PROJET DE LOI RENFORÇANT LA SÉCURITÉ INTÉRIEURE ET LA LUTTE CONTRE LE TERRORISME

———

Présentation générale

———

I - DISPOSITIONS RENFORÇANT LA PRÉVENTION D'ACTES DE TERRORISME

Le chapitre Ier regroupe un ensemble de dispositions renforçant la prévention d'actes de terrorisme en créant dans le droit commun des outils adaptés à la lutte anti-terroriste.

- L'**article 1er** confie au **préfet la compétence pour instaurer des périmètres de protection** permettant d'assurer la sécurité de lieux ou d'événements soumis à un risque d'actes de terrorisme à raison de leur nature ou de l'ampleur de leur fréquentation.

Au sein de ce périmètre de protection, le préfet peut réglementer l'accès, la circulation et le stationnement des personnes, afin de pouvoir organiser le filtrage des accès au périmètre protégé.

- L'**article 2** permet au préfet de procéder, aux fins de prévenir des actes de terrorisme, à la **fermeture administrative**, pour une durée maximum de six mois, **des lieux de culte** dans lesquels les propos qui sont tenus, les idées ou théories qui sont diffusées, provoquent à la commission d'actes de terrorisme en France ou à l'étranger, incitent à la violence, ou font l'apologie de tels actes.

Afin d'encadrer l'exercice de ce pouvoir de fermeture administrative, une procédure contradictoire préalable est prévue, ainsi qu'un délai d'exécution permettant d'introduire un recours en référé devant le juge administratif. Ce recours sera suspensif.

- L'**article 3** établit des **mesures de surveillance que le ministre de l'intérieur peut prendre**, aux fins de **prévenir des actes de terrorisme**, à l'encontre de toute 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.

Le ministre de l'intérieur peut imposer à ces personnes :

- **de ne pas se déplacer à l'extérieur d'un périmètre géographique déterminé**, qui ne peut être inférieur à la commune, sans pouvoir, à la différence de la mesure d'assignation à résidence de l'état d'urgence, l'astreindre à demeurer dans un lieu déterminé pendant une partie de la journée. Cette mesure peut être assortie de l'obligation de se présenter au maximum une fois par jour aux services de police et de **déclarer son lieu d'habitation** et tout changement de ce dernier. L'intéressé peut être dispensé de cette obligation de présentation s'il accepte d'être **placé sous surveillance électronique mobile**. Ce placement, subordonné à l'accord écrit de la personne concernée, permet à tout moment à l'autorité administrative de s'assurer à distance que la personne n'a pas quitté le périmètre défini ;
- la déclaration des numéros d'abonnement et identifiants techniques de tout moyen de communication électronique ;

- l'interdiction de se trouver en relation avec certaines personnes dont il existe des raisons sérieuses de penser que leur comportement constitue une menace pour la sécurité publique.

La légalité de ces mesures peut être soumise au contrôle du juge administratif.

- L'**article 4** prévoit la **possibilité pour le préfet de faire procéder, sur autorisation du juge des libertés et de la détention (JLD), à une visite de tout lieu** pour lequel il existe des raisons sérieuses de penser qu'il est fréquenté par 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. **Cette visite peut s'accompagner de la saisie de documents, objets ou données** qui s'y trouvent.

Cette possibilité de visite est subordonnée à l'information du procureur de la République de Paris afin de ne pas interférer avec d'éventuelles procédures judiciaires en cours.

Comme pour tous les régimes de visites ordonnées en dehors d'une procédure judiciaire, la personne concernée peut contester à la fois l'ordonnance du JLD ayant autorisé la visite et la régularité de son déroulement.

L'exploitation des données informatiques contenues dans un équipement présent sur les lieux de la visite est également soumise à l'autorisation du JLD.

- Les **articles 5 et 6** visent à adapter et compléter notre législation pour satisfaire à l'obligation de **transposition de la directive dite PNR**[1] adoptée le 21 avril 2016.

Depuis plusieurs années, la France s'est dotée de plusieurs traitements de données à caractère personnel en vue d'exploiter les données de réservation ou **données « PNR »** (*Passenger Name Record*) ainsi que les données d'enregistrement ou **données « API »** (*Advanced Passenger Information*)[2] des passagers aériens, transmises par les transporteurs et par les opérateurs de voyage.

