans le cadre de la lutte contre la cybercriminalité, afin notamment de permettre une transmission plus rapide des éléments pour prévenir et caractériser les attaques informatiques et neutraliser leurs effets : il s'agit, chacun agissant dans le cadre de ses missions, des services de renseignement, de l'Agence nationale de sécurité des systèmes d'information (ANSSI), service à compétence nationale rattaché au secrétaire général de la défense et de la sécurité nationale, et du chef d'état-major des armées *via* l'état-major de la cyberdéfense, pour les système d'information du ministère de la défense.

En effet, l'explosion du volume de cyberattaques auquel la France fait face, ainsi que leur sophistication croissante, rendent indispensable une coopération accrue entre l'autorité judiciaire et les services de l'Etat compétents en la matière. Appelée de ses vœux par la revue stratégique de cyberdéfense, cette coopération accrue nécessite un partage d'informations plus dense et plus rapide pour garantir l'efficacité opérationnelle des services d'enquête ainsi que des services de l'Etat compétents en matière de cyberdéfense.

Des obstacles à l'exploitation judiciaire des nombreuses données de nature technique sont observés, malgré leur extrême richesse pour les services de renseignement et pour l'ANSSI. L'exploitation de ces données peut être extrêmement éclairante sur les modes opératoires utilisés par les attaquants. Grâce à leur exploitation, les services compétents de l'Etat sont en mesure de protéger plus efficacement les systèmes d'informations des entités critiques de la Nation en détectant au plus tôt les tentatives d'attaques et en identifiant des victimes potentielles. L'échange d'informations entre les services judiciaires et les services de l'Etat concourant directement à la mission de cyberdéfense se révèle d'autant plus crucial pour lutter contre les menaces cyber que la matière est marquée par la fragmentation et l'obsolescence rapide des éléments d'intérêt. Trop souvent, les acteurs étatiques engagés dans cette lutte disposent d'une vision parcellaire des menaces traitées et des modes opératoires adverses, ce qui nuit à leur efficacité respective et commune. Renforcer le partage d'informations entre ces entités permettra d'obtenir des gains opérationnels significatifs dans le traitement des cyberattaques sur l'ensemble du spectre d'activités de ces services. Plus encore que sur d'autres terrains infractionnels, l'espace cyber exige une très forte réactivité aux menaces identifiées et rend dès lors indispensable la transmission rapide des informations disponibles. C'est en acquérant très rapidement la meilleure compréhension technique d'un phénomène cyber menaçant que les services compétents de l'Etat peuvent prévenir, détecter et traiter ses

conséquences et limiter les dommages notamment en condamnant les accès aux systèmes d'information compromis.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Il aurait pu être envisagé de ne prévoir aucune disposition législative particulière, ou de prévoir ces dispositions de façon très large, pour l'ensemble des infractions graves.

La première option, celle d'un *statu quo*, n'apparaît pas satisfaisante dès lors que des dispositions législatives encadrant ces échanges ont été introduites en matière de lutte contre le terrorisme. Une telle disposition apparaît donc désormais nécessaire pour permettre à l'autorité judiciaire de communiquer des informations aux services de renseignement dans d'autres domaines.

La seconde option, qui consiste à prévoir des dispositions particulièrement larges pour permettre à l'autorité judiciaire de communiquer des informations issues de procédures judiciaires aux services de renseignement, quelle que soit l'infraction poursuivie, et quel que soit le motif guidant une telle transmission, ne répond pas à l'exigence de proportionnalité de l'atteinte ainsi portée à la vie privée des personnes concernées.

3.2. DISPOSITIF RETENU

Il est proposé d'introduire un nouvel article 706-105-1 au sein du chapitre II du titre XXV du livre IV du code de procédure pénale. Cet article étend les modalités de communication existantes, prévues à l'article 706-25-2 du code de procédure pénale et limitées à la prévention du terrorisme, d'une part, à la cybercriminalité et, d'autre part, à la criminalité organisée.

Au sein des autorités judiciaires, il est prévu que ces échanges soient centralisés par le parquet et le juge d'instruction de Paris, dont les services sont spécialisés dans ces deux matières.

Afin d'assurer la nécessité et la proportionnalité de l'atteinte portée au secret de l'enquête et de l'instruction, le dispositif retenu traite, de manière distincte, le cas de la cybercriminalité et de la criminalité organisée, non seulement en termes de finalités mais également s'agissant de l'étendue des services pouvant être rendus destinataires des données judiciaires concernées.

Concernant la cybercriminalité (I du nouvel article 706-105-1), le procureur de la République de Paris peut, pour les procédures d'enquête ou d'instruction en matière de lutte contre la cybercriminalité, communiquer des données issues de ces procédures à quatre services de l'État exerçant des missions en matière de sécurité et de défense des systèmes d'informations, visés par l'article L. 2321-2 du code de la défense : deux services spécialisés de renseignement (la DGSE et la DGSI), l'ANSSI et le commandant de la cyberdéfense ou comcyber, qui relève du

chef d'état-major des armées. Ne peuvent être transmis, dans ce cadre, que les éléments nécessaires à l'exercice, par ces services, de leur mission en matière de sécurité et de défense des systèmes d'information : il s'agit de leur permettre de capitaliser de la connaissance et de mieux prévenir les cyberattaques, d'en identifier les auteurs ou les modes opératoires et de neutraliser autant que possible leurs effets qui peuvent être systémiques et porter atteinte à l'intégrité de biens civils et militaires essentiels comme à la sécurité des personnes.

Concernant la criminalité organisée (II du nouvel article 706-25-1), le procureur de la République de Paris peut transmettre des éléments issus de procédures d'enquête ou d'instruction en matière de lutte contre la criminalité organisée d'une part, aux services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure, d'autre part, aux services de renseignement mentionnés à l'article L. 811-4 qui exercent des missions en matière de prévention de la criminalité et de la délinquance organisées, dont la liste sera définie par décret en Conseil d'État. De même qu'en matière cyber, ne peuvent être transmis que les éléments nécessaires à l'exercice des missions de ces services au titre de la prévention de la criminalité et de la délinquance organisées : il s'agit de leur permettre de capitaliser de la connaissance sur des réseaux et des modes opératoires particulièrement complexes, aux fins de prévenir les atteintes aux intérêts fondamentaux de la Nation.

Dans les deux cas, si la procédure fait l'objet d'une information, cette communication ne peut intervenir qu'avec l'avis favorable du juge d'instruction. Le juge d'instruction peut également procéder à cette communication, et pour les mêmes finalités que celles précitées, pour les procédures d'information dont il est saisi après avoir recueilli l'avis du procureur de la République de Paris.

Contrairement au dispositif prévu par l'article 706-25-2 du code de procédure pénale concernant les procédures terroristes, les informations brutes communiquées ne peuvent être transmises par les services qui en ont été destinataires à d'autres services. Elles ne peuvent non plus faire l'objet d'un échange avec des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement. Toute personne qui en est destinataire est tenue au secret professionnel (III du nouvel article 706-105-1),

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

La section VIII du chapitre II du titre XXV du livre IV du code de procédure pénale sera complété par un nouvel article 706-105-1.

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES

La mise en œuvre de cette disposition engendrera davantage de transmissions de l'autorité judiciaire vers les services de renseignement, l'ANSSI et le comcyber. Néanmoins, il ne s'agit

aucunement d'une obligation de transmission de la part de l'autorité judiciaire, mais seulement d'une possibilité. La charge pesant ainsi sur elle apparaît mesurée.

4.3. IMPACTS SUR LES PARTICULIERS

Les transmissions d'information par l'autorité judiciaire aux services de renseignement en matière de lutte contre la criminalité organisée et la cybercriminalité et à l'ANSSI et au commandement cyber pour cette dernière finalité, répondront à un cadre strict fixé par le législateur, garantissant une atteinte adaptée et proportionnée au droit au respect de la vie privée.

5. MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée à la Commission nationale informatique et liberté qui a rendu son avis le 15 avril 2021.

5.2. APPLICATION DANS LE TEMPS

Ces dispositions entreront en vigueur le lendemain de la publication de la loi.

5.3. APPLICATION DANS L'ESPACE

Les dispositions s'appliqueront à l'échelle nationale. Une modification de l'article 804 du code de procédure pénale est nécessaire pour étendre l'application de ces dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

CHAPITRE III – DISPOSITIONS RELATIVES A LA LUTTE CONTRE LES AERONEFS CIRCULANT SANS PERSONNE A BORD PRESENTANT UNE MENACE

Article 18 : Lutte contre les aéronefs circulant sans personne à bord présentant une menace

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Les aéronefs circulant sans personne à bord, couramment appelés « drones », sont de plus en plus nombreux (le nombre de drones de plus de 800 grammes, soumis à obligation de déclaration, est de 40 000) à circuler au-dessus du territoire. Ces « drones aériens » constituent des aéronefs dont le télépilote est la personne qui contrôle manuellement les évolutions ou, dans le cas d'un vol automatique, celle qui est en mesure à tout moment d'intervenir sur sa trajectoire ou, dans le cas d'un vol autonome, celle qui détermine directement la trajectoire ou les points de passage de cet aéronef.

Le faible coût des aéronefs circulant sans personne à bord, l'évolution de leurs technologies (autonomie, qualité des vidéos) et l'intérêt qu'ils suscitent dans la population entraînent un accroissement important de leur nombre[39]. Cette augmentation entraîne une utilisation de l'espace aérien susceptible de présenter des risques pour la sécurité des personnes, des biens ou de certains sites alors que cette utilisation est soumise au respect de certaines règles. Ainsi, le nombre des survols illicites constatés de zones interdites (dont des centrales nucléaires) est élevé et constant sur les 3 dernières années selon les données du ministère de l'intérieur (2017 : 384 ; 2018 : 370, 2019 : 335). Les données du ministère de la justice font également apparaître le phénomène des survols de prisons par drone (2018 : 48 ; 2019 : 54, 2020 : 53).

En outre, il s'agit de prendre en compte la menace terroriste. En effet, bien qu'à ce jour, l'usage de drones à des fins terroristes n'ait pas été identifié sur le territoire national, les utilisations des drones par Daesh ont démontré l'étendue des menaces qui peuvent un jour se déporter sur le territoire national. Conformément aux dispositions de l'article L. 6211-1 du code des transports, « *Tout aéronef peut circuler librement au-dessus du territoire français* (…). » Cette disposition est complétée par l'article L. 6211-4 du même code qui prévoit que *« Le survol de certaines zones du territoire français peut être interdit pour des raisons d'ordre militaire ou de sécurité publique dans des conditions fixées par décret en Conseil d'Etat. L'emplacement et l'étendue*

[39] Sur le territoire national, le marché du drone (loisir et pro) était de 200 millions d'euros en 2017, estimé à 304 millions d'euros en 2020 et la projection pour 2025 est de 652 millions d'euros.

des zones interdites sont définis par l'autorité administrative. »[40] Enfin, l'article L. 6211-5 précise que « *L'aéronef qui s'engage au-dessus d'une zone interdite est tenu, dès qu'il s'en aperçoit, d'atterrir sur l'aérodrome le plus rapproché en dehors de la zone interdite*. »

Lorsqu'un aéronef circulant sans personne à bord s'engage dans une zone interdite de survol, de manière temporaire ou permanente, pour des raisons d'ordre militaire ou de sécurité publique, il appartient à l'Etat de mettre en œuvre les moyens nécessaires pour faire cesser cette situation. A cette fin, les capacités techniques disponibles peuvent lui permettre de recourir à un dispositif de brouillage des ondes émises et reçues par l'aéronef, lequel intègre des équipements radioélectriques.

Le recours à de tels dispositifs par l'autorité administrative apparait également nécessaire aux fins de prévenir les menaces susceptibles d'affecter la sécurité de grands événements (sommets internationaux, manifestations sportives, cérémonies nationales), de certains convois (convois officiels, convois de matières dangereuses…) ou de certaines installations sensibles (centrales nucléaires, centres pénitentiaires, emprises militaires). En effet, la menace constituée par les drones « malveillants » se caractérise par sa mobilité, sa célérité et la difficulté de repérage visuel en phase d'approche vers des lieux, zones, personnes ou véhicules à protéger. En outre, les drones ont une grande capacité de repérage et de prise de vidéos. Enfin, ils sont susceptibles d'entraîner des risques de collision et potentiellement, grâce à leur capacité d'emport de charge (explosifs, stupéfiants), des menaces terroristes et de trafics au profit de réseaux de criminalité organisée.

1.2. CADRE CONVENTIONNEL

La Convention relative à l'aviation civile internationale, conclue à Chicago le 7 décembre 1944, précise, en son article 1er, que « *chaque Etat a la souveraineté complète et exclusive sur l'espace aérien au-dessus de son territoire* ».

Cette disposition est complétée par le b) de l'article 9 prévoyant que « *Chaque Etat contractant se réserve également le droit, dans des circonstances exceptionnelles, en période de crise ou dans l'intérêt de la sécurité publique, de restreindre ou d'interdire temporairement et avec effet immédiat les vols au-dessus de tout ou partie de son territoire, à condition que cette restriction ou interdiction s'applique, sans distinction de nationalité, aux aéronefs de tous les autres Etats*. »

[40] Par ailleurs et pour une autre finalité, les dispositions du code des transports qui confient au ministre des Transports la faculté d'interdire le survol de certaines zones pour des raisons de sécurité n'ont pas pour objet et ne sauraient avoir pour effet de priver le maire de la possibilité d'utiliser ses pouvoirs de police pour réglementer, en vue d'assurer la tranquillité et la sécurité des habitants de sa commune, l'utilisation des appareils d'aéromodélisme sur le territoire de sa commune (CE, 8 mars 1993, Commune des Molières, n° 102027).

Enfin, l'article 36 de la Convention relative à l'aviation civile internationale prévoit que « *Tout Etat contractant peut interdire ou réglementer l'usage d'appareils photographiques à bord des aéronefs survolant son territoire*. »

Ces dispositions ont été déclinées en droit interne par les articles L. 6211-1 et suivants du code des transports.

1.3. CADRE CONSTITUTIONNEL

Le législateur doit assurer la conciliation entre le respect des droits et libertés de chacun et la protection de l'ordre public ainsi que des exigences inhérentes à la sauvegarde des intérêts fondamentaux de la Nation. Dans un objectif de protection de la sécurité intérieure, de la défense nationale et du service public de la justice, la neutralisation de l'équipement radioélectrique d'un aéronef circulant sans personne à bord malveillant est susceptible d'impacter plusieurs libertés.

- *La liberté de communication*

L'usage de brouilleurs est susceptible d'altérer la liberté de communication (découlant de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789) d'un tiers dont la fréquence du moyen de communication, tel un téléphone portable ou une radio, serait temporairement affectée.

Dans sa récente décision n° 2020-801 DC du 18 juin 2020, le Conseil constitutionnel a rappelé : « *Aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi ». […] L'article 34 de la Constitution dispose : « La loi fixe les règles concernant ... les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ». Sur ce fondement, il est loisible au législateur d'édicter des règles concernant l'exercice du droit de libre communication et de la liberté de parler, d'écrire et d'imprimer. Il lui est aussi loisible, à ce titre, d'instituer des dispositions destinées à faire cesser des abus de l'exercice de la liberté d'expression et de communication qui portent atteinte à l'ordre public et aux droits des tiers. […]. Il s'ensuit que les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi*. »

En l'absence d'autres moyens permettant de lutter contre un aéronef circulant sans personne à bord et présentant une menace pour la sécurité des personnes, des biens ou des sites sensibles, la neutralisation de l'équipement radioélectrique de cet aéronef, par l'autorité administrative dans des circonstances précises pendant une période adaptée au temps de la menace, répond aux critères de nécessité, d'adaptation et de proportionnalité, tels qu'exigés par le Conseil constitutionnel.

➢ *Le droit de propriété*

Ce droit, garanti par les articles 2 et 17 de la Déclaration des droits de l'Homme et du Citoyen, est susceptible de faire l'objet d'une atteinte si l'utilisation de brouilleurs a pour conséquence de faire chuter le drone et d'entrainer sa détérioration ou sa destruction.

Néanmoins selon le type d'aéronef en cause et sa programmation et selon l'usage qui est fait du brouilleur, l'aéronef est également susceptible de dévier de sa trajectoire, de retourner à son point de départ ou d'atterrir. L'atteinte au droit de propriété n'est alors que potentielle.

En tout état de cause, le droit de propriété doit être concilié avec les autres exigences constitutionnelles, en particulier la sauvegarde de l'ordre public ainsi que les exigences inhérentes à la sauvegarde des intérêts fondamentaux de la Nation.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Les droits et libertés susceptibles d'être affectés par l'usage des brouilleurs contre les drones malveillants étant constitutionnellement garantis, le recours à la loi est nécessaire.

De fait, à ce jour, le livre II relatif aux communications électroniques du code des postes et des communications électroniques ne comporte pas de disposition particulière permettant de lutter spécifiquement contre les drones aériens malveillants. Les dispositions du code des postes et des communications électroniques méritent ainsi d'être précisées pour fonder et permettre explicitement la mise en œuvre d'un dispositif de neutralisation des ondes émises ou reçues par un aéronef circulant sans personne à bord dont la trajectoire ou le positionnement sont de nature à créer une menace pour l'ordre public.

2.2. OBJECTIFS POURSUIVIS

Il apparait utile de prévoir un nouveau dispositif permettant d'étayer l'action des services de l'Etat pour lutter contre les aéronefs circulant sans personne à bord susceptibles de présenter des risques pour les personnes, les biens ou à l'encontre de certains sites.

L'objectif est de prévenir les menaces susceptibles d'affecter la sécurité de grands événements (sommets internationaux, manifestations sportives, cérémonies nationales), de certains convois (convois officiels, convois de matières dangereuses…) ou de certains sites sensibles (centrales nucléaires, centres pénitentiaires, emprises militaires).

Par ailleurs, un autre des objectifs est d'empêcher que l'aéronef transmette pendant son vol des données sensibles ou protégées, telles que des vidéos prises à l'intérieure de sites sensibles.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

Les dispositions pouvaient être introduites dans le code des transports ou dans le code des postes et des communications électroniques, néanmoins, il a paru plus cohérent d'insérer ces nouvelles dispositions législatives dans le code des postes et des communications électroniques pour compléter et expliciter le régime de brouillage des appareils de communication électronique existant.

La mesure envisagée prévoit de rendre inopérant l'équipement radioélectrique d'un aéronef circulant sans personne à bord considéré comme malveillant par les services de l'Etat concourant à la sécurité intérieure, à la défense nationale et au service public de la justice. La neutralisation est autorisée aux seules fins de prévenir les menaces pour la sécurité des personnes et des biens ou le survol d'une zone en violation d'une interdiction.

La neutralisation de l'équipement radioélectrique de ce type d'aéronef a pour effet de l'empêcher de recevoir et d'émettre des ondes lui permettant de se localiser dans l'espace et de perturber ainsi son itinéraire et, le cas échéant, la transmission immédiate de données captées pendant le vol au télépilote ou à un tiers. Cette neutralisation de l'équipement radioélectrique, par brouillage ne permet pas à l'aéronef de continuer son vol tel que programmé initialement ou tel que prévu par le télépilote.

Un décret en Conseil d'État détermine les modalités de mise en œuvre de ces dispositifs. Ce décret aura vocation à préciser les modalités procédurales du brouillage (les autorités compétentes, les procédures de validation technique des brouilleurs…).

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

La mesure envisagée prévoit la création de nouvelles dispositions qui seront codifiées dans le livre II « les communications électroniques » de la partie législative du code des postes et des communications électroniques à l'article L. 33-3-1.

La modification de l'article L. 33-3-2 du code des postes et des communications électroniques permet de rendre applicable la modification effectuée à l'article L. 33-3-1 en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises et en Nouvelle-Calédonie.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services de l'Etat concernés sont ceux chargés de la sécurité intérieure, de la défense nationale et du service public de la justice.

Les services de L'Etat relevant des autorités compétentes chargées de la prévention des menaces pour la sécurité des personnes et des biens et du respect de l'interdiction de survol d'une zone du territoire qui seront mentionnées dans le décret en Conseil d'Etat mettront en œuvre les dispositifs permettant de rendre inopérants l'équipement électrique des aéronefs circulant sans personne à bord malveillants.

Les services de police sont déjà équipés de matériels de détection et de neutralisation. Concernant la préfecture de police et le RAID, un déploiement au profit d'autres directions de police est envisagé pour couvrir une gamme plus de large de missions et d'évènements (environ 60 000 euros, très variable). Pour la police nationale, les opérations de neutralisation sont encadrées par une doctrine d'emploi des moyens de lutte anti drone, des consignes particulières opérationnelles qui prévoient ainsi les finalités, le matériel utilisé, les ressources humaines affectées pour les opérations (2/3 personnels pour constitution d'une équipe : superviseur/chef de mission, détecteur/guetteur, opérateur brouilleur), les mesures de sécurisations de sites, les coordination 3D et les autorisations administratives à recevoir, les procédures d'autorisation à respecter (un compte rendu écrit doit être réalisé après chaque opération de brouillage auprès de l'agence nationale des fréquence (ANFR)), les moyens de compte rendu et de traçabilité des opérations (une application de reporting et de planification des missions Drones pourra utilement être utilisée à cette fin), les consignes de reconnaissances de sites et d'études d'impact, le protocole d'intervention avec la définition de l'autorité d'emploi (chef de service), et le processus décisionnel prévu pour l'autorisation du bouillage (autorisation hiérarchique impérative) (les instructions d'engagement peuvent être, sur instruction de l'autorité d'emploi, en cas de légitime défense ou d'initiative).

4.3. IMPACTS SUR LES PARTICULIERS

La mise en œuvre de dispositifs rendant inopérant l'équipement radioélectrique d'un aéronef circulant sans personne à bord est susceptible de restreindre la liberté du télépilote de faire circuler son aéronef, de porter atteinte à la liberté de communication des tiers, et de porter atteinte au droit de propriété du propriétaire de l'aéronef circulant sans personne à bord.

La mise en œuvre de ces dispositifs répondra au cadre fixé par la loi et devra être nécessaire et proportionnée aux finalités poursuivies.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Cette disposition a été présentée, conformément à L. 36-5 du code des postes et communications électroniques, à l'autorité de régulation des communications électroniques, des postes et de la distribution de la pressequi a rendu son avis le 16 avril 2021.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les dispositions de la loi entrent en vigueur au lendemain de la publication de la loi au Journal officiel de la République française.

5.2.2. Applications dans l'espace

La mesure envisagée s'appliquera sur l'ensemble du territoire.

5.2.3. Textes d'application

Un décret en Conseil d'Etat fixera les modalités de mise en œuvre des dispositifs de lutte contre les aéronefs circulant sans personne à bord présentant une menace, ainsi que les autorités compétentes pour procéder à cette mise en œuvre.

CHAPITRE IV – DISPOSITIONS RELATIVES AUX ARCHIVES INTERESSANT LA DEFENSE NATIONALE

Article 19 : Accès aux archives publiques

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Le champ des archives intéressant la défense nationale présente un intérêt croissant, pour la recherche, qu'elles concernent les forces armées, les services de renseignement ou les différentes administrations qui y concourent. Simultanément, certaines de ces archives peuvent susciter l'intérêt de services de renseignement étrangers ou d'organisations non-étatiques hostiles.

Le secret de la défense nationale, qui contribue à l'exigence constitutionnelle de protection des intérêts fondamentaux de la Nation, doit donc, dans le cas des archives, être concilié avec l'impératif constitutionnel de droit d'accès aux archives publiques.

L'article L. 213-1 du code du patrimoine, dans sa rédaction issue de l'article 17 de la loi n° 2008-696 du 15 juillet 2008 relative aux archives, pose ainsi le principe de la communicabilité de plein droit des archives publiques sous réserve des délais prévus à l'article L. 213-2. Ce dernier article prévoit notamment que les archives dont la communication porte atteinte au secret de la défense nationale ne deviennent communicables qu'à l'expiration d'un délai de cinquante ans. Ce délai est porté à cent ans pour celles, classifiées ou non, dont la communication est de nature à porter atteinte à la sécurité de personnes nommément désignées ou facilement identifiables.

Par ailleurs, le II de l'article L. 213-2 du code du patrimoine définit, par dérogation au principe de communicabilité de plein droit des archives publiques, une catégorie de documents perpétuellement incommunicables, à savoir ceux dont la communication est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de destruction d'un niveau analogue.

S'agissant des archives dont la communication porte atteinte au secret de la défense nationale (c'est-à-dire les archives ayant fait l'objet d'une mesure de classification mentionnée à l'article 413-9 du code pénal), les dispositions de l'article L. 213-2 du code du patrimoine sont à lire de manière combinée avec celles des articles 413-9 et suivants du code pénal. Ce code réprime, en effet, l'accès ou le fait de donner accès à des informations ou supports présentant le caractère de secret de la défense nationale à toute personne non qualifiée, délits usuellement qualifiés de

« compromission ». Aux termes de l'article 413-9, « *présentent un caractère de secret de la défense nationale* (…) *les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès* ».

Prenant acte de l'impossibilité de définir de manière stable et homogène le contenu du secret de la défense nationale, respectueuse du principe constitutionnel de séparation des pouvoirs et conforme à l'office particulier du juge pénal en cette matière, la définition du secret de la défense nationale introduite par le code pénal entré en vigueur en 1994 est ainsi purement formelle.

Les différents niveaux de classification, de même que les conditions à remplir pour qu'une personne puisse être regardée comme qualifiée pour accéder à des informations et supports classifiés, sont, pour leur part, définis aux articles R. 2311-1 et suivants du code de la défense. Les critères et modalités de la classification sont, enfin, précisés par l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

Cette instruction, approuvée par arrêté du Premier ministre du 23 juillet 2010, et des deux instructions qui l'ont suivie (arrêtés des 30 novembre 2011 et 13 novembre 2020), organisent l'articulation entre les dispositions du code du patrimoine et celles du code pénal. A ce titre, elle rappelle qu'avant toute communication d'un document classifié, y compris d'un document classifié devenu communicable de plein droit au titre du code du patrimoine, ce document doit faire l'objet, pour que sa divulgation et sa consultation ne soient pas constitutives d'une infraction pénale, d'une décision formelle de déclassification, matérialisée sur le document par l'apposition d'un timbre de déclassification.

Dans les faits, cette obligation, qui résulte de la nécessaire conciliation du code du patrimoine et du code pénal – conciliation qui découle, elle-même, de la nécessaire combinaison d'impératifs constitutionnels (cf. *infra*) – se traduit par un allongement significatif des délais de consultation. La décision des services détenteurs d'archives reste, en effet, suspendue à celle de l'autorité émettrice quant à la déclassification des documents concernés.

1.2. CADRE CONSTITUTIONNEL

Par une décision n° 2017-655 QPC du 15 septembre 2017, le Conseil constitutionnel a jugé que les dispositions de l'article 15 de la Déclaration des droits de l'homme et du citoyen de 1789, aux termes desquelles « *la société a le droit de demander compte à tout agent public de son administration* », garantissent le droit d'accès aux documents d'archives publiques.

Il a cependant, par la même occasion, précisé qu'il est loisible au législateur d'apporter à ce droit des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi.

Le Conseil constitutionnel, par une décision n° 2011-192 QPC du 10 novembre 2011, a également jugé que le secret de la défense nationale participe au respect des exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation.

L'accès aux documents d'archives classifiés doit ainsi permettre la conciliation de ces deux impératifs constitutionnels.

1.3. ÉLEMENTS DE DROIT COMPARE

À la différence de la France, où la loi fixe les délais de communicabilité applicables aux archives publiques, le cadre juridique des États-Unis d'Amérique confie au service producteur le soin de fixer librement les délais qu'il estime souhaitables pour la mise à disposition des documents au public ; sous la limite, cependant, de trente ans. Au-delà, tous les documents deviennent en principe communicables. Toutefois, pour des raisons touchant principalement à la protection des intérêts supérieurs du pays (sûreté de l'État, défense nationale), le délai de restriction peut être prolongé. Il appartient alors aux instances gouvernementales de désigner les documents concernés. Cette procédure a pour nom la « classification ». Elle n'est limitée par aucun plafond : seule l'autorité qui a procédé à la classification peut en lever l'effet lorsque la durée écoulée lui semble suffisante (« déclassification »). C'est aussi cette même autorité qui peut accorder une autorisation de consultation anticipée aux documents, après instruction du dossier par le service d'archives concerné.

Le principe est assez similaire en Israël, où les archives qui portent atteinte à la sûreté de l'État sont communicables à l'issue d'un délai de cinquante ans, sauf si elles ont été classifiées comme « secrètes ».

D'autres pays, en revanche, prévoient un système de classification soumis à un ou plusieurs plafonds de durée : au Royaume-Uni, le délai qui protège les archives relatives à la sûreté de l'État est de cinquante, soixante-quinze ou cent ans ; en Tunisie, il est de soixante ou de cent ans.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

L'instruction générale interministérielle 1300, qui a explicité l'articulation entre le code pénal et le code du patrimoine, prévoit qu'un document classifié devenu communicable de plein droit au titre du code du patrimoine ne peut être communiqué à une personne non habilitée et ne disposant pas du besoin d'en connaître qu'après avoir fait l'objet d'une décision formelle de déclassification, matérialisée par l'apposition d'un timbre de déclassification sur le document. Cette diligence est nécessaire pour exonérer tant le service détenteur d'un document classifié que celui qui en demande la consultation du risque pénal associé à la compromission du secret de la défense nationale.

Ces modalités d'articulation sont aujourd'hui contestées par nombre d'historiens et archivistes qui considèrent qu'elles sont source d'un allongement inacceptable des délais de consultation, voire constituent une entrave au travail historique et au devoir de mémoire.

L'allongement des délais de traitement des demandes d'accès aux archives classifiées se révèle particulièrement conséquent lorsque la déclassification préalable exige une intervention de l'autorité émettrice ou de son service héritier. En moyenne, cette phase peut s'étendre sur des durées allant de six mois à plus d'un an. Au ministère des armées, le chantier de déclassification des archives de la seconde guerre mondiale a marqué les chercheurs autant que le service historique de la défense, dont le fonds relatif à cette période comptait 100 000 cartons. Aux archives nationales, la mise en œuvre de la dérogation générale du 24 décembre 2015 sur les archives de la seconde guerre mondiale a mobilisé l'équivalent de 100 mois d'agents équivalents temps plein, essentiellement affectés à des tâches de déclassification.

Les fonds des archives nationales comportant des documents classifiés auxquels l'accès est le plus souvent demandé sont ceux des ministères des armées, de l'intérieur et de la justice ainsi que ceux des cabinets du Président de la République et services du Premier ministre. Ces demandes d'accès sont formulées le plus souvent pour des recherches portant sur les périodes de la seconde guerre mondiale, de la guerre d'Algérie et de la guerre froide, étudiées selon des prismes très variés, allant de l'histoire institutionnelle, politique et diplomatique à l'histoire sociale (prosopographie, microhistoire, *etc*.), voire culturelle (histoire des représentations politiques, histoire des mentalités *etc.*). De manière fréquente, également, des demandes de déclassification sont formulées dans le cadre de recherches personnelles (descendants de personnes assassinées, disparues ou condamnées par exemple durant la guerre d'Algérie).

La demande des historiens, des étudiants et du monde de la recherche retient toute l'attention du Gouvernement et le conduit à proposer une modification de la loi. D'ores et déjà, des aménagements ponctuels ont été mis en œuvre, qu'il s'agisse du recours temporaire à un renfort en personnel ou de la fluidification de l'instruction des demandes de communication en procédant à la déclassification de cartons d'archives entiers et non document par document. La situation actuelle ne peut cependant être résolue de façon pérenne, sur le plan du droit, sans modification législative, dès lors que les normes en tension sont chacune de niveau législatif et viennent, chacune, préciser la mise en œuvre de principes constitutionnels.

2.2. OBJECTIFS POURSUIVIS

Il apparaît nécessaire de modifier le point d'équilibre entre les impératifs constitutionnels susmentionnés, dans le sens d'une large ouverture de l'accès aux archives publiques classifiées. Ainsi, afin de donner sa pleine effectivité au principe de libre communicabilité des archives, il est proposé d'inscrire expressément dans la loi, en créant un nouveau III à l'article L. 213-2 du code du patrimoine modifié, la règle selon laquelle, sauf exception, *« toute mesure de classification mentionnées à l'article 413-9 du code pénal prend automatiquement fin à la date à laquelle le document qui en a fait l'objet devient communicable de plein droit* […] ». Dès lors, à l'échéance des délais applicables au titre de l'article L. 213-2 du code du patrimoine,

tout document classifié pourra être communiqué, sans qu'aucune formalité complémentaire ne soit nécessaire, à l'exception des documents, peu nombreux, classifiés ou non, perpétuellement incommunicables en application du II du même article (*cf*. 1.1)

Parallèlement, la modification de l'article L. 213-2 du code du patrimoine offre l'occasion d'améliorer la protection de certaines catégories de documents d'une sensibilité particulière, qu'ils soient classifiés ou non, dont la communication prématurée serait de nature à nuire aux intérêts fondamentaux de la Nation. Cette mesure concerne notamment les documents relatifs aux caractéristiques techniques d'emprises militaires, de missions diplomatiques et consulaires, de centrales nucléaires, de barrages hydrauliques de grande hauteur, les informations techniques permettant la neutralisation de systèmes d'armes défensifs ou la reproduction de matériel de guerre, ou encore les procédures opérationnelles et les capacités techniques des services de renseignement.

Ce projet permet également d'adapter le champ des armes de destructions massives à la réalité de la menace contemporaine, en y ajoutant la menace radiologique (*cf*. modification du II de l'article L. 213-2 du code du patrimoine).

Il permet, enfin, d'ajuster au plus près des besoins le champ de la protection des documents dont la communication serait de nature à porter atteinte à la sécurité de personnes nommément désignées ou facilement identifiables.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Dans le cadre de ses travaux préparatoires, le Gouvernement s'est interrogé sur la possibilité de moduler la conciliation des deux régimes juridiques par voie réglementaire, à travers une lecture volontariste du code du patrimoine, en reconnaissant, *via* l'instruction générale n° 1300, une pleine effectivité à la notion de communicabilité de plein droit, et en supprimant par conséquent l'obligation d'une déclassification préalable des archives classifiées devenues librement communicables.

Cette option n'est pas apparue satisfaisante car elle reviendrait à ignorer la portée des dispositions du code pénal et ne permettrait pas de clarifier l'existence ou non d'un risque pénal auquel seraient exposés les archivistes donnant accès à des documents non démarqués, de même que les personnes en obtenant la communication. Elle priverait par ailleurs de toute protection certains des documents classifiés de plus de cinquante ans, dont la communication pourrait porter atteinte aux intérêts fondamentaux de la nation et en particulier ceux des services de renseignement.

C'est pourquoi l'option d'une simple modification réglementaire a été écartée.

S'est alors posée la question des modifications législatives à opérer.

Parmi les options envisagées, la possibilité de modifier à la fois le code pénal et le code du patrimoine a été explorée. Elle aurait consisté à limiter la modification du code du patrimoine à l'amélioration de la protection de certaines catégories de documents (*cf.* point 3.2 b) et à « neutraliser », par modification du code pénal, les effets répressifs attachés à la manipulation d'un document classifié dès lors qu'il serait devenu pleinement communicable au sens du code du patrimoine.

Dans un souci de lisibilité pour les services d'archives et leurs usagers, le Gouvernement a préféré insérer l'ensemble des modifications législatives souhaitées à l'article L. 213-2 du code du patrimoine. Il est à noter que cette option est cohérente avec l'économie générale du titre modifié qui, aux articles L. 214-1 et suivants, intègre déjà un ensemble de dispositions pénales.

S'agissant du fond, il aurait pu être envisagé de s'en tenir à une disposition mettant automatiquement fin à toute mesure de classification à l'issue du délai de cinquante ans prévu par le 3° du I. Cette option, cependant, présentait l'inconvénient de priver de la protection pénale relative au secret de la défense nationale tous les documents de plus de cinquante ans, y compris les plus sensibles, par exemple en matière de dissuasion nucléaire ou ceux appartenant à la catégorie définie au II, pour lesquelles l'incommunicabilité est perpétuelle aux fins de prévenir toute prolifération d'armes de destruction massive.

La définition au a), b) et c) du 3° du I de l'article L. 213-2 du code du patrimoine de catégories de documents pouvant donner lieu à une prolongation du délai de communicabilité de 50 ans et les modalités de cette prolongation ont également donné lieu à réflexion.

S'agissant des nouvelles catégories de documents justifiant un délai d'incommunicabilité plus long, le Gouvernement s'est encore une fois placé dans la perspective d'une ouverture maximale des archives publiques. Ainsi, il a volontairement restreint son projet aux seuls documents dont l'exploitation par des acteurs malveillants aurait la portée la plus grave. Ainsi, par exemple, alors qu'il aurait pu, dans une logique de sécurité, choisir d'intégrer dans ces nouvelles catégories l'ensemble des documents relatifs à la conception, à l'élaboration et aux fonctionnements des infrastructures d'importance vitale définies aux articles L. 1332-1 et L. 1332-2 du code de la défense (soit environ 1500 emprises), il s'est limité aux informations les plus névralgiques, en ne prenant en compte que les documents relatifs aux caractéristiques techniques des infrastructures de défense, des centrales nucléaires civiles, des barrages hydrauliques de grande hauteur et des missions diplomatiques et consulaires.

S'agissant des modalités de prolongation, le Gouvernement a considéré qu'un report du point de départ du délai de 50 ans à compter de la fin d'usage des infrastructures et matériels de guerre concernés ou de la fin de valeur opérationnelle des informations techniques relatives à la dissuasion nucléaire, sur le modèle retenu par la loi n° 2018-670 du 30 juillet 2018 pour les prisons[41], aurait été excessif. C'est pourquoi le Gouvernement propose que le délai de 50 ans

[41] L'article L213-2 du code du patrimoine actuellement en vigueur dispose en effet que pour les documents relatifs à la construction, à l'équipement et au fonctionnement des ouvrages, bâtiments ou parties de bâtiment utilisés pour la détention des personnes ou recevant habituellement des personnes, le délai de 50 ans « *est décompté depuis la fin de l'affectation à ces usages des ouvrages, bâtiments ou parties de bâtiment en cause* ».

soit, le cas échéant, prolongé jusqu'à la fin de l'usage ou de la valeur opérationnelle ; lorsque la perte de cette valeur opérationnelle se sera produite avant l'arrivée à échéance du délai de 50 ans, ce qui sera le plus souvent le cas, la prolongation de l'incommunicabilité n'a en effet pas lieu d'être. Pour que cette approche libérale ne préjudicie pas aux impératifs de sécurité, le projet de loi précise toutefois que la fin d'affectation doit être entendue comme la fin d'affectation de l'infrastructure considérée ou des autres infrastructures présentant des caractéristiques similaires. Ainsi, demeurent protégées les constructions toujours en service et bâties sur le même modèle que d'autres infrastructures nouvellement désaffectées (cas par exemple des prisons ou de certaines centrales nucléaires ou des parties de ces bâtiments).

3.2. DISPOSITIF RETENU

➢ *S'agissant de l'articulation des dispositions du code du patrimoine et du code pénal*

Le premier alinéa du 3° de l'article L. 213-2 est modifié afin que la désignation d'un document classifié corresponde à la définition du code pénal.

Par ailleurs, les nouvelles dispositions introduites au III nouveau du même article prévoient expressément que la protection accordée à un document au titre du secret de la défense nationale prend automatiquement fin dès lors que le document qui en fait l'objet est devenu communicable de plein droit. Cette rédaction permet de s'assurer que les documents qui ne sont pas communicables de plein droit peuvent, le cas échéant, bénéficier, y compris au-delà de cinquante ans, de la protection résultant de leur classification. La classification expire ainsi automatiquement, selon les cas, à l'issue d'un délai de cinquante ou cent ans, ou d'un délai de cinquante ans prolongé. Aucune expiration automatique de classification ne peut intervenir s'agissant des documents perpétuellement incommunicables mentionnés au II de l'article L. 213-2 (*cf*. 1.1).

Une exception à cette règle est prévue pour les seuls documents mentionnés au 4° du I de l'article L. 213-2. Ces archives – notamment les documents relatifs aux affaires portées devant les juridictions – font, en effet, l'objet de fréquentes demandes de consultation anticipée sur le fondement du I de l'article L. 213-3. Or il arrive que ces documents soient classifiés et doivent, par suite, être déclassifiés avant toute communication. L'expérience ayant montré que la classification de ces documents devient sans objet avant l'expiration du délai de soixante-quinze ans, le Gouvernement propose, afin de fluidifier l'accès anticipé à ces archives, de distinguer, dans ce cas seulement, la communicabilité de plein droit, dont les conditions demeurent inchangées, de l'expiration automatique des mesures de classification, qui, pour sa part, interviendra à l'issue du délai prévu au 3°, c'est-à-dire 50 ans à compter de la date du document ou du document le plus récent inclus dans le dossier.

➢ *S'agissant de l'amélioration de la protection de certaines catégories de documents*

L'option retenue consiste à identifier, au sein des catégories visées au 3° du I de l'article L. 213-2, des sous-ensembles de documents pour lesquels le délai d'incommunicabilité de 50 ans à compter de la date du document ou du document le plus récent du dossier peut s'avérer insuffisant. Il s'agit des documents relatifs :

- aux caractéristiques techniques des installations militaires, des installations et ouvrages nucléaires civils, des barrages hydrauliques de grande hauteur, des locaux des missions diplomatiques et consulaires françaises et des installations utilisés pour la détention des personnes, à compter de la date, constatée par un acte publié, de fin de l'affectation à ces usages de ces infrastructures ou d'infrastructures présentant des caractéristiques similaires ;

- à la conception technique et aux procédures d'emploi de certains types de matériels de guerre et matériels assimilés mentionnés au second alinéa de l'article L. 2335-2 du code de la défense, identifiés *ex ante* par un arrêté du ministre de la défense, révisé chaque année, comme étant particulièrement sensibles, tant que ceux-ci demeurent utilisés par les forces armées et les formations rattachées mentionnées à l'article L. 3211-1-1 du même code. Il s'agit d'abord de protéger les militaires qui les utilisent et de préserver les avantages opérationnels que ces équipements leur confèrent sur les théâtres d'opérations. Il est en outre indispensable de ne pas divulguer les informations qui permettraient de développer des stratégies ou des techniques de contre-mesures. Ce besoin se conçoit aisément lorsqu'il s'agit par exemple de ne pas révéler d'éventuels points de fragilité du châssis ou de la tourelle d'un véhicule terrestre de combat, ainsi que les capacités techniques des matériels d'imagerie ou de détection. Cette nécessité correspond à un besoin de plus en plus prégnant pour les forces armées au regard de l'allongement de la période de conception de certains de ces matériels, qui diffère par voie de conséquence la date de leur entrée en service opérationnel, justifiant ainsi une protection de la documentation correspondante supérieure au délai de droit commun de cinquante ans. A titre d'illustration, ce phénomène peut être constaté à travers des fleurons du secteur aéronautique militaire, à savoir les aéronefs de combat de type *Rafale* ou de transport de type A400M, dont les travaux de conception ont été engagés dans les années 1980 et dont la date prévisionnelle de retrait de service est postérieure à 2040 ;

- aux capacités techniques et procédures opérationnelles des services de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure ainsi qu'à ceux des services mentionnés à l'article L. 811-4 du même code désignés, au regard de leurs missions, par décret en Conseil d'État, à compter de la perte de leur valeur opérationnelle. Les procédures opérationnelles – notion qui figure à l'article L. 833-9 du code de la sécurité intérieure et les capacités techniques des services de renseignement désignent quant à elles,

  - d'une part, les moyens et accès techniques utilisés par ces services pour recueillir des renseignements et protéger leurs opérations ainsi que leurs personnels
  - et, d'autre part les procédures et méthodes mises en œuvre par leurs agents pour la collecte de renseignement et la mise en œuvre de certaines mesures d'entrave,

ainsi que celles qui permettent la sécurité des opérations et des agents qui les conduisent sur le terrain. Ces procédures, en effet, constituent des savoir-faire caractéristiques, acquis en grande partie depuis la seconde guerre mondiale, capitalisés et améliorés progressivement et sur lesquelles repose encore aujourd'hui la sécurité des agents (contre-filature, systèmes de liaison, techniques de contre-espionnage et de clandestinité). Une protection particulière de ces capacités et de ces procédures se justifie donc par l'incidence de leur diffusion éventuelle sur l'activité actuelle des agents des services de renseignement et leur sécurité, y compris physique, comme sur la capacité de ces services à assumer certaines de leurs missions ;

- à l'organisation, la mise en œuvre et la protection des moyens de la dissuasion nucléaire, à compter de la perte de leur valeur opérationnelle des documents. Le champ couvert correspond au cadre défini aux articles L. 1411-1 et suivants et R*1411-1 à R*1411-18 du code de la défense. Si l'élaboration et la conception de la politique de dissuasion nucléaire doivent être ouvertes aux travaux de recherche, l'organisation détaillée des composantes de la dissuasion comme celle de la chaîne de responsabilité la caractérisant ou les systèmes destinés à garantir l'intégrité de ses moyens doivent être très rigoureusement protégés. La liste des moyens de la dissuasion nucléaire est fixée par un arrêté non publié du Premier ministre. Ils comprennent notamment des matières nucléaires, des installations, ou encore des systèmes d'information, et peuvent dépendre tant du ministère de la défense que du Commissariat à l'énergie atomique et aux énergies alternatives ou d'opérateurs publics ou privés. Dans le cadre du contrôle gouvernemental de la dissuasion nucléaire, ils font l'objet de mesures visant en particulier à les protéger contre la malveillance et les atteintes au secret de la défense nationale : mesures organisationnelles avec mise en place de chaînes de responsabilité indépendantes, protection physique des installations, organisation et surveillance des transports, cybersécurité…

> ➢ *S'agissant de la sécurité des personnes nommément désignées ou facilement identifiables*

L'option retenue consiste :

- d'une part, à élargir la portée de la protection figurant au 5° du I en l'appliquant à l'ensemble des documents d'archives, qu'ils aient fait ou fassent ou non l'objet d'une mesure de classification eu égard aux enjeux de protection de la sécurité de personnes nommément désignées ou facilement identifiables qui justifient cette disposition ;
- d'autre part, à en préciser la portée en indiquant que cette disposition ne vise à protéger que les personnes impliquées dans une activité de renseignement.

> ➢ *Prise en compte des armes radiologiques dans le champ des armes de destruction massive*

Afin de s'adapter à l'évolution de la menace et à la définition aujourd'hui retenue pour les armes de destruction massive, par analogie avec la terminologie retenue à l'article 421-2-6 du code pénal, il est proposé d'introduire au II de l'article L. 213-2 du code du patrimoine, portant sur

les documents perpétuellement incommunicables, les documents dont la communication est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes radiologiques.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La modification de l'article L. 213-2 du code du patrimoine portée par le présent article propose une articulation rénovée des régimes juridiques relatifs à la protection du secret de la défense nationale, d'une part, et à la communicabilité des archives publiques, d'autre part. Dans un esprit d'ouverture massive des archives publiques, la nouvelle conciliation proposée donnera une pleine effectivité au principe de communicabilité de plein droit des archives publiques.

Elle implique également la modification de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale et des instructions ministérielles, ainsi que, le cas échéant, des directives techniques particulières qui en découlent.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Le droit de l'Union européenne ne régit pas le droit d'accès aux archives publiques.

La modification de l'article L. 213-2 du code du patrimoine portée par le présent article est sans incidence sur les engagements conventionnels de la France. En effet, cet article ne saurait s'appliquer aux informations et supports classifiés étrangers reçus par la France et dont la protection pénale, garantie par les articles 414-8 et 414-9 du code pénal, est organisée par des accords intergouvernementaux *ad-hoc* dits « accords de sécurité ».

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

A la différence de la France et en dépit des accords intergouvernementaux en vigueur, certains Etats étrangers ne respectent pas l'obligation d'obtenir l'accord de l'Etat émetteur de documents classifiés avant de les rendre librement communicables. Ainsi, un certain nombre de documents d'archives français classifiés sont librement accessibles dans plusieurs services publics d'archives américains. D'autres, encore, ont pu être publiées dans des ouvrages étrangers.

En mettant fin à ces distorsions et en simplifiant l'accès des chercheurs aux archives classifiées devenues librement communicables, les mesures envisagées auront une incidence positive sur la compétitivité de la recherche française à l'international.

4.2.2. Impacts budgétaires

En supprimant l'obligation de déclassification formelle et physique des documents classifiés devenus communicables de plein droit, les mesures envisagées permettront à court terme au ministère des armées de libérer les ressources actuellement affectées au démarquage préalable des documents.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Aujourd'hui, la majorité des archives classifiées sont conservées par les archives nationales, les archives diplomatiques et le service historique de la défense. Les archives départementales détiennent cependant parfois quelques documents classifiés anciens et ne disposent pas toujours des équipements nécessaires pour les traiter conformément aux exigences de la réglementation relative à la protection du secret.

La modification envisagée prévoyant que toute mesure de classification prend automatiquement fin à la date à laquelle le document qui en a fait l'objet devient communicable de plein droit, les documents détenus par les archives départementales pourront être manipulés sans mesure de protection spécifique, en toute régularité au regard des règles relatives au secret de la défense nationale et donc sans risque de compromission.

Cette modification est ainsi source de sécurisation juridique pour les agents des archives départementales et leurs publics.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

- *Une avancée pour les services d'archives*

En rendant communicable l'écrasante majorité des documents classifiés datant de plus de cinquante ans, la mesure projetée allégera significativement la charge qui pèse actuellement sur les services publics d'archives pour la préparation matérielle des demandes de déclassification, leur suivi et le démarquage des documents concernés. Ces opérations sont aujourd'hui rendues particulièrement chronophages par l'absence d'identification des documents classifiés dans les dossiers versés, parfois de très longue date, dans les services publics d'archives. La mesure projetée permettra de recentrer leurs missions de service public sur la collecte, la conservation, la description, la communication, la mise en valeur et la diffusion des archives (art. R. 212-4-1 du code du patrimoine), et de relancer ainsi les chantiers dont le lancement a pu être différé par la charge de travail que faisait peser sur eux l'obligation de déclassification formelle préalable de documents d'archives classifiés qu'ils conservent.

La modification envisagée est également un gage de sérénité pour les agents des services publics d'archives et leurs publics, le risque pénal associé à la communication de documents portant un timbre de classification devenus librement communicables étant désormais écarté.

➢ *Une meilleure protection pour les membres des services de renseignement*

La mesure envisagée permettra également, au travers du nouveau point c) du 3° de l'article L. 213-2 du code du patrimoine modifié, de renforcer la protection des documents relatifs aux capacités opérationnelles des services de renseignement et contribuera ainsi à sécuriser leur action.

4.5. IMPACTS SUR LES PARTICULIERS

La mesure aura à la fois un impact significatif sur l'accès de toute personne aux archives publiques et permettra, dans le même temps, de renforcer la sécurité des citoyens contre des actes malveillants.

➢ *Un accès aux archives publiques significativement renforcé*

La mesure envisagée permettra l'ouverture de plusieurs millions de documents classifiés, dont la communication n'était aujourd'hui possible qu'après déclassification formelle et démarquage préalable. Ainsi, notamment, au seul service historique de la défense, cette mesure permettra d'ouvrir l'accès de plus de 650 000 dossiers d'archives représentant jusqu'à 20 km linéaires. Aux Archives nationales, la mesure permettra l'accès à près de 600 000 documents.

En rendant ainsi désormais immédiatement accessibles des documents dont la déclassification préalable supposait jusqu'à présent des délais de traitement de plusieurs mois, cette mesure aura pour conséquence directe une fluidification du traitement des demandes d'accès aux archives publiques, que la loi impose de satisfaire à l'issue d'un délai d'un mois (deux mois lorsqu'elles ne sont pas librement communicables), et une très nette amélioration des conditions de travail des chercheurs, notamment pour l'accès aux sources de l'histoire contemporaine. Elle permettra ainsi de mettre fin aux retards affectant actuellement les travaux de nombre d'entre eux. Cette mesure permettra également d'éliminer le risque pénal qui, sous l'empire de la législation actuelle, pèse sur les personnes ayant accédé à un document qui, bien que communicable de plein droit en application du code du patrimoine, serait toujours porteur d'une marque de classification.

➢ *Une meilleure protection du citoyen*

La mesure portant création de nouvelles catégories de document soumis au délai de cinquante ans (nouveau a), b) et c) de l'article L. 213-2 du code du patrimoine modifié) permettra, par ailleurs, de renforcer la sécurité des citoyens, en améliorant la protection offerte par le code du patrimoine aux documents, classifiés ou non, dont l'exploitation malveillante pourraient avoir de lourdes conséquences : plans de centrales nucléaires, de barrages hydrauliques, d'infrastructures militaires ; système de contrôle gouvernemental de la dissuasion nucléaire, etc.

Il convient de noter que cette extension à de nouvelles catégories est articulée de façon proportionnée avec l'objectif de renforcement de l'accès aux archives publiques. En effet, l'accès aux documents ainsi visés, tout comme l'accès à l'ensemble des documents dont il est question au I. de l'article L. 213-2 du code du patrimoine, demeurera possible dans le cadre de demandes de consultation anticipée (*cf.* point I de l'article L. 213-3 du code du patrimoine), tel qu'encadré par la jurisprudence du Conseil d'Etat (décision n° 422327 du 16 juin 2020) voire dans le cadre d'arrêtés d'ouverture anticipée (*cf.* point II du même article).

5. MODALITES D'APPLICATION

5.1. APPLICATION DANS L'ESPACE

Les modifications de l'article L. 213-2 du code du patrimoine portées par le présent article s'appliqueront de plein droit aux collectivités régies par le principe d'identité législative, et sont applicables au territoire des Terres australes et antarctiques françaises sous la seule réserve, s'agissant de Wallis et Futuna, des dispositions de l'article L. 760-2 du code du patrimoine. Elles n'ont pas vocation à être étendues en Nouvelle-Calédonie et en Polynésie française.

5.2. TEXTES D'APPLICATION

L'instruction générale n° 1300 sur la protection du secret de la défense nationale, ainsi que les instructions ministérielles et, le cas échéant, les directives techniques particulières qui en découlent, devront être adaptées pour être mise en cohérence avec les nouvelles dispositions de l'article L. 213-2 du code du patrimoine.

Un décret en Conseil d'Etat sera pris pour désigner ceux des services de renseignement mentionnés à l'article L. 811-4 du code de la sécurité intérieure (dits « du second cercle ») auxquelles pourra s'appliquer la disposition de prolongation de l'incommunicabilité des documents relatifs à leurs procédures opérationnelles et à leurs capacités techniques au-delà du délai de cinquante ans et jusqu'à la perte de leur valeur opérationnelle.

5.3. APPLICATION DANS LE TEMPS

Les dispositions résultant de la modification proposée sont d'application immédiate.

Toutefois, les documents non classifiés de plus de cinquante ans qui étaient devenus communicables par application de la législation antérieure ne sont pas soumis aux règles de communicabilité plus strictes prévues par le présent article. Ainsi, l'adaptation de certains délais pour mieux prendre en compte les enjeux actuels de certaines catégories de documents désormais expressément visées à l'article L. 213-2 du code du patrimoine ne rendra pas de nouveau incommunicables des documents qui peuvent déjà être communiqués sous l'empire de la législation actuelle.

S’agissant des documents classifiés de plus de cinquante ans, leur communicabilité étant jusqu’à présent subordonnée à leur déclassification préalable, ils ne sont pas communicables, en l’état de la législation actuelle. Ils le deviennent, par l’effet de l’entrée en vigueur de la loi nouvelle, à moins de relever de l’un des cas spécifiques définis par la loi dans lesquels le délai de communicabilité est plus tardif et n’est pas encore atteint.