CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

PJL RELATIF À LA PRÉVENTION D'ACTES DE TERRORISME ET AU RENSEIGNEMENT

Assemblée nationale

> Lien vers le texte adopté

L'Assemblée nationale a adopté en nouvelle lecture, le 13 juillet 2021, le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement. Il sera examiné en nouvelle lecture au Sénat le 22 juillet.

CONTENU DU PROJET DE LOI

1. PRÉVENTION D'ACTES DE TERRORISME

❖ Pérennisation de la Loi SILT

– **L'article 1er** vise à **pérenniser 4 mesures expérimentées** dans le cadre de la Loi SILT : les périmètres de protection, les fermeture des lieux de culte, les mesures individuelles de contrôle et de surveillance et visites domiciliaires. Initialement, le Parlement avait autorisé leur mise en œuvre jusqu'au 31 décembre 2020, délai qui a ensuite été prorogé jusqu'au 31 juillet 2021.

- **L'article 1er *bis*** consacre au niveau législatif **l'effectivité continue du contrôle exercé par les OPJ sur les agents de sécurité privée et limite le caractère renouvelable des périmètres de protection institués par la « Loi SILT »** à une seule fois pour une durée ne pouvant excéder un mois.

❖ Fermeture des locaux dépendant de lieux de culte

– **L'article 2** vise à **élargir le champ d'application de la mesure de fermeture des lieux de culte** afin qu'elle puisse également s'appliquer aux **locaux qui dépendent du lieu de culte**, dès lors :

- qu'il existe des raisons sérieuses de penser que ces locaux sont utilisés pour diffuser des propos, des idées ou des théories ou que les activités qui s'y déroulent provoquent à la violence, à la haine, à la discrimination, à la commission d'actes de terrorisme ou font l'apologie de tels actes.
- que ces locaux sont utilisés pour faire échec à l'exécution de la mesure de fermeture du lieu de culte.

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

La **violation de la mesure de fermeture d'un lieu dépendant du lieu de culte** est punie des mêmes peines que celle de la violation de la fermeture du lieu de culte, à savoir d'une **peine de 6 mois d'emprisonnement** et de **7500 € d'amende**.

- **L'article 3** vise à **adapter le régime des MICAS** en renforçant les pouvoirs du ministère de l'intérieur en la matière, qui pourra éventuellement prononcer les obligations suivantes à l'égard de la personne faisant l'objet de telles mesures :
    - **Obliger la personne** à déclarer non plus seulement son lieu d'habitation mais également de **fournir un justificatif d'habitation ou de domicile**, ainsi que tout changement de lieu d'habitation ou de domicile
    - **Assortir** à l'obligation de ne pas se déplacer à l'extérieur d'un périmètre déterminé **une interdiction de paraître** dans un ou plusieurs lieux déterminés se trouvant au sein de ce périmètre déterminé et dans lesquels se tient un événement exposé, par son ampleur ou ses circonstances particulières, à un risque de menace terroriste.
        - Cette interdiction doit tenir compte de la vie familiale et professionnelle de la personne.
        - Sa durée est strictement limitée à celle de l'événement, dans la limite de 30 jours.
        - Sauf urgence dûment justifiée, elle doit être notifiée à la personne concernée au moins 48h avant son entrée en vigueur.
        - Le périmètre déterminé ne peut être inférieur au territoire de la commune et doit permettre à la personne de poursuivre une vie familiale et professionnelle
    - **Prolonger jusqu'à 24 mois** et non plus jusqu'à 12 mois **les MICAS** lorsque les obligations sont prononcées dans un délai de 6 mois à compter de la libération d'une personne condamnée à une peine d'emprisonnement d'au moins 5 ans pour des faits de terrorisme (à au moins 3 ans dans le cadre d'une récidive légale).
        - Chaque renouvellement de la mesure, d'une durée maximale de trois mois, est subordonné à l'existence d'éléments nouveaux ou complémentaires.
    - **Interdire à la personne 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.
    - **Se présenter périodiquement aux services de police ou aux unités de gendarmerie**, dans la limite d'une fois par jour, en précisant si cette obligation s'applique les dimanches et jours fériés ou chômés.

En cas de saisine d'un tribunal territorialement incompétent pour annuler la décision de renouvellement des obligations, le délai de jugement de 72h 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 7 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.

Les obligations prononcées par le ministre de l'intérieur doit tenir compte, dans le respect des principes de nécessité et de proportionnalité, **des obligations déjà prescrites par l'autorité judiciaire**.

❖ Saisie de supports informatiques dans le cadre des visites domiciliaires

- **L'article 4** vise à **permettre la saisie de supports informatiques** (« *système informatique* » et « *équipement terminal* ») **dans le cadre des visites domiciliaires**, y compris lorsque l'occupant des lieux (ou son représentant) fait obstacle à l'accès aux données contenues dans les supports informatiques présent sur les lieux de la visite.
    - Le refus de donner accès aux informations contenues dans les supports informatiques doit être mentionné sur le procès-verbal.
    - La saisie peut être effectuée soit par la copie des données, soit par la saisie du support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la visite.

- **L'article 4 bis** vise à **garantir l'anonymat des témoins** qui ont **assisté à la visite domiciliaire** et signé le procès-verbal correspondant.

❖ Mesure judiciaire de prévention de la récidive terroriste et de réinsertion

- **L'article 5** crée, dans le code de procédure pénale, une **mesure judiciaire de prévention de la récidive terroriste et de réinsertion** (MJPRTR) qui ne peut être prononcée qu'à l'encontre des **personnes condamnées** à une peine d'emprisonnement d'au moins 5 ans (ou 3 ans en récidive légale) **pour des faits de terrorisme** et qui ne font l'objet d'aucune autre mesure de suivi judiciaire. Le dispositif prévu par la présente loi adapte le régime des mesures de sûreté censuré par le Conseil constitutionnel dans sa décision du 7 août 2020.

  Le tribunal de l'application des peines de Paris (ci-après « TJ de Paris ») peut, sur réquisitions du procureur de la République antiterroriste, **ordonner une MJPRTR** à l'encontre de ces personnes aux seules fins de **prévenir leur récidive** et **d'assurer leur réinsertion**. **Deux conditions cumulatives** doivent être établies à l'issue du réexamen :
    - présenter une **particulière dangerosité caractérisée par une probabilité très élevée de récidive**
    - constater **une adhésion persistante à une idéologie ou à des thèses incitant à la commission d'actes de terrorisme**

  La décision prise par **le juge de l'application des peines** (JAP) du TJ de Paris doit **définir** les conditions d'une **prise en charge sanitaire, sociale, éducative, psychologique** ou psychiatrique destinée à permettre la réinsertion et l'acquisition des valeurs de la citoyenneté. Cette prise en charge peut s'effectuer au sein d'un établissement d'accueil adapté.
    - Le **rôle du tribunal et du JAP** :
        - Le JAP, assisté du service pénitentiaire d'insertion et de probation (SPIP) et, le cas échéant, avec le concours des organismes habilités à cet effet, sont chargés de la mise en œuvre des obligations auxquelles la personne est astreinte.
        - Le TJ de Paris ne peut prononcer la MJPRTR **qu'après s'être assuré que la personne condamnée a été mise en mesure de bénéficier**, pendant l'exécution de sa peine, **de mesures favorisant sa réinsertion**.
    - Les **obligations auxquelles l'intéressé peut être soumis** :
        - Exercer une activité professionnelle
        - Suivre un enseignement ou une formation professionnelle

        - Ne pas se livrer à l'activité dans l'exercice à ou l'occasion de laquelle l'infraction a été commise.
        - Astreindre à établir sa résidence en lieu déterminé
    - La décision doit **préciser obligatoirement les condition**s dans lesquelles dans lesquelles il doit :
        - Communiquer au SPIP les renseignements ou documents permettant le contrôle de ses moyens d'existence et de l'exécution de ses obligations
        - Répondre aux convocations du JAP ou du SPIP.
    - La durée maximale de la MJPRTR est **allongée à 24 mois maximum** :
        - Elle peut être ordonnée pour une durée maximale d'1 an
        - A l'issue de cette période, elle peut être renouvelé pour au plus 1 an, périodes de suspension comprises, dans la limite de 5 ans (3 ans pour un mineur), sur réquisitions du procureur de la République antiterroriste, après avis de la commission pluridisciplinaire des mesures de sûreté (CPMR).
        - Chaque renouvellement est subordonné à l'existence de faits nouveaux.

La mesure ne peut être ordonnée que si elle apparaît strictement nécessaire pour prévenir la récidive et assurer la réinsertion.

- Elle n'est pas applicable si la personne a été condamnée ou fait l'objet :
    - d' un suivi socio-judiciaire
    - d'une mesure de surveillance judiciaire
    - d'une mesure de surveillance de sûreté
    - d'une rétention de sûreté.

La situation de la personne doit être **examinée par la CPMR**, sur réquisition du procureur de la République antiterroriste, au moins 3 mois avant la date de libération. L'examen doit permettre d'évaluer sa dangerosité et sa capacité à se réinsérer.

- A cette fin, la CPMR demande le placement de la personne concernée, pour une durée d'au moins 6 semaines, dans un service spécialisé chargé de l'observation des personnes détenues afin de mener une évaluation pluridisciplinaire de dangerosité.
- A l'issue de cette période, la CPMR adresse au TJ de Paris et à la personne concernée un avis motivé sur la pertinence de prononcer la mesure.

La décision doit être prise par un **jugement rendu après un débat contradictoire et public** (si le condamné le demande) au cours **duquel le condamné est assisté par un avocat choisi ou commis d'office** , avant la date de libération. Elle doit être **spécialement motivée** au regard des conclusions de l'évaluation et de l'avis de CPMR.

- Le jugement doit préciser les obligations et leur durée.
- La décision est exécutoire immédiatement à l'issue de la libération.
- Le TJ de Paris peut, sur réquisitions du procureur de la République antiterroriste ou à la demande de la personne concernée (après avis dudit procureur), modifier la mesure ou ordonner sa mainlevée. Cette compétence s'exerce sans préjudice de la possibilité, pour le JAP, d'adapter à tout moment les obligations de la mesure.

Les décisions du TJ de Paris relatifs au MJPRTR sont **susceptibles d'appel** devant la chambre de l'application des peines de la cour d'appel ou devant le président de cette chambre.

Les obligations imposées sont **suspendues par toute détention intervenue au cours de leur exécution**. Si la détention excède une durée de 6 mois, la reprise d'une ou de plusieurs des

obligations doit être confirmée par TJ de Paris au plus tard dans un délai de 3 mois après la cessation de la détention. A défaut, il doit être mis fin d'office à la mesure.

Les manquements aux obligations auxquelles la personne est soumise et astreinte sont punis d'une **peine d'emprisonnement de 3 ans** et de **45 000 € d'amende**.

Un décret en conseil d'Etat précise les modalités et les conditions d'application de la MJPRTR.

❖ **Transmission des données de santé au préfet de département**

– **L'article 6** insère un nouvel article dans le code de santé publique visant à permettre au **préfet de département** (ou préfet de police de Paris), ainsi qu'aux services de renseignement désignés par décret en Conseil d'Etat, de **se voir communiquer,** lorsque la **personne fait l'objet d'une mesure de soins psychiatriques sans consentement** et qu'elle représente une menace grave pour la sécurité et l'ordre publics en raison de sa radicalisation à caractère terroriste, **les données d'identification** de cette personne et les données relatives à sa situation administrative.
  - Ces informations ne peuvent être transmises qu'aux seules fins d'assurer le suivi de cette personne.
  - Ces informations ne peuvent porter, sans le consentement de la personne concernée, sur des faits antérieurs de plus de 3 ans à compter de la date levée de la mesure de soins.

2. Renseignement

❖ **Exploitation et échanges d'information entre services de renseignement**

- **L'article 6 bis** complète le rapport annuel du Gouvernement sur les mesures prises en application de la « Loi SILT » à l'ensemble des mesures administratives prises en matière de lutte contre le terrorisme.

– **L'article 7** vise à **encadrer les conditions dans lesquelles les services de renseignement peuvent exploiter les renseignements qu'ils ont obtenus pour une finalité différente de celle qui en a justifié le recueil** et **transmettre les renseignements qu'ils ont collectés** par la mise en œuvre de **techniques de recueil de renseignement soumises à autorisation**.

Les renseignements collectés **ne peuvent être transmis pour d'autre finalités que les missions des services spécialisés de renseignement**, à savoir la défense et la promotion des intérêts fondamentaux de la Nation. Initialement, cette interdiction ne visait que la collecte, l'extraction et la transcription des données collectées sans traiter du cas de leur transmission.
  - Lorsqu'un service spécialisé de renseignement ou un service désigné par le décret en Conseil d'État obtient des renseignements utiles à la poursuite d'une finalité différente de celle qui a en a justifié le recueil, à la suite de la mise en œuvre d'une technique de recueil de renseignement soumises à autorisation, il peut les transcrire ou les extraire pour le seul exercice de ses missions.
  - Les **techniques de recueil de renseignement soumises à autorisation** sont :

- Les accès administratifs aux données de connexion
- Les interceptions de sécurité
- La sonorisation de certains lieux et véhicules et la captations d'images et de données informatiques
- Les mesures de surveillance des communications électroniques internationales
- Les mesures de surveillance de certaines communications hertziennes

Un service de renseignement peut **transmettre les renseignements collectés, extraits ou transcrits dont il dispose à un autre service de renseignement** uniquement si cette transmission est **strictement nécessaire à l'exercice des missions du service destinataire**.

- Les transmissions sont **subordonnées à une autorisation préalable du Premier ministre**, après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), lorsqu'elles :
  - poursuivent une finalité différente de celle qui en a justifié le recueil
  - 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
- Ces transmissions sont sans effet sur la durée de conservation de chacun des renseignements collectés, qui court à compter de la date de recueil. A l'issue de cette durée, chaque service possédant les renseignements en cause procède à leur destruction. Pour rappel, ils doivent être détruits au bout de :
  - **30 jours** à compter de leur recueil pour les correspondances et les paroles captées
  - **120 jours** à compter de leur recueil pour les renseignements collectés par la mise en œuvre techniques de recueil de renseignement soumises à autorisation
  - **4 ans** à compter de leur recueil pour les informations ou documents collectés à partir de la technique des accès administratifs aux données de connexion.
- Le responsable de chaque service spécialisé de renseignement ou de chaque service désigné par le décret en Conseil d'Etat désigne un agent chargé de veiller, sous son contrôle, au respect de principes posés en matière de collecte et d'extraction des données.
  - L'agent est informé par ses homologues dans les autres services de la destruction des renseignements transmis.
  - Il rend compte, sans délai, au responsable du service auprès duquel il est placé de toute difficulté dans l'application de ces principes.
- Les opérations de collecte, de transmission et d'extraction de renseignements sont soumises au contrôle de la CNCTR .

Les **opérations de destruction** des renseignements collectés, des transcriptions, des extractions et des transmissions doivent être effectuées par des agents individuellement désignés et spécialement habilités. Ces opérations de destruction doivent faire l'objet de relevés tenus à la disposition de la CNCTR qui précisent :

- S'agissant des transcriptions ou des extractions : si elles ont été effectuées pour une finalité différente de celle qui en a justifié le recueil
- S'agissant des transmissions : leur nature, leur date et leur finalité ainsi que le ou les services qui en ont été destinataires

- 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 CNCTR .

Les autorités administratives, c'est-à-dire **l'ensemble des administrations publiques**, peuvent **transmettre aux services spécialisés de renseignement et aux services désignés par décret en Conseil d'État**, 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**.

- Les autorités administratives qui refusent de communiquer certaines informations aux services de renseignement doivent **justifier leur refus.**
- Les informations doivent être détruites dès lors qu'elles ne sont pas ou plus nécessaires à l'accomplissement des missions du service auquel elles ont été transmises.
- Un décret fixe les conditions dans lesquelles la traçabilité des transmissions est mise en œuvre dans les traitements de données à caractère personnel des autorités administratives concernées.
- Toute personne qui en est rendue destinataire est tenue au secret professionnel. En cas de manquement à cette obligation, la personne encourt **des peines d'un an d'emprisonnement** et de **15 000 € d'amende**.
- L'agent habilité à la destruction des renseignements est chargé d'assurer une traçabilité de ces transmissions et de veiller au respect de l'application de ces dispositions.

Les articles L. 135 S du livre des procédures fiscales et 22 de la loi n° 2007 1824 du 25 décembre 2007 de finances rectificative pour 2007 sont **supprimés**. Ils prévoient la **possibilité pour les agents des administrations fiscales de transmettre des informations aux services de renseignement**, **sans que ne puisse leur être opposé le secret professionnel**, aux seules fins de recherche et de prévention des atteintes aux intérêts fondamentaux de la nation en matière de sécurité publique et de sûreté de l'Etat.

Les articles 48 et 49 de la loi n°78-17 du 6 janvier 1978, dite Informatique et Libertés, sont modifiés :

- **Le droit à l'information concernant les données à caractère personnel prévu par le RGPD ne s'applique à l'information transmise par une autorité administrative à un service spécialisé de renseignement** ou à un service désignés par décret en Conseil d'État, dans le but de préserver les intérêts fondamentaux de la Nation.
- **Le droit d'accès de la personne à ses données personnelles, prévu par le RGPD, ne s'applique pas :**
  - 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.
  - À l'information transmise par une autorité administrative à un service de renseignement dans le but de préserver les intérêts fondamentaux de la Nation.

❖ Conservation des renseignements collectés pour la recherche et le développement

- **L'article 8** vise à autoriser les services spécialisés de renseignement à **conserver au-delà des durées légales** les renseignements collectés **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**. 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. De plus, l'article institue **une durée unique de conservation pour les données collectées** par les dispositifs de captation de paroles et d'images (120 jours).
    - Les renseignements collectés sont conservés de façon 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 fassent plus apparaître les motifs et finalités pour lesquels ils ont été collectés e
        - ne permettant pas de rechercher l'identité des personnes concernées.
    - Les paramètres techniques applicables à chaque programme de recherche ainsi que toute évolution substantielle de ces paramètres sont soumis à une autorisation préalable du Premier ministre, délivrée après avis de la CNCTR.
    - Les renseignements collectés **doivent être détruits dès que leur conservation n'est plus indispensable** à la validation de capacités techniques de recueil et d'exploitation et, au plus tard, 5 ans après leur recueil.
    - La CNCTR veille à ce que la mise en œuvre des programmes de recherche respecte les conditions posées par la loi. 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.

  Le service du Premier ministre, chargé de recueillir les informations ou documents auprès des opérateurs et des fournisseurs d'accès à internet, **peut conserver les renseignements collectés avec l'accord du ou des services** pour lesquels ils ont été collectés**.** Il doit en **organiser la centralisation**.

  Le CNCTR dispose d'un accès permanent, complet et direct aux dispositifs de traçabilité des renseignements collectés et aux **locaux où sont centralisés ces renseignements**.

❖ Encadrement des techniques de sonorisation et de captation d'images et de données

- **L'article 9** vise à **autoriser la mise en œuvre des techniques de sonorisation de certains lieux et véhicules et de captation d'images et de données informatiques**. Cette autorisation est délivrée pour **une durée maximale de 2 mois** (initialement fixée à 4 mois). De plus, l'article **facilite le recours aux techniques de captation et de recueil des données informatiques.**

❖ Renforcement des pouvoirs du ministre chargé des communications électroniques

- **L'article 10** vise à **permettre au ministre chargé des communications électroniques** de veiller à ce que l'exploitant public, les autres exploitants de réseaux publics de communications

électroniques et les autres fournisseurs de services de communications électroniques autorisés **prennent les mesures nécessaires pour assurer l'application**, dans le respect du secret de la défense nationale, des dispositions **des sections 5 et 6 du chapitre II du titre XXV du livre IV du code de procédure pénale** relatifs :

- L'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique
- Des autres techniques spéciales d'enquête, qui sont :
  - Le recueil des données techniques de connexion et des interceptions de correspondances émises par la voie des communications électroniques
  - Les sonorisations et des fixations d'images de certains lieux ou véhicules
  - La captation des données informatiques

❖ Expérimentation de l'interception des communications satellitaires

– **L'article 11** vise à **autoriser**, **jusqu'au 31 juillet 2025**, **l'interception des correspondances émises ou reçues par la voie satellitaire** au moyen d'un appareil ou d'un dispositif technique spécifique **lorsque cette interception ne peut être mise en œuvre sur le fondement des interceptions de sécurité**, soit pour des raisons techniques soit pour des motifs de confidentialité faisant obstacle au concours des opérateurs ou des personnes fournissant un accès à internet.

- Elle est permise pour les services spécialisés de renseignement et les services mentionnés à l'article L. 811-4 désignés, au regard de leurs missions, par décret en Conseil d'État après avis de la Commission nationale de contrôle des techniques de renseignement.
- Ces interceptions doivent respecter les conditions posées pour pratiquer des techniques de recueil de renseignement soumises à autorisation.
- Elles ne peuvent être mises en œuvre que pour les finalités suivantes :
  - L'indépendance nationale, l'intégrité du territoire et la défense nationale
  - Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère
  - La prévention du terrorisme
  - La prévention de la criminalité et de la délinquance organisées

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 de :

- **30 jours** à compter de leur recueil pour les correspondances et les paroles captées
- **120 jours** à compter de leur recueil pour les renseignements collectés par la mise en œuvre techniques de recueil de renseignement soumises à autorisation
- **4 ans** à compter de leur recueil pour les informations ou documents collectés à partir de la technique des accès administratifs aux données de connexion.

L'autorisation est délivrée pour une **durée maximale de 30 jours**, renouvelable dans les mêmes conditions de durée. Elle vaut autorisation de recueil des informations ou documents associés à l'exécution de l'interception et à son exploitation.

Un service du Premier ministre organise la centralisation des correspondances interceptées et des informations ou documents recueillis. 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.

- La demande d'autorisation effectuée doit préciser les motifs faisant obstacle à la centralisation immédiate des correspondances interceptées.
- Les opérations de transcription et d'extraction des communications interceptées, auxquelles la CNCTR dispose d'un accès permanent, complet, direct et immédiat, sont effectuées au sein du service du Premier ministre concerné.

Le nombre maximal des autorisations d'interception en vigueur simultanément est arrêté par le Premier ministre, après avis de la CNCTR. La décision fixant ce contingent et sa répartition entre les ministres, ainsi que le nombre d'autorisations d'interception délivrées, sont portés à la connaissance du CNCTR.

Un décret en Conseil d'État, pris après avis de la CNCTR , **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 d'interception des données satellitaires**.

Un rapport d'évaluation de l'application de ce dispositif doit être adressé par le Gouvernement au Parlement au plus tard 6 mois avant l'échéance du 31 juillet 2025.

- **L'article 12 pérennise les dispositions** de l'article L. 851-3 du code de la sécurité intérieure relatives à **l'utilisation des algorithmes** destinés à détecter des connexions susceptibles de révéler une menace terroriste.

- **L'article 13** renforce l'encadrement de la mise en œuvre des algorithmes régie par l'article L. 851-3 et **étend leur champ aux URL.**

- **L'article 14** vise, d'une part, à **intégrer les URL aux données de connexion pouvant être recueillies en temps réel** et d'autre part, à préciser que la durée de conservation des URL s'élève à cent vingt jours.

- **L'article 15 supprime toute possibilité d'effacement différé des données de connexion** par les opérateurs, fournisseurs d'accès à Internet et hébergeurs sauf en cas de menace grave, actuelle ou prévisible sur la sécurité nationale.

  Les données relatives à l'identité civile de l'utilisateur et les autres informations fournies par l'utilisateur lors de la souscription du contrat ([173]) **sont conservées jusqu'à l'expiration d'un délai de cinq ans après la fin du contrat**.

  - Pour les seuls impératifs de **la lutte contre la criminalité grave et à la délinquance grave**, la **prévention des menaces** à la sécurité publique et **la sauvegarde de la sécurité nationale,** les données techniques permettant **d'identifier les sources de la connexion sont conservées pour une durée d'un an** à compter de la connexion ou de l'utilisation des équipements terminaux.

- Pour le seul impératif de **sauvegarde de la sécurité nationale**, uniquement en cas de menace grave, actuelle ou prévisible, la conservation généralisée et indifférenciée de certaines données de trafic et de localisation ([174]) peut être imposée par une injonction du Premier ministre, d'une **durée maximale d'un an renouvelable** à l'issue d'un réexamen de l'état des menaces. Cette injonction pourra faire l'objet d'une contestation devant le Conseil d'État par voie d'action ou d'exception.

  Il prévoit **une mesure de « conservation rapide »** qui peut être imposée par injonction des autorités judiciaires et administratives aux opérateurs, fournisseurs d'accès et hébergeurs à des fins de prévention et de répression de la criminalité grave.

- **L'article 16** renforce le contrôle préalable de la CNCTR pour l'ensemble des techniques de renseignement sur le territoire national en conférant un effet contraignant à ses avis, tout en ménageant une exception en cas d'urgence.

- **L'article 16 bis** modifie l'article L. 853-3 du code de la sécurité intérieure afin de simplifier la procédure de maintenance et de retrait des dispositifs installés dans des lieux d'habitation ou lorsqu'ils concernent une technique de recueil de données informatiques.

- **L'article 17** permet la communication, par le procureur de la République de Paris ou par le juge d'instruction, d'informations issues de procédures judiciaires en matière de lutte contre la cybercriminalité et la criminalité organisée d'une très grande complexité.

- **Les articles 17 bis et ter** renforcent et précisent les prérogatives de la délégation parlementaire au renseignement.

- **L'article 17 ter A** modifie l'article 154 de la loi n° 2001-1275 du 28 décembre 2001 de finances pour 2002 afin d'y inscrire que le rapport de la commission de vérification des fonds spéciaux n'est plus remis, mais est présenté aux présidents et rapporteurs généraux des commissions de l'Assemblée nationale et du Sénat chargées des finances, au président de l'Assemblée nationale et au président du Sénat. Les exemplaires de ce rapport demeureront cependant à la disposition de ces autorités si elles en font la demande.

- **L'article 18** modifie le code des postes et des communications électroniques afin d'autoriser le recours, par les services de l'État, à des dispositifs de brouillage destinés à rendre inopérant l'équipement radioélectrique intégré dans des « drones » 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 au-dessus de laquelle ces équipements ne sont pas autorisés.

- **L'article 19** modifie l'article L. 213-2 du code du patrimoine afin d'y inscrire un principe de déclassification automatique des documents intéressant la défense nationale à l'échéance du délai de cinquante ans prévus au même article, tout en autorisant le prolongement de ce délai pour certains de ces documents dont il dresse une liste exhaustive.

3. Lutte contre les drones présentant une menace pour la sécurité nationale

- **L'article 18** vise à **encadrer les conditions dans lesquelles l'autorité administrative peut recourir**, sur le territoire national, **à des opérations de brouillage des drones** (« aéronefs sans personne à bord ») afin de **prévenir les menaces susceptibles d'affecter la sécurité nationale**.
    - Il élargit la prohibition de détention d'utilisation de tout dispositif destiné à rendre inopérants des équipements radioélectriques ou des appareils intégrant des équipements radioélectriques, et non plus seulement des appareils de communications électroniques.
    - L'Etat est autorisé à utiliser des dispositifs destinés à rendre inopérant l'équipement radioélectrique d'un drone en cas de menace imminente, uniquement pour les besoins suivants :
        - L'ordre public
        - La défense et la sécurité nationale
        - Le service public de la justice
        - Afin de prévenir le survol d'une zone en violation d'une interdiction pour des raisons d'ordre militaire ou de sécurité publique

  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.

4. Outre-mer

- **Les article 20 à 29** sont des articles rédactionnels permettant l'application des dispositions de la présente loi dans les territoires d'outre-mer.