Les articles L. 232-1 à L. 232-6 du code de la sécurité intérieure ont autorisé le ministre de l'intérieur à mettre en oeuvre des traitements des données « API » et « PNR », lorsqu'elles sont recueillies à l'occasion de déplacements internationaux en provenance ou à destination d'États n'appartenant pas à l'Union européenne, afin **d'améliorer le contrôle aux frontières, de lutter contre l'immigration clandestine et de prévenir et réprimer des actes de terrorisme**. Sur ce fondement a été créé le **traitement de données dénommé SETRADER** (système européen de traitement des données d'enregistrement et de réservation) par arrêté du 11 avril 2013.

Après des années de négociation, la directive (UE) 2016/681 dite « directive PNR » a été adoptée le 21 avril 2016. En application de cette directive, les **transporteurs aériens** qui proposent des vols entre un pays tiers et le territoire d'au moins un État membre de l'Union européenne **seront contraints de communiquer les données « PNR » aux autorités compétentes de cet État membre.**

Bien que le « système API-PNR France » ait été construit sur la base de la proposition de la directive en cours de discussion, **le cadre législatif national des traitements de données recueillies à l'occasion de déplacements internationaux doit être ajusté et complété pour satisfaire à l'obligation de transposition de la directive avant le 25 mai 2018.**

---

[1] *Les données « PNR » (Passenger Name Record) sont des informations déclaratives fournies par une personne, un organisme ou une agence de voyage afin de réserver un voyage auprès d'un transporteur aérien.*

[2] *Les données « API »* (*Advanced Passenger Information*) *sont les données recueillies par les transporteurs aériens lors de l'enregistrement et l'embarquement du voyageur.*

- L'**article 7** crée un **système national de centralisation des données des dossiers passagers du transport maritime** à destination ou au départ de la France (distinct du système « PNR » concernant les passagers du transport aériens), toujours afin de prévenir et de détecter les infractions terroristes.

II - DISPOSITIONS RELATIVES AUX TECHNIQUES DE RENSEIGNEMENT

Le chapitre II relatif aux techniques de renseignement comprend les **articles 8 et 9** qui instaurent un **nouveau régime légal de surveillance des communications hertziennes**[3], pour tirer les conséquences de la décision QPC du 21 octobre 2016 par laquelle le Conseil constitutionnel a censuré, avec effet différé au 31 décembre 2017, les dispositions du code de la sécurité intérieure qui permettent aux pouvoirs publics de prendre, à des fins de défense des intérêts nationaux, des **mesures de surveillance et de contrôle des transmissions empruntant la voie hertzienne**.

Le code de la sécurité intérieure est modifié pour **permettre aux services de renseignement d'intercepter et d'exploiter les communications électroniques empruntant la voie exclusivement hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques** exploitant un réseau ouvert au public.

III - DISPOSITIONS RELATIVES AUX CONTRÔLES DANS LES ZONES FRONTALIÈRES

Le chapitre III relatif aux contrôles dans les zones frontalières comprend l'**article 10** qui **élargit les possibilités de contrôle dans les zones frontalières intérieures et extérieures**, afin de mieux contrôler l'immigration et prévenir les actes de terrorisme.

Le code de procédure pénale prévoit actuellement que ces contrôles peuvent être effectués, notamment, dans une bande de vingt kilomètres le long des frontières intérieures, ainsi que dans les zones accessibles au public des ports, des aéroports et des gares ferroviaires et routières ouverts au trafic international.

L'article 10 du PJL **élargit le périmètre de contrôle** dans cette zone. La zone frontalière de vingt kilomètres le long des frontières intérieures est maintenue, de même que la possibilité de contrôle dans les zones accessibles au public des ports, aéroports et gares ferroviaires ou routières ouverts au trafic international. L'article 10 **élargit les possibilités de contrôles aux abords de ces gares,** compte tenu de la nécessité de pouvoir exercer ces mêmes contrôles dans leur environnement immédiat.

Par ailleurs l'article 10 **étend la durée du contrôle**. Celle-ci doit être limitée, conformément à la jurisprudence de la Cour de justice de l'Union européenne. Toutefois, l'actuelle durée de six heures est, dans le contexte actuel, beaucoup trop courte. Le texte porte cette **durée à un maximum de douze heures** consécutives de présence dans un même lieu.

---

[3] *On vise ici l'interception et l'exploitation des communications radio très longue distance (gamme VLF, très basses fréquences), longue distance (gamme « HF », hautes fréquences) et courte distance (gamme V/UHF, très et ultra hautes fréquences).*
Exemple : Des individus impliqués dans une prise d'otage ou une opération terroriste peuvent ainsi utiliser des talkies walkies ou des PMR (gamme V/UHF, la PMR - private mobile radio - étant une version numérique du talkie-walkie *analogique) pour se coordonner ou communiquer avec des complices.